UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Jure Markun

Prevoji kubičnih krivulj

Delo diplomskega seminarja

Mentorica: doc. dr. Anita Buckley

Ljubljana, 2018

Kazalo

Prevoji kubičnih krivulj

Povzetek

Namen tega diplomskega seminarja je obravnava algebraičnih krivulj tretje stopnje in njihovih prevojnih točk. Opisane so lastnosti kubičnih krivulj ter struktura Abelove grupe na točkah gladke kubike ter v posebnem primeru na prevojnih točkah. Predstavljen je problem eksplicitnega izračuna prevojev iz koeficientov krivulje. Rešljivost tega problema je ekvivalentna rešljivosti Galoisove grupe, prirejene krivulji. Podan je tudi postopek za ekspliciten izračun prevojev. Z izračunanim prevojem lahko kubično krivuljo s projektivnimi transformacijami preoblikujemo v Weierstrassovo obliko.

Flexes of Cubic Curves

Abstract

The topic of this seminar are algebraic curves of degree three - cubic curves and their flexes. We study properties of curves and introduce Abelian group structure on the points of a nonsingular cubic and also on the flexes. We explain how to calculate the 9 flexes explicitely from the coefficients of a curve. To show that the calculation is always possible, we prove the solvability of the Galois group of flexes. Given a flex on a cubic curve, it is possible to put the curve into Weierstrass form using projective transformations.

Math. Subj. Class. (2010): 14H52,14H50,14L35,51N30

Ključne besede: kubične krivulje, prevoji kubičnih krivulj, Galoisove grupe, Abelova grupa na kubični krivulji, Hessejeva konfiguracija

Keywords: cubic curves, flexes of cubic curves, Galois groups, Abelian group on cubic curve, Hesse configuration

1. Uvod

Algebraične krivulje so področje matematike, ki je preučevano že več kot 2000 let; z njimi so se ukvarjali Grki, Arabci ter kasneje renesančni slikarji (med drugimi tudi Da Vinci). Vendar so se šele od 17. stoletja naprej, ko so v geometrijo uvedli uporabo koordinat (Descartes, Fermat), začele pojavljati v obliki, kot jih poznamo danes. Leta 1700 je Isaac Newton izdal poglobljeno raziskavo kubičnih krivulj ter opisal 72 različnih primerov. Matematiki tistega časa so preučevali zgolj realne algebraične krivulje.

Šele v 19. stoletju so se z uvedbo kompleksnih števil pokazale prednosti, da algebraične krivulje preučujemo tudi nad obsegom $\mathbb{C}$. Prav tako so se takrat postavili temelji projektivne geometrije, ki so dodatno pospešili raziskovanje ter povezali algebraične krivulje s topologijo in kompleksno analizo. Vodilni na tem področju so bili Riemann, Dedekind in Weber.[6, poglavje 1.1]

Prevoje kubičnih krivulj so preučevali že klasični geometri Hesse, Steiner, Cayley in Clebsch. Prvi, ki je problem iskanja prevojev kubičnih krivulj povezal z Galoisovo teorijo že v času pričetka njenega razvoja, je bil francoski matematik Camille Jordan v svojem delu iz leta 1870, *Traité des substitutions et des équations algébriques.* Tam je izhajal iz Hessejeve interpretacije prevojev kubičnih krivulj in na njih našel Galoisovo grupo.[3, str. 686]

Algebraične krivulje se aktivno preučujejo še danes in njihova teorija je uporabna na mnogih področjih, vse od kriptografije, teorije števil do teoretične fizike. Razlogi za to so številne algebraične lastnosti, izpeljane povezave z Riemannovimi ploskvami v kompleksni analizi ter njihova praktična uporaba v kriptografiji. Tudi prevojne točke kubičnih krivulj imajo v teoriji velik pomen. Geometrijska konfiguracija prevojnih točk omogoča njihov ekspliciten izračun, ki ima tako teoretično kot tudi praktično vrednost.

2. Algebraične krivulje

Najprej podajmo definicijo in lastnosti afinih ter projektivnih prostorov, v katerih bomo algebraične krivulje definirali. Naj bo $\mathcal{O}$ komutativen obseg. Z $\mathcal{A}^n = \mathcal{O}^n$ označimo afin prostor dimenzije n, to je n-dimenzionalni vektorski prostor nad obsegom $\mathcal{O}$, ki ga bomo obravnavali kot geometrijski prostor.

Izreki in definicije iz tega poglavja so, če ni drugače navedeno, povzeti po [1], [6] in [11].

Definicija 2.1. Naj bo $U \subseteq \mathcal{A}^n$ vektorski podprostor in $a \in \mathcal{A}^n$. *Afin podprostor* prostora je množica

$$\mathcal{A} = a + U = \{a + u; u \in U\}.$$

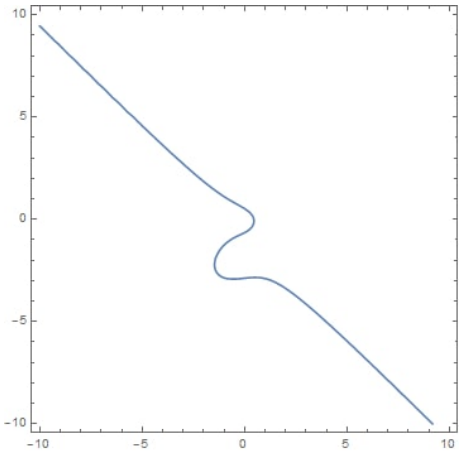
Definicija 2.2. Afina podprostora $A = a + U$ in $B = b + W$ v $\mathcal{A}^n$ sta si *vzporedna* natanko tedaj, ko velja $U \subset W$ ali $W \subset U$.

Definicija 2.3. *Algebraično zaprt obseg* je obseg, v katerem vsak nekonstanten polinom v eni spremenljivki razpade na linearne faktorje.

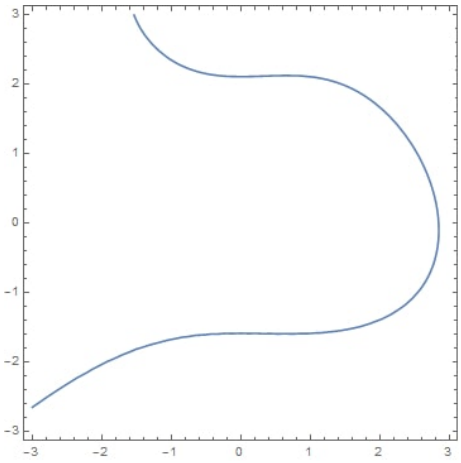
Definicija 2.4. Naj bo $\mathcal{O}$ algebraično zaprt obseg, $p(X,Y)$ pa polinom v dveh spremenljivkah s koeficienti iz obsega $\mathcal{O}$. Množica točk

$$M_p = \{(X,Y) \in \mathcal{A}^2; p(X,Y) = 0\}$$

je *množica ničel* polinoma $p(X,Y)$. Množico točk $\mathcal{C} \subset \mathcal{A}^2$ imenujemo *afina algebraična krivulja*, če obstaja tak polinom $p(X,Y)$ v dveh spremenljivkah s koeficienti iz obsega $\mathcal{O}$, da velja $\mathcal{C} = M_p$.



Slika 1. Afina krivulja, podana s polinomom $p(X,Y) = X^3 + Y^3 + 3Y^2 + XY + 2X - 1$.



Slika 2. Afina krivulja, podana s polinomom $p(X,Y) = X^3 - Y^3 - X^2 + 5Y^2 + Y - 15$.

Afine algebraične krivulje so torej množice ničel polinomov. Vzemimo sedaj afin prostor $\mathcal{A}^n$. Če sta dva afina podprostora $A = a + U$ in $B = b + W$ vzporedna in $a \neq b$, se ne sekata v nobeni točki.

Poleg afinih pa definirajmo še projektivne prostore.

Definicija 2.5. [10, Definicija 4.1] Naj bo V končnorazsežen vektorski prostor nad obsegom $\mathcal{O}$. Množica vseh vektorskih podprostorov v V se imenuje *projektivna geometrija* $\mathbb{P}(V)$ nad V. Enorazsežne podprostore imenujemo točke projektivne geometrije, dvorazsežne projektivne premice, vektorske podprostore korazsežnosti 1 pa imenujemo projektivne hiperravnine. *Projektivni prostor* $\mathcal{P}(V)$ je množica vseh točk projektivne geometrije $\mathbb{P}(V)$.

Za lažje razumevanje pojasnimo, kako pridemo do projektivnih prostorov s pomočjo afinih prostorov. V afinem prostoru $\mathcal{A}^n$ smo že omenili, da se različni vzporedni

podprostori ne sekajo v nobeni točki. Drugače pa je v projektivni geometriji: če je med dvema podprostoroma afinega prostora relacija vzporednosti, podprostoroma dodamo neko množico v neskončnosti, v kateri se sekata. Z dodajanjem množice v neskončnosti vsem vzporednim podprostorom afinega prostora $\mathcal{A}^n$ dobimo projektivni prostor $\mathcal{P}^n$. Množica, ki jo podprostoroma dodamo, je za eno dimenzijo manjša od dimenzije manjšega od teh podprostorov. Tako se v projektivni ravnini $\mathcal{P}^2$ dve vzporedni premici sekata v točki v neskončnosti, v projektivnem prostoru $\mathcal{P}^3$ se vzporedna premica in ravnina sekata v točki v neskončnosti, dve vzporedni ravnini se sekata v premici v neskončnosti ipd.

Prvo omenjeno situacijo si lahko predstavljamo s tirnicami, ki jih smatramo za dve vzporedni premici. Vidimo, da kljub njuni vzporednosti na obzorju izgleda, kot da imata premici presečišče. Točki v neskončnosti rečemo tudi točka na obzorju.

Tudi več paroma vzporednih podprostorov se seka v isti množici v neskončnosti, ki je eno dimenzijo manjša od dimenzije najmanjšega podprostora. Torej, če vzamemo šop vzporednih premic v afinem prostoru, se bodo te premice v projektivnem prostoru sekale v isti točki v neskončnosti.

Slika 3. Prikaz dveh vzporednih premic, ki se sekata v točki v neskončnosti [16].

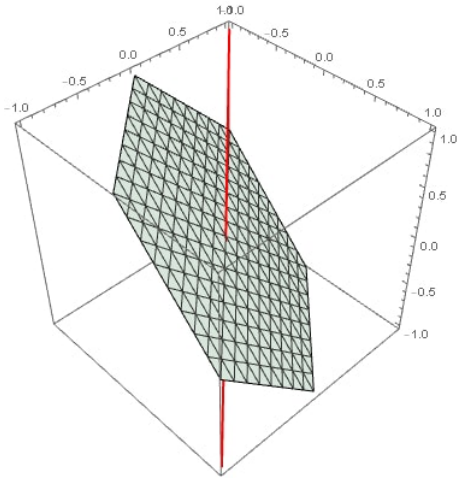
V nadaljevanju se bomo osredotočili zgolj na projektivni prostor $\mathcal{P}^2 = \mathcal{P}^2(\mathbb{C})$ nad obsegom kompleksnih števil, ki ga imenujemo tudi *kompleksna projektivna ravnina.*

Kompleksna projektivna ravnina $\mathcal{P}^2$ je množica vseh točk, ki na tej ravnini ležijo. *Točke kompleksne projektivne ravnine* so predstavljene s *projektivnimi* oziroma *homogenimi koordinatami* oblike $[x,y,z]$, kjer so x,y,z iz obsega $\mathbb{C}$. Tak zapis ponazarja množico

$$[x,y,z] = \{\lambda(x,y,z); \lambda \in \mathbb{C} \setminus \{0\}, (x,y,z) \neq (0,0,0)\}.$$

Kot vidimo, so točke na kompleksni projektivni ravnini kompleksni enodimenzionalni podprostori vektorskega prostora $\mathbb{C}^3$ brez izhodišča. Premice na kompleksni projektivni ravnini pa so kompleksni dvodimenzionalni podprostori vektorskega prostora $\mathbb{C}^3$ brez izhodišča. Vsaki dve projektivni premici v projektivni ravnini se sekata natanko v eni točki projektivne ravnine.

Kompleksna projektivna ravnina $\mathcal{P}^2(\mathbb{C})$ ima kompleksno dimenzijo 3. Ker nam prevelika dimenzija onemogoča geometrijsko predstavo, si točke na njej predstavljamo v 3-dimenzionalnem realnem evklidskem prostoru $\mathbb{R}^3$ kot premice skozi izhodišče, premice projektivne ravnine pa kot ravnine skozi izhodišče. Vendar pa se moramo vedno zavedati, da smo dejansko nad obsegom $\mathbb{C}$, zato ima vsaka podmnožica $\mathcal{P}^2$ poleg realnega dela še nek kompleksni del, ki ga pa na grafičnih prikazih ne moremo videti.



SLIKA 4. Točka $[-1,1,1]$ in premica $y + x + z = 0$ v projektivni ravnini.

Tudi pri definiciji algebraičnih krivulj v $\mathcal{P}^2$ moramo upoštevati homogenost koordinat in jih v projektivnem prostoru malce drugače definirati.

Definicija 2.6. Naj bo $\mathcal{O}$ algebraično zaprt obseg, $p(x,y,z)$ pa homogen polinom s koeficienti iz obsega $\mathcal{O}$. Množica točk v kompleksni projektivni ravnini

$$M_p = \{[x,y,z] \in \mathcal{P}^2; p(x,y,z) = 0\}$$

je *množica ničel* polinoma $p(x,y,z)$. Množico točk $\mathcal{C} \subset \mathcal{P}^2$ imenujemo *projektivna algebraična krivulja*, če obstaja tak homogen polinom $p(x,y,z)$ v treh spremenljivkah s koeficienti iz obsega $\mathcal{O}$, da velja $\mathcal{C} = M_p$.

V nasprotju z njihovim poimenovanjem si projektivne algebraične krivulje v $\mathcal{P}^2$ lahko predstavljamo kot ploskve skozi izhodišče kompleksne dimenzije 2. Spomnimo se, da so projektivne točke afine premice skozi izhodišče (brez izhodišča), projektivne algebraične krivulje pa so unije teh afinih premic - projektivnih točk.

Trditev 2.7. *Obstaja neskončno različnih polinomov, katerih množica ničel je ista algebraična krivulja.*

Dokaz. Za dokaz zadošča že, da vzamemo en polinom $p(x,y,z)$, ki podaja krivuljo $\mathcal{C}$, ter definiramo množico

$$\{p(x,y,z)^n; n \in \mathbb{N}\}.$$

To je očitno neskončna množica polinomov, katerih ničle podajajo algebraično krivuljo $\mathcal{C}$. □

Definicija 2.8. Nekonstantni polinom $p(x,y,z)$ s koeficienti iz obsega $\mathcal{O}$ je nad $\mathcal{O}$ *nerazcepen*, če ga ni mogoče zapisati kot produkt dveh nekonstantnih polinomov s koeficienti iz $\mathcal{O}$.

Definicija 2.9. Projektivna algebraična krivulja $\mathcal{C}$ v projektivni ravnini $\mathcal{P}^2(\mathbb{C})$ je *nerazcepna*, če je polinom $p(x,y,z)$ s koeficienti iz $\mathbb{C}$, ki jo podaja, nerazcepen nad poljem $\mathbb{C}$.

Izrek 2.10. [11] *Naj bo $\mathcal{C}$ algebraična krivulja. Potem ima $\mathcal{C}$ enoličen zapis kot unija nerazcepnih krivulj*

$$\mathcal{C} = \mathcal{C}_1 \bigcup \mathcal{C}_2 \bigcup \cdots \bigcup \mathcal{C}_r,$$

kjer je $\mathcal{C}_i$ *nerazcepna in* $\mathcal{C}_i \nsubseteq \bigcup_{\substack{j=1 \\ j\neq i}}^{r} \mathcal{C}_j$ *za vsak* $i \in \{1,2,\ldots,r\}$.

Naj bo $\mathcal{C} = \mathcal{C}_1 \bigcup \mathcal{C}_2 \bigcup \cdots \bigcup \mathcal{C}_r$ razcep krivulje na nerazcepne komponente. Potem je polinom $p(x,y,z)$, ki določa $\mathcal{C}$, oblike

$$p(x,y,z) = q_1(x,y,z)^{k_1} q_2(x,y,z)^{k_2} \cdots q_r(x,y,z)^{k_r},$$

kjer je $q_i(x,y,z)$ nerazcepen in določa $\mathcal{C}_i$. Za ta polinom $p(x,y,z)$ definirajmo drug polinom $p'(x,y,z) = q_1(x,y,z)q_2(x,y,z)\cdots q_r(x,y,z)$. Ta polinom imenujemo *minimalni polinom* krivulje $\mathcal{C}$. Kljub temu, da ima vsaka algebraična krivulja $\mathcal{C}$ neskončno polinomov, ki jo podajajo, pa lahko za vsako enolično izberemo tisti polinom krivulje, ki je produkt polinomov njenih nerazcepnih faktorjev na potenco 1. *Stopnja algebraične krivulje* $\mathcal{C}$ je definirana kot stopnja minimalnega polinoma, ki krivuljo podaja. Označimo jo s $\operatorname{st}\mathcal{C}$. V tem besedilu se bomo ukvarjali s krivuljami tretje stopnje oziroma *kubičnimi krivuljami* v projektivni ravnini $\mathcal{P}^2(\mathbb{C})$. Koeficienti njihovih polinomov bodo iz obsega $\mathbb{C}$.

Vrnimo se k algebraičnim krivuljam v afini ravnini. Splošna oblika polinoma, ki podaja afino kubično krivuljo, je

$$p(X,Y) = a_{30}X^3 + a_{03}Y^3 + a_{21}X^2Y + a_{12}XY^2 + a_{20}X^2 + a_{02}Y^2 + a_{11}XY + a_{10}X + a_{01}Y + a_{00}, a_{i,j} \in \mathbb{C}.$$

Vsako afino algebraično krivuljo je možno prevesti v projektivno algebraično krivuljo. To naredimo s *homogenizacijo* njenega polinoma, ki je definirana kot preslikava

$$p(X,Y) \mapsto z^{(\operatorname{st} p(X,Y))} p(\frac{x}{z}, \frac{x}{z}),$$

ki nam polinom v dveh spremenljivkah preslika v homogen polinom v treh spremenljivkah enake stopnje. Splošna oblika polinoma, ki podaja projektivno kubično krivuljo, je potem

$$p(x,y,z) = a_{30}x^3 + a_{03}y^3 + a_{21}x^2y + a_{12}xy^2 + a_{20}x^2z + a_{02}y^2z + a_{11}xyz + a_{10}xz^2 + a_{01}yz^2 + a_{00}z^3, a_{i,j} \in \mathbb{C}.$$

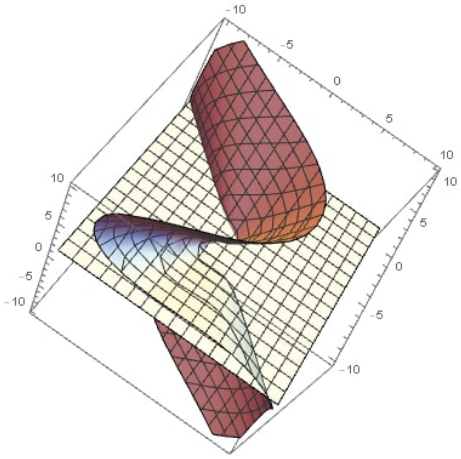
Če pa želimo narediti obratno, torej obravnavati projektivno krivuljo kot afino, si moramo izbrati kompleksno afino ravnino v $\mathbb{C}^3$, v kateri bi krivuljo opazovali. Edini pogoj za to afino ravnino je, da ne gre skozi izhodišče, saj izhodišče ni vsebovano v $\mathcal{P}^2$. Običajno se zaradi enostavnosti zapisa odločimo kar za ravnino $z = 1$. Presek afine ravnine s projektivno algebraično krivuljo nam da afino algebraično krivuljo. V primeru $z = 1$ za polinom $p(x,y,z)$ je ta podana s polinomom $p(X,Y) = p(X,Y,1)$. Afine krivulje, ki jih dobimo s preseki projektivne krivulje z različnimi ravninami, so si projektivno ekvivalentne.

Opomba 2.11. Ker je obseg $\mathbb{C}$ algebraično zaprt, so vsi polinomi v eni spremenljivki s koeficienti iz tega obsega razcepni do linearnih faktorjev, kar pa ne velja za polinome več spremenljivk.

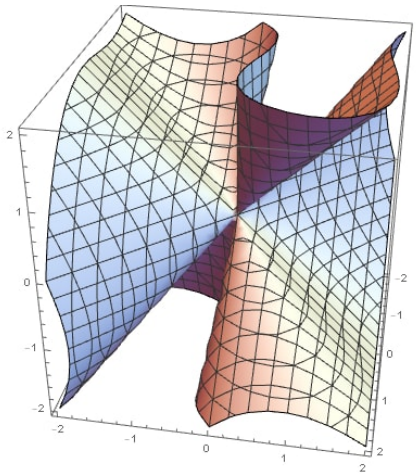
Velja pa za homogene polinome v dveh spremenljivkah.

Lema 2.12. [6, Lema 2.8] *Naj bo* $p(x,y)$ *neničelen homogen polinom stopnje* d *v dveh spremenljivkah s koeficienti iz* $\mathbb{C}$. *Ta polinom je mogoče razcepiti na produkte linearnih polinomov*

$$p(x,y) = \prod_{i=1}^{d} (\alpha_i x + \beta_i y).$$



Slika 5. Projektivna kubična krivulja, podana s polinomom $p(x,y,z) = x^3 + y^3 + 3y^2z + xyz + 2xz^2 - z^3$ v preseku z afino ravnino $z = 1$. Presek je afina kubična krivulja na sliki 1 .



Slika 6. Projektivna krivulja, podana s polinomom $p(x,y,z) = x^3 + y^3 + x^2z - yz^2$.

Dokaz. Ker je polinom homogen, ga lahko zapišemo kot

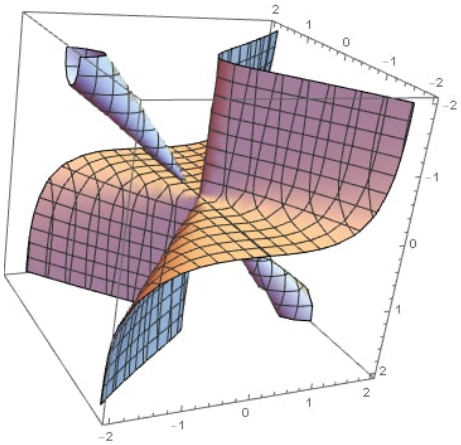
$$p(x,y) = \sum_{r=0}^{d} a_r x^r y^{d-r} = y^d \sum_{r=0}^{d} a_r \left(\frac{x}{y}\right)^r,$$

kjer $a_1,a_2,\ldots,a_n \in \mathbb{C}$ niso vsi ničelni. Naj bo e največji tak element iz $\{0,\ldots,d\}$, za katerega velja $a_e \neq 0$. Potem je

$$\sum_{r=0}^{d} a_r \left(\frac{x}{y}\right)^r = \sum_{r=0}^{e} a_r u^r$$

polinom s kompleksnimi koeficienti stopnje e v eni spremenljivki $u = \frac{x}{y}$. Ker je $\mathbb{C}$ algebraično zaprt obseg, lahko po definiciji 2.3 polinom faktoriziramo kot

$$\sum_{r=0}^{e} a_r u^r = a_e \prod_{i=1}^{e} (u - \gamma_i)$$



SLIKA 7. Projektivna krivulja, podana s polinomom $p(x,y,z) = 4x^2z + xyz + y^3 - 2y^2z + yz^2$.

za neke $\gamma_1,\gamma_2,\ldots,\gamma_e \in \mathbb{C}$. Zato velja

$$p(x,y) = a_e y^d \prod_{i=1}^{e} \left(\frac{x}{y} - \gamma_i\right) = a_e y^{d-e} \prod_{i=1}^{e} (x - \gamma_i y).$$

To je produkt linearnih faktorjev, zato je dokaz končan. □

Definicija 2.13. [10, Definicija 4.26 in Definicija 4.34] Naj bosta V in V' vektorska prostora nad obsegom $\mathcal{O}$ razsežnosti $\operatorname{st} V = \operatorname{st} V' \geq 3$. Bijektivno linearno preslikavo $\phi : \mathcal{P}(V) \to \mathcal{P}(V')$, ki poljubne tri kolinearne točke preslika v kolinearne, imenujemo *projektivnost* ali *projektivna transformacija*.

Definicija 2.14. Naj bo $\mathcal{C}$ nerazcepna kubična krivulja, podana s polinomom

$$p(x,y,z) = -zy^2 + x^3 + axz^2 + bz^3,$$

kjer sta $a,b \in \mathbb{C}$. Tako obliko zapisa kubične krivulje imenujemo *Weierstrassova kanonična forma*. Krivulja v tej obliki je s koeficientoma a in b natanko določena.

Opomba 2.15. Krivuljo v Weierstrassovi formi pogosto opazujemo kot afino algebraično krivuljo v ravnini $z = 1$. Tam je njena enačba $Y^2 = X^3 + aX + b$.

Brez dokaza podajmo naslednjo trditev.

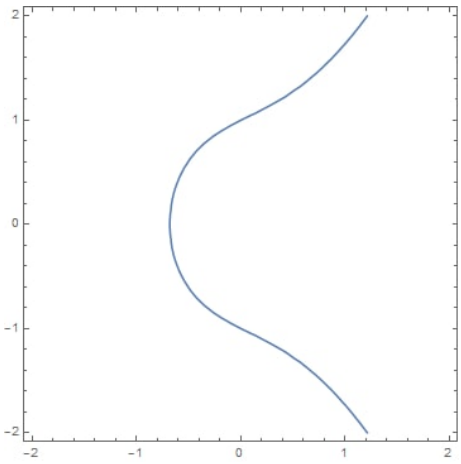
Trditev 2.16. *Vsako nerazcepno kubično krivuljo lahko s projektivnimi transformacijami pretvorimo v Weiestrassovo formo.*

Ker lahko vsako kubično krivuljo s projektivnimi transformacijami preslikamo v Weierstrassovo formo za točno določena $a,b \in \mathbb{C}$, opazimo, da je kubičnih krivulj, ki si niso projektivno ekvivalentne, ravno za dva kompleksna prosta parametra $a,b \in \mathbb{C}$ oziroma 4 realne dimenzije.

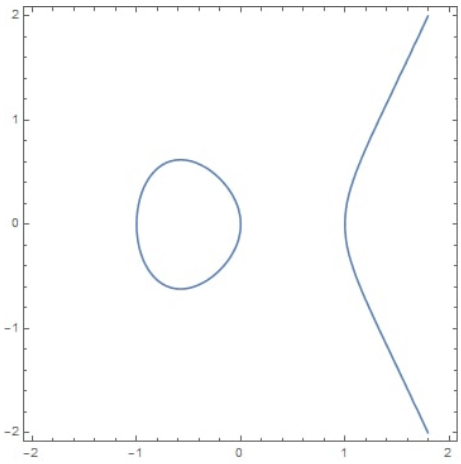
Definicija 2.17. Naj bo $\mathcal{O}$ obseg. *$\mathcal{O}$-racionalna točka* je taka točka $[x,y,z]$ na projektivni algebraični krivulji $\mathcal{C}$, za katero so x,y,z v obsegu $\mathcal{O}$. Če ni drugače določeno, običajno vzamemo $\mathcal{O} = \mathbb{Q}$.

Kubične krivulje v Weierstrassovi obliki se zelo pogosto uporabljajo v kriptografiji. Vendar pa so pri uporabi na tem področju krivulje že pri zastavitvi problema podane na ta način. Če pa želimo krivuljo, ki je podana s homogenim polinomom, pretvoriti v Weierstrassovo obliko, v splošnem potrebujemo vsaj eno njeno prevojno točko ali racionalno točko nad poljem $\mathbb{Q}$. Če imamo zgolj racionalno točko na krivulji, ta primore k postopku iskanja prevoja, vendar pa je postopek precej hitrejši, če smo prevoj predhodno že našli. To je ena izmed osnovnih praktičnih motivacij, zakaj je izračun prevojev kubične krivulje pomemben.

Geometrijske lastnosti prvotne krivulje se pri postopku prevedbe krivulje na Weierstrassovo obliko ohranijo, ali so v kanonični formi celo lepše izpostavljene. Med te lastnosti spadajo singularne točke na krivulji ter celotna struktura Abelove grupe na kubiki, katere prikaz je na transformirani kubiki mnogo elegantnejši. Na slikah 8, 9, 10 si lahko ogledamo, kako različne krivulje v Weiestrassovi obliki izgledajo v afini ravnini $z = 1$.



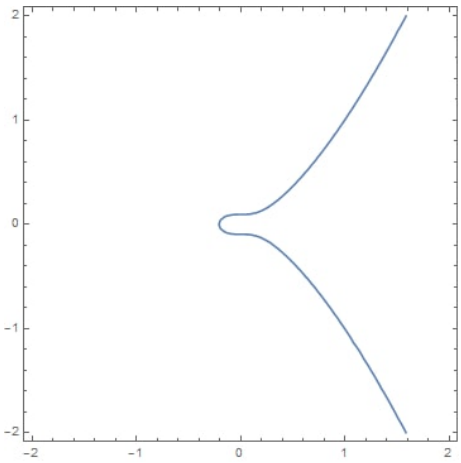
Slika 8. Weierstrassova kubika $y^2 = x^3 + x + 1$.



Slika 9. Weierstrassova kubika $y^2 = x^3 - x$.

3. Prevoji kubičnih krivulj

Definicija 3.1. [6, Definicija 3.27] Naj bo $p(x,y,z)$ homogen polinom stopnje d, ki podaja projektivno algebraično krivuljo $\mathcal{C}$. *Hessejeva matrika* krivulje $\mathcal{C}$ je definirana



SLIKA 10. Weierstrassova kubika $y^2 = x^3 + \frac{1}{108}$.

kot matrika drugih parcialnih odvodov polinoma $p(x,y,z)$:

$$H_p(x,y,z) = \begin{pmatrix} \frac{\partial^2 p}{\partial x^2} & \frac{\partial^2 p}{\partial x \partial y} & \frac{\partial^2 p}{\partial x \partial z} \\ \frac{\partial^2 p}{\partial y \partial x} & \frac{\partial^2 p}{\partial y^2} & \frac{\partial^2 p}{\partial y \partial z} \\ \frac{\partial^2 p}{\partial z \partial x} & \frac{\partial^2 p}{\partial z \partial y} & \frac{\partial^2 p}{\partial z^2} \end{pmatrix}.$$

Determinanta te matrike je polinom $h(x,y,z) = \det H_p$, ki podaja neko drugo krivuljo $\mathcal{H}_\mathcal{C}$. To krivuljo pa imenujemo *Hessejeva krivulja* prvotne krivulje $\mathcal{C}$.

Stopnja polinoma $h(x,y,z)$ je največ $3(d-2)$, zato je tudi stopnja Hessejeve krivulje lahko največ $3(d-2)$.

Če je $\mathcal{C}$ kubična krivulja, opazimo, da je stopnja polinoma Hessejeve krivulje $h(x,y,z)$ največ 3. Zato je v splošnem Hessejeva krivulja kubične krivulje prav tako kubična krivulja. Včasih pa se zgodi, da so Hessejeve krivulje kubičnih krivulj tudi krivulje manjših stopenj.

Definicija 3.2. [6, Definicija 3.29] Nesingularna točka $A = [s,t,u]$ na projektivni krivulji $\mathcal{C}$ v $\mathcal{P}^2$, ki je podana s polinomom $p(x,y,z)$, se imenuje *prevoj* ali *prevojna točka* krivulje $\mathcal{C}$, če velja

$$h(s,t,u) = 0,$$

kjer je $h(x,y,z)$ polinom Hessejeve krivulje.

Prevojne točke so torej točke na $\mathcal{C}$, ki ležijo tudi na $\mathcal{H}_\mathcal{C}$. Zato si najprej oglejmo presek dveh kubičnih krivulj $\mathcal{C}_1$ in $\mathcal{C}_2$. Zanj velja sledeče:

- Krivulji $\mathcal{C}_1$ in $\mathcal{C}_2$ se sekata v vsaj eni točki;
- Če imata $\mathcal{C}_1$ in $\mathcal{C}_2$ skupno komponento, potem je točk v preseku neskončno;
- Če $\mathcal{C}_1$ in $\mathcal{C}_2$ nimata skupne komponente, je v preseku končno število točk.

Če imamo podani dve kubični krivulji brez skupne komponente, nas seveda zanima, koliko točk vsebuje končni presek teh krivulj. Na to vprašanje nam odgovori Bezoutjev izrek. Za njegovo razumevanje pa bo potrebno razjasniti še pojma rezultante in presečne večkratnosti dveh krivulj v posamezni točki.

Definicija 3.3. [6, Definicija 3.2] Naj bosta $p(x,y,z)$ in $q(x,y,z)$ homogena polinoma stopenj n in m s koeficienti iz $\mathbb{C}$, ki določata krivulji $\mathcal{C}_1$ in $\mathcal{C}_2$. Brez škode za splošnost

predpostavimo, da velja $n \geq m$. Razvijmo ta polinoma po potencah x, in tako dobimo

$$p(x,y,z) = a_0(y,z) + a_1(y,z)x + \cdots + a_n(y,z)x^n,$$
$$q(x,y,z) = b_0(y,z) + b_1(y,z)x + \cdots + b_m(y,z)x^m.$$

Rezultanta $\mathcal{R}_{p,q}(y,z)$ polinomov $p(x,y,z)$ in $q(x,y,z)$ je determinanta kvadratne $n+m$ matrike v odvisnosti od koeficientov polinomov, razvitih po x,

$$R_{p,q}(y,z) = \det \begin{pmatrix} a_0 & & \dots & \dots & & a_n & & \\ & \ddots & & & & & \ddots & \\ & & a_0 & & \dots & \dots & & a_n \\ b_0 & \dots & \dots & b_m & & & & \\ & & \ddots & & & \ddots & & \\ & & & & & & & \\ & & & & b_0 & \dots & \dots & b_m \end{pmatrix}.$$

Koeficienti a_i so vsebovani v m vrsticah, b_j pa v n. Rezultanta je bodisi homogen polinom stopnje nm v spremenljivkah y in z, ali pa je enaka 0.

Opomba 3.4. Rezultanta se uporablja tudi za polinome v eni ali dveh spremeljivkah. Za polinom v eni spremenljivki so koeficienti a_i in b_j konstantni in rezultanta nam vrne numerično rešitev.

Opomba 3.5. Rezultanto lahko razvijemo po katerikoli od spremenljivk x,y ali z. Da pa se izognemo singularnim primerom, moramo upoštevati:

- Razvijamo lahko po spremenljivki x, če [1,0,0] ni ničla polinomov p in q.
- Razvijamo lahko po spremenljivki y, če [0,1,0] ni ničla polinomov p in q.
- Razvijamo lahko po spremenljivki z, če [0,0,1] ni ničla polinomov p in q.

Tako se izognemo situacijam, ko bi imela oba polinoma, razvita po določeni spremeljivki, koeficient pri maksimalni stopnji te spremenljivke enak 0. To bi namreč povzročilo, da bi bila njuna rezultanta enaka 0, saj bi vsi koeficienti v zadnjem stolpcu matrike enaki 0. Brez dokaza podajmo naslednjo lemo.

Lema 3.6. [6, Lema 3.3, Lema 3.4] *Za rezultanto dveh polinomov velja sledeče:*

(a) Polinoma $p(x)$ in $q(x)$ v eni spremenljivki imata nekonstantni skupni faktor natanko tedaj, ko velja

$$\mathcal{R}_{p,q} = 0.$$

(b) Naj bosta $p(x,y,z)$ in $q(x,y,z)$ taka nekonstantna homogena polinoma, da je

$$p(1,0,0) \neq 0, q(1,0,0) \neq 0.$$

Potem imata polinoma p in q skupni homogeni faktor natanko tedaj, ko velja

$$\mathcal{R}_{p,q}(y,z) = 0.$$

Pogoj $p(1,0,0) \neq 0$ in $q(1,0,0) \neq 0$ v lemi zopet zagotavlja, da polinom pri razvoju po spremenljivki x ni manjše stopnje, kot je polinom v vseh spremenljivkah (x,y,z).

Pri tej lemi dobimo idejo, da bi morda lahko prevoje kubične krivulje iskali preko rezultante. Naj bo $p(x,y,z)$ polinom, ki podaja kubično krivuljo $\mathcal{C}$. Najprej lahko izračunamo njeno Hessejevo krivuljo, ki ima polinom $h(x,y,z)$, ter potem oba polinoma razvijemo po y; brez škode za splošnost dodatno predpostavimo, da [0,1,0] ne leži na obeh krivuljah. Ko izračunamo rezultanto, dobimo polinom 9. stopnje v

x in z. Kar lahko še storimo za poenostavitev problema je, da se osredotočimo na krivuljo v neki afini ravnini – to metodo bomo večkrat uporabili tudi v nadaljevanju. Naj bo ta afina ravnina $z = 1$. Tako nam ostane polinom stopnje 9 v x. Tukaj pa se postopek izračuna zaenkrat ustavi: ničel splošnega polinoma stopnje 9 namreč ni možno eksplicitno izračunati. V nadaljevanju bomo videli, da za naš polinom to vendarle lahko storimo, vendar moramo pred tem še pojasniti, zakaj je tako.

Sedaj pa si poglejmo še pojem presečne večkratnosti.

Definicija 3.7. [6, Izrek 3.18] Za vsako točko v $\mathcal{P}^2$ lahko določimo *presečno večkratnost* dveh projektivnih krivulj $\mathcal{C}_1$ in $\mathcal{C}_2$ v tej točki. Presečno večkratnost v točki A označimo z $I_A(\mathcal{C}_1,\mathcal{C}_2)$. Presečna večkratnost je enolično določena z naslednjimi lastnostmi:

(1) $I_A(\mathcal{C}_1,\mathcal{C}_2) = I_A(\mathcal{C}_2,\mathcal{C}_1)$.

(2) $I_A(\mathcal{C}_1,\mathcal{C}_2) = \infty$, če točka A leži na skupni komponenti obeh krivulj, sicer pa je nenegativno celo število.

(3) $I_A(\mathcal{C}_1,\mathcal{C}_2) = 0$ če $A \notin \mathcal{C}_1 \cap \mathcal{C}_2$.

(4) Vsaki dve projektivni premici se sekata v natanko eni točki in v tej točki je presečna večkratnost enaka 1.

(5) Če sta $\mathcal{C}_1$ in $\mathcal{C}_2$ definirani s homogenima polinomoma $p_1(x,y,z)$ in $p_2(x,y,z)$ in je $\mathcal{C}_3$ definiran z
$$p_3 = p_1 p_2,$$
potem velja
$$I_A(\mathcal{C}_3,\mathcal{C}_4) = I_A(\mathcal{C}_1,\mathcal{C}_4) + I_A(\mathcal{C}_2,\mathcal{C}_4).$$

(6) Naj bosta krivulji $\mathcal{C}_1$in $\mathcal{C}_2$, podani s polinomoma $p(x,y,z)$ in $q(x,y,z)$ stopenj n in m, in krivulja $\mathcal{C}_3$ s polinomom $p(x,y,z)r(x,y,z)+q(x,y,z)$, kjer je $r(x,y,z)$ homogen polinom stopnje $m-n$. Tedaj velja
$$I_A(\mathcal{C}_1,\mathcal{C}_2) = I_A(\mathcal{C}_1,\mathcal{C}_3).$$

(7) Naj bosta krivulji $\mathcal{C}_1$ in $\mathcal{C}_2$, podani s polinomoma $p(x,y,z)$ in $q(x,y,z)$ brez skupne komponente in izberimo take projektivne koordinate, ki ustrezajo pogojem:
- Točka [1,0,0] ne pripada $\mathcal{C}_1 \cap \mathcal{C}_2$,
- Točka [1,0,0] ne leži na nobeni premici, ki vsebuje različni točki iz $\mathcal{C}_1 \cup \mathcal{C}_2$,
- Točka [1,0,0] ne leži na nobeni tangentni premici krivulj, ki se premice dotika v eni izmed točk $A \in \mathcal{C}_1 \cap \mathcal{C}_2$.

Potem je presečna večkratnost točke $[a,b,c]$, ki leži v $\mathcal{C}_1 \cap \mathcal{C}_2$, enaka kar največjemu pozitivnemu celemu številu k, za katerega velja
$$(bz - cy)^k \mid \mathcal{R}_{p,q}(y,z).$$

Kljub obsežni definiciji pa je pojem presečne večkratnosti definiran z namenom, da čim bolj preprosto in intuitivno pojasni presek med dvema algebraičnima krivuljama. Naštejmo par osnovnih primerov preseka premic ali algebraičnih krivulj. Generični presek dveh krivulj ali premic je enostaven in ima presečno večkratnost enako 1. Če je premica l tangentna na krivuljo $\mathcal{C}$, vendar točka preseka ni prevoj krivulje, je presečna večkratnost enaka 2. Če pa je premica l tangentna na prevojno točko krivulje, imata premica in krivulja v tej točki točka presečno večkratnost enako vsaj 3.

Sedaj predstavimo Bezout-jev izrek, ki nam prešteje, koliko točk se nahaja v preseku dveh projektivnih krivulj.

Izrek 3.8 (Bezout-jev izrek)**.** [6, Izrek 3.1] *Če sta $\mathcal{C}_1$ in $\mathcal{C}_2$ projektivni algebraični krivulji brez skupne komponente v $\mathcal{P}^2$, potem velja*

$$\sum_{A \in \mathcal{C}_1 \cap \mathcal{C}_2} \mathcal{I}_A(\mathcal{C}_1,\mathcal{C}_2) = mn,$$

kjer je $\operatorname{st} \mathcal{C}_1 = m$ *in* $\operatorname{st} \mathcal{C}_2 = n$.

Iz Bezout-jevega izreka sledi, da je v preseku dveh kubičnih krivulj brez skupne komponente bodisi 9 različnih točk s presečno večkratnostjo 1, ali pa manj točk z vsaj eno presečno večkratnostjo, strogo večjo od 1. Bistvena uporabnost Bezout-jevega izreka za nas je, da za drugo krivuljo vzamemo Hessejevo krivuljo prvotne krivulje. Presek algebraične krivulje s svojo Hessejevo krivuljo pa so ravno njeni prevoji. Tako vidimo, da je prevojev splošne kubične krivulje največ 9. V resnici se s primeri, ki imajo manj kot 9 prevojev, ne ukvarjamo preveč, saj so ti izolirani. Zelo redko namreč pride do situacije, da bi ravno v točki preseka dveh krivulj njuni tangenti sovpadali (kar je pogoj, da je presečna večkratnost vsaj 2).

Opomba 3.9. Nekateri izmed prevojev so tudi kompleksni. Za krivuljo z realnimi koeficienti so realni natanko trije prevoji. [3, str. 696]

Opomba 3.10. Za kubično krivuljo $\mathcal{C}$ v Weierstrassovi obliki velja, da je ena od njenih prevojnih točk točka [0,1,0]. Hitro se lahko prepričamo, da to drži: za Weierstrassovo krivuljo s polinomom

$$p(x,y,z) = -zy^2 + x^3 + axz^2 + bz^3$$

ter njeno Hessejevo krivuljo

$$h(x,y,z) = 8(3xy^2 + 3ax^2z + 9bxz^2 - a^2z^3)$$

dobimo

$$p(0,1,0) = 0,$$
$$h(0,1,0) = 0.$$

Ker je [0,1,0] točka na $\mathcal{C}$, ki leži tudi na $\mathcal{H}_\mathcal{C}$, je po definiciji 3.2 ena od prevojnih točk krivulje.

Preden dokažemo Bezout-jev izrek, navedimo milejši izrek.

Izrek 3.11. [6, Izrek 3.8] *Vsaki dve projektivni krivulji $\mathcal{C}_1$ in $\mathcal{C}_2$ v $\mathcal{P}^2$ se sekata v vsaj eni točki.*

Dokaz. Naj bosta krivulji $\mathcal{C}_1$ in $\mathcal{C}_2$, podani s homogenima polinomoma $p(x,y,z)$ in $q(x,y,z)$, stopenj m in n. Po definiciji rezultante vemo, da je njuna rezultanta bodisi homogen polinom stopnje mn ali pa enaka 0. Če je neničelna, po lemi 2.12 velja, da je rezltanta produkt mn linearnih faktorjev oblike $bz - cy$, kjer $b,c \in \mathbb{C}$ ter b in c nista hkrati enaka 0. V vsakem primeru torej obstaja točka (b_0,c_0) za katero velja

$$\mathcal{R}_{p,q}(b_0,c_0) = 0.$$

Ker je rezultanta polinomov $p(x,b_0,c_0)$ in $q(x,b_0,c_0)$ v eni spremenljivki, ki jih razvijemo po x enaka 0, imata polinoma $p(x,b_0,c_0)$ in $q(x,b_0,c_0)$ po točki a) leme 3.6 za eno spremenljivko nekonstantni skupni faktor in torej skupno ničlo $a_0 \in \mathbb{C}$. Potem velja

$$p(a_0,b_0,c_0) = q(a_0,b_0,c_0) = 0$$

in tako $[a_0,b_0,c_0] \in \mathcal{C}_1 \cap \mathcal{C}_2$. □

Dokaz Bezout-jevega izreka. [6, str. 54] Dokažimo najprej šibko verzijo izreka, ki pravi, da se projektivni krivulji $\mathcal{C}_1$ in $\mathcal{C}_2$ brez skupne komponente, ki ju podajata polinoma $p(x,y,z)$ in $q(x,y,z)$, sekata v največ mn točkah.

Recimo, da bi se krivulji sekali v vsaj $mn+1$ točkah. Dokazali bomo, da imata tedaj krivulji skupno komponento. Izberimo množico vseh različnih točk, v katerih se krivulji sekata in jo označimo z M. Potem izberimo točko, ki ne leži na nobeni od krivulj in na nobeni premici skozi različni točki iz M. Brez škode za splošnost lahko predpostavimo, da je ta točka [1,0,0].

Rezultanta $\mathcal{R}_{p,q}(y,z)$ pri razvoju polinomov po x je homogen polinom stopnje mn v spremenljivkah y in z. Če ni enaka 0, je produkt nm linearnih faktorjev oblike $bz-cy$, kjer b,c nista hkrati 0. Za vsaka taka b,c je $bz-cy$ faktor v rezultanti $\mathcal{R}_{p,q}(y,z)$ natanko tedaj, ko je rezultanta polinomov $p(x,b,c)$ in $q(x,b,c)$ enaka 0, tj.

$$\mathcal{R}_{p,q}(b,c)=0.$$

Po lemi 2.12 imata polinom $p(x,b,c)$ in $q(x,b,c)$ skupni faktor. Drugače povedano, obstaja neki $a\in\mathbb{C}$, da velja

$$p(a,b,c)=q(a,b,c)=0.$$

Zato je projektivna točka $[a,b,c]$ v preseku krivulj in tako v množici M, $by-cz$ pa eden izmed faktorjev rezultante. Ker točka [1,0,0] ni vsebovana v tej množici, mora veljati, da b,c nista hkrati enaka 0. Vzemimo še drug $[\alpha,\beta,\gamma]\in M$, različen od $[a,b,c]$.

Trdimo, da $\beta z-\gamma y$ ni skalarni večkratnik $bz-cy$. Če bi bil, bi vse tri točke $[a,b,c]$,$[\alpha,\beta,\gamma]$ in [1,0,0] ležale na premici, definirani z enačbo

$$bz=cy.$$

To pa bi bilo v protislovju s predpostavko, da [1,0,0] ne leži na premici, ki vsebuje dve točki iz M. Ker to velja za vsaki $[a,b,c]$,$[\alpha,\beta,\gamma]\in M$ je vseh $mn+1$ točk iz M med seboj linearno neodvisnih in nobena ni skalarni večkratnik druge.

Vsaki točki, ki je v množici M, je prirejen nek linearni faktor v rezultanti $\mathcal{R}_{p,q}(y,z)$. Iz tega sledi, da ima rezultanta $\mathcal{R}_{p,q}(y,z)$ vsaj $mn+1$ različnih linearnih faktorjev. Ker pa je rezultanta polinomov stopenj n in m bodisi polinom stopnje mn ali enaka 0, je potem edina možnost, da je rezultanta polinomov $p(x,y,z)$ in $q(x,y,z)$ identično enaka 0. Iz leme 3.6 potem vemo, da imata $p(x,y,z)$ in $q(x,y,z)$ skupen homogen linearni faktor in krivulji $\mathcal{C}_1$ in $\mathcal{C}_2$ skupno komponento, kar je v protislovju s predpostavko. Dokazali smo, da se krivulji lahko sekata v največ mn točkah.

Naj bosta sedaj $\mathcal{C}_1$ in $\mathcal{C}_2$ krivulji brez skupne komponente. Za močnejšo verzijo izreka moramo dokazati še, da je število točk v preseku krivulj $\mathcal{C}_1$ in $\mathcal{C}_2$ z upoštevanjem presečnih večkratnosti enako natanko mn.

Ker sta krivulji brez skupne komponente, po lemi 3.6 vemo, da rezultanta $\mathcal{R}_{p,q}(y,z)$ ni enaka 0. Torej jo kot homogen polinom lahko po lemi 2.12 izrazimo kot produkt linearnih faktorjev,

$$\mathcal{R}_{p,q}(y,z)=\prod_{i=1}^{k}(c_iz-b_iy)^{e_i}.$$

Koeficienti e_i so pozitivna cela števila in velja

$$e_1+\cdots+e_k=mn,$$

ter (b_i,c_i) ni skalarni večkratnik (b_j,c_j) za $i\neq j$. Na tem koraku se problema lotimo enako kot pri šibki obliki izreka. Za vsaka taka b_i,c_i iz rezultante velja $\mathcal{R}_{p,q}(b_i,c_i)=0$.

Torej imata polinoma $p(x,b_i,c_i)$ in $q(x,b_i,c_i)$ po lemi 3.6 skupni faktor, tj. obstaja tak $a_i \in \mathbb{C}$, da velja

$$p(a_i,b_i,c_i) = 0 = q(a_i,b_i,c_i).$$

To velja za vsak i iz produkta v rezultanti. Torej obstajajo take projektivne točke $A_i = [a_i,b_i,c_i]$, da je

$$\mathcal{C}_1 \cap \mathcal{C}_2 = \{A_i : 1 \leq i \leq k\},$$

in presečna večkratnost preseka krivulj v točki A_i je enaka

$$I_{A_i}(\mathcal{C}_1,\mathcal{C}_2) = e_i.$$

Skupno bo teh točk z upoštevanjem presečne večkratnosti natanko mn. □

Definirajmo sedaj pojem singularne točke na projektivni algebraični krivulji.

Definicija 3.12. [6, Definicija 2.27] Točka A na projektivni krivulji $\mathcal{C}$ v $\mathcal{P}^2$, podani s homogenim polinomom $p(x,y,z)$ je *singularna točka*, če velja

$$\frac{\partial p}{\partial x}(A) = \frac{\partial p}{\partial y}(A) = \frac{\partial p}{\partial z}(A) = 0.$$

Če to za točko A to ne velja, rečemo, da je A *nesingularna* ali *gladka* točka na krivulji. Če krivulja ne vsebuje nobene singularne točke, rečemo, da je *nesingularna* ali *gladka*.

Definicija 3.13. Naj bo $\mathcal{C}$ nerazcepna krivulja in naj za gladko točko A na krivulji velja $A \in \mathcal{H}_\mathcal{C}$. Točka A je *enostaven prevoj*, če velja $I_A(\mathcal{C},\mathcal{H}_\mathcal{C}) = 1$.

Druga ekvivalentna definicija prevoja je povezana s presečno večkratnostjo v točki krivulje pri preseku s tangento na krivuljo.

Izrek 3.14 (Eulerjeva Formula)**.** [1, Odlomek 3.6] *Naj bo $p(x,y,z)$ homogen polinom stopnje n s koeficienti iz $\mathbb{C}$. Potem velja*

$$x\frac{\partial p(x,y,z)}{\partial x} + y\frac{\partial p(x,y,z)}{\partial y} + z\frac{\partial p(x,y,z)}{\partial z} = np(x,y,z).$$

Dokaz. Eulerjevo formulo lahko preprosto preverimo tako, da v formulo vstavimo nek splošen homogen polinom. Naj bo $x^{k_1}y^{k_2}z^{k_3}$ homogen člen v polinomu $p(x,y,z)$ stopnje n, torej velja $k_1+k_2+k_3 = n$. Če člen vstavimo v levo stran enačbe, dobimo

$$x(k_1x^{k_1-1}y^{k_2}z^{k_3}) + y(k_2x^{k_1}y^{k_2-1}z^{k_3}) + z(k_3x^{k_1}y^{k_2}z^{k_3-1}) =$$

$$= (k_1+k_2+k_3)x^{k_1}y^{k_2}z^{k_3} = nx^{k_1}y^{k_2}z^{k_3}$$

Tako vidimo, da je za poljuben homogen člen v polinomu $p(x,y,z)$ ta formula veljavna. Ker je polinom vsota takih členov, pa je formula posledično veljavna za celoten polinom. □

Trditev 3.15. [1] *Naj bo $\mathcal{C}$ algebraična krivulja in $p(x,y,z)$ njen minimalni polinom. Za točko A na krivulji velja:*

- *Krivulja $\mathcal{C}$ je gladka v točki A natanko tedaj, ko velja*

$$grad_A p := \left(\frac{\partial p}{\partial x}(A),\frac{\partial p}{\partial y}(A),\frac{\partial p}{\partial z}(A)\right) \neq 0.$$

- *Če je $\mathcal{C}$ gladka v točki A, potem je* projektivna tangenta $T_A\mathcal{C}$ *v tej točki podana z linearno enačbo*

$$x\frac{\partial p}{\partial x}(A) + y\frac{\partial p}{\partial y}(A) + z\frac{\partial p}{\partial z}(A) = 0.$$

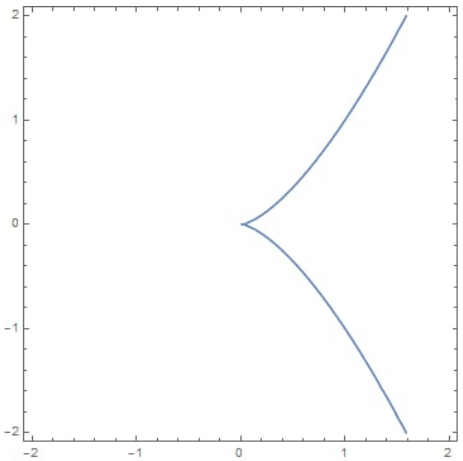
Opomba 3.16. Za tangento na krivuljo v vsaki gladki točki A velja

$$I_A(\mathcal{C},T_A\mathcal{C}) \geq 2.$$

Definicija 3.17. Gladka točka $A \in \mathcal{C}$ je prevoj, če $I_A(\mathcal{C},T_A\mathcal{C}) \geq 3$.

V primeru enačaja je A *enostavni prevoj*. Tangenti v prevojni točki rečemo *prevojna tangenta*.

Vidimo, da se v singularnih točkah zaradi ničelnih prvih odvodov zatakne pri določanju tangente, saj je enačba tangente v prazno izpolnjena. Primer singularne točke bi bila točka, ki leži v preseku dveh premic razcepne krivulje. Premici, ki sta kandidatki za tangenti v tej točki bi bili ravno obe premici ki gresta skozi njo, pa vendar mora biti tangenta enolično določena, kar pa očitno v tej točki ne moremo storiti. Singularnost je možno lepo razbrati iz Weierstrassove oblike kubike, če ustrezno izberemo ravnino, v kateri jo opazujemo. Za kubiki na slikah 11 in 12 dobimo singularnost v točki [0,0,1]. Opazimo, da v teh točkah tangente na krivuljo res ni možno določiti.



SLIKA 11. Kubična krivulja, podana s polinomom $p(x,y,z) = y^2z - x^3$ in prikazana v ravnini $z = 1$.

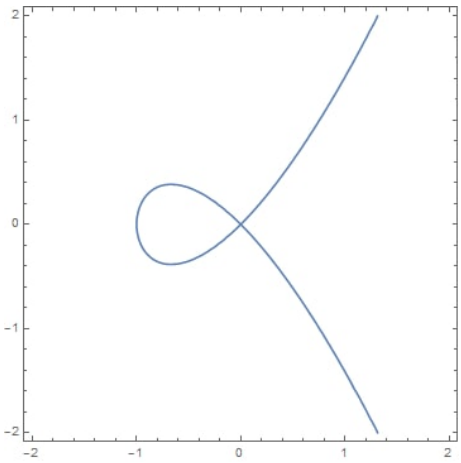
Za konec poglavja si poglejmo še primer kubične krivulje z enostavno simetrično enačbo.

Primer 3.18. *Fermatova kubika* je gladka kubika, definirana kot množica ničel polinoma

$$p(x,y,z) = x^3 + y^3 + z^3.$$

Izračunajmo njeno Hessejevo krivuljo:

$$h(x,y,z) = \det\begin{pmatrix} \frac{\partial^2 p}{\partial x^2} & \frac{\partial^2 p}{\partial x \partial y} & \frac{\partial^2 p}{\partial x \partial z} \\ \frac{\partial^2 p}{\partial y \partial x} & \frac{\partial^2 p}{\partial y^2} & \frac{\partial^2 p}{\partial y \partial z} \\ \frac{\partial^2 p}{\partial z \partial x} & \frac{\partial^2 p}{\partial z \partial y} & \frac{\partial^2 p}{\partial z^2} \end{pmatrix} = det\begin{pmatrix} 6x & 0 & 0 \\ 0 & 6y & 0 \\ 0 & 0 & 6z \end{pmatrix} = 6^3xyz.$$



SLIKA 12. Kubična krivulja, podana s polinomom $p(x,y,z) = y^2z - x^2(x+1)$ in prikazana v ravnini $z = 1$.

Enostavnost obeh krivulj nam omogoča izračun prevojnih točk. Ker mora za prevoj veljati

$$xyz = 0,$$

postavimo eno od spremenljivk na 0. Naj bo

$$x = 0.$$

To vstavimo v formulo prvotne krivulje in dobimo

$$y^3 + z^3 = 0.$$

V afini ravnini $y = 1$ dobimo enačbo

$$1 + z^3 = 0,$$

ki nam vrne rešitve

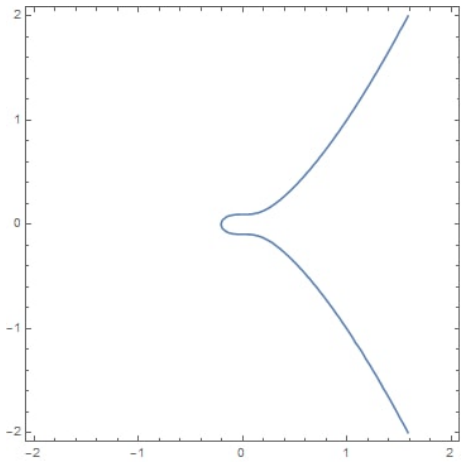
$$\begin{aligned} z_1 &= -1, \\ z_2 &= -e^{2/3\pi i}, \\ z_3 &= -e^{4/3\pi i}. \end{aligned}$$

Uspelo nam je izračunati tri prevojne točke:

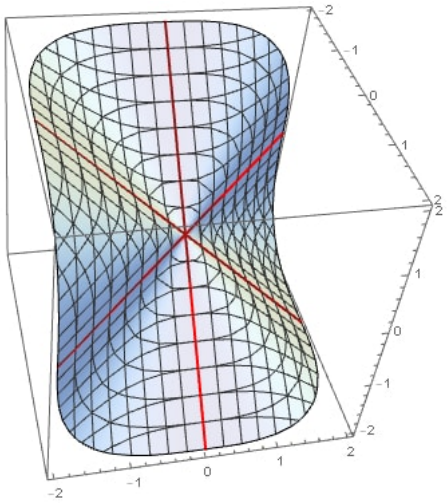
$$\begin{aligned} A_1 &= [0,1,-1], \\ A_2 &= [0,1,-e^{2/3\pi i}], \\ A_3 &= [0,1,-e^{4/3\pi i}]. \end{aligned}$$

Zaradi simetrije spremenljivk x,y,z z njihovo menjavo analogno pridemo do ostalih 6 prevojev:

$$\begin{aligned} A_4 &= [1,-1,0], \\ A_5 &= [1,-e^{2/3\pi i},0], \\ A_6 &= [1,-e^{4/3\pi i},0], \\ A_7 &= [-1,0,1], \\ A_8 &= [-e^{2/3\pi i},0,1], \\ A_9 &= [-e^{4/3\pi i},0,1]. \end{aligned}$$



Slika 13. Fermatova kubika v Weierstrassovi obliki v ravnini $z = 1$.



Slika 14. Fermatova kubika in njeni trije realni prevoji.

Izračunajmo še rezultanto polinomov $p(x,y,z)$ in $h(x,y,z)$ pri razvoju po x:

$$R_{\mathcal{C}}(y,z) = \begin{Bmatrix} y^3+z^3 & 0 & 0 & 1 \\ 0 & 6^3yz & 0 & 0 \\ 0 & 0 & 6^3yz & 0 \\ 0 & 0 & 0 & 6^3yz \end{Bmatrix} = 6^9y^3z^3(y^3+z^3)$$

Vidimo, da je v vseh izračunanih prevojih rezultanta krivulje enaka 0.

Poskusimo še obratno: na podlagi izračunane rezultante izračunajmo enega od prevojev. Potreben pogoj zanj je, da je rezultanta enaka 0, torej bo eden od treh elementov produkta moral biti enak 0. Predpostavimo, da je $y^3 = 0$, ter opazujmo krivuljo v $z = 1$. Pogoj za x dobimo tako, da $[x,0,1]$ vstavimo v prvotno enačbo krivulje, in dobimo

$$x^3 = -1.$$

Tako dobimo zadnje tri rešitve, ostale pa izračunamo analogno iz drugih faktorjev rezultante.

Pri zahtevnejših krivuljah seveda tako preprost izračun prevojev ni mogoč. Zato se moramo tam poslužiti drugačnih metod. ♢

4. Abelova grupa na kubičnih krivuljah

Naslednja tema je zelo zanimiva algebraična lastnost kubičnih krivulj: na točkah krivulje lahko uvedemo strukturo grupe. Abelova grupa na kubikah je uporabna v kriptografiji, za nas pa bo prav tako bistvenega pomena, saj ta struktura grupe igra pomembno vlogo pri izračunu prevojev.

Definicija 4.1. Naj bo $\mathcal{C}$ gladka kubika. Na $\mathcal{C}$ definiramo operacijo

$$\begin{array}{rccc} * : & \mathcal{C} \times \mathcal{C} & \to & \mathcal{C} \\ & A \times B & \mapsto & C \end{array},$$

kjer je $C = A * B$ tretja točka v preseku premice skozi točki $A, B \in \mathcal{C}$ in krivulje $\mathcal{C}$. Če velja $A = B$, tedaj za premico vzamemo tangento na $\mathcal{C}$ v tej točki.

Opomba 4.2. Po Bezout-jevem izreku iz prejšnjega poglavja vemo, da se premica l in kubična krivulja $\mathcal{C}$ sekata v natanko

$$\operatorname{st} l * \operatorname{st} \mathcal{C} = 3$$

točkah (z upoštevanjem presečnih večkratnosti). Zato bo operacija dobro definirana za vsaki dve točki A,B na krivulji.

Ta operacija je sicer zgolj pomožna operacija, s pomočjo katere bomo definirali aditivno operacijo na gladki kubiki.

Trditev 4.3. *Lastnosti operacije $*$ so:*

(1) *Komutativnost* $A * B = B * A$;
(2) *Absorpcija* $(A * B) * A = B$;
(3) $((A * B) * C) * D = A * ((B * D) * C)$.

Dokaz.
(1) Točka $C = A * B$ je tretja točka v preseku premice, ki gre skozi A in B, s kubično krivuljo $\mathcal{C}$. To pa je hkrati tudi točka $C = B * A$, saj je druga premica skozi točki B in A enaka prejšnji.
(2) Očitno velja $(A * B) * A = C * A = B$, kjer je C tretja točka v preseku premice skozi A in B in krivulje $\mathcal{C}$.
(3) Za ta dokaz bi potrebovali Izrek o devetih točkah, ki ga v tem besedilu ne bomo omenjali. Dokaz je tehničen in za nas ni bistven, zato ga bomo izpustili.

□

Sedaj izberimo in fiksirajmo neko točko na krivulji, in jo označimo z O.

Definicija 4.4. Naj bo $\mathcal{C}$ gladka kubika v $\mathcal{P}^2$ in $O \in \mathcal{C}$ izbrana točka. Potem na $\mathcal{C}$ definiramo linearno operacijo

$$\begin{array}{rccc} + : & \mathcal{C} \times \mathcal{C} & \to & \mathcal{C} \\ & A \times B & \mapsto & C, \end{array}$$

kjer je

$$C = A + B = (A * B) * O.$$

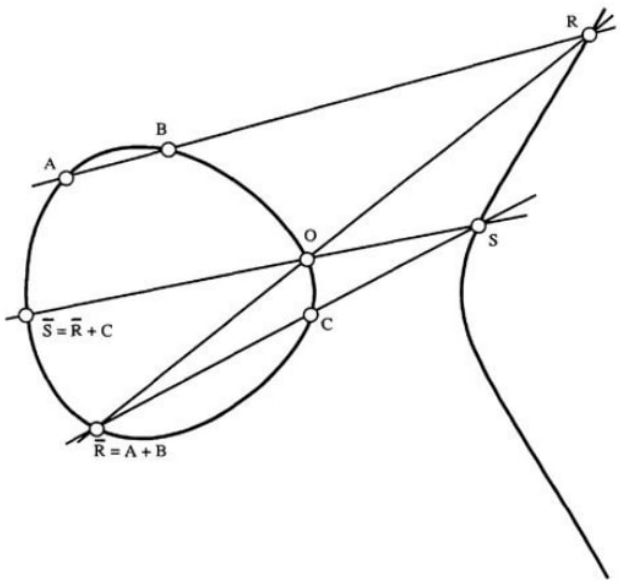
Izrek 4.5. *Naj bo $\mathcal{C}$ gladka kubika v $\mathcal{P}^2$ in $O \in \mathcal{C}$ izbrana točka. Potem je $(\mathcal{C},+)$ Abelova grupa. Pri tem je O nevtralni element, nasprotni element elementa A pa je enak $-A = A * (O * O)$.*

Dokaz. Preverimo, da veljajo vse lastnosti Abelove grupe:

(1) Komutativnost: $A + B = (A * B) * O = (B * A) * O = B + A$;

(2) Element O je nevtralni element: $A + O = (A * O) * O = (O * A) * O = A$;
(3) Element $-A$ je nasprotni element: $A + (-A) = A + (A * (O * O)) = A * (A * (O * O)) * O = (O * O) * O = O$;
(4) Asociativnost: $(A + B) + C = ((A * B) * O) + C = (((A * B) * O) * C) * O = (A * ((B * C) * O)) * O = (A * (B + C)) * O = A + (B + C)$.

Dokazali smo, da je ($\mathcal{C}$,+) Abelova grupa. □



Slika 15. Abelova grupa na Weierstrassovi kubiki.[7, str. 34]

Pogosto v povezavi s strukturo grupe naletimo tudi na pojem *eliptična krivulja*, ki označuje dvojico $(\mathcal{C}, O)$, kjer je $\mathcal{C}$ kubična krivulja v Weierstrassovi obliki skupaj z izbrano točko O.

Izkaže se, da nam različne izbire točke O na isti krivulji določajo izomorfne grupe.

Izrek 4.6. *Na kubiki $\mathcal{C}$ naj bosta definirani grupa G_1 = ($\mathcal{C}$,+) z nevtralnim elementom O_1 in grupa G_2 = ($\mathcal{C}$,+) z nevtralnim elementom O_2. Potem je preslikava*

$$\begin{array}{rccc} \theta: & G_1 & \to & G_2 \\ & A & \mapsto & A * (O_1 * O_2) \end{array}$$

izomorfizem grup.

Dokaz. Označimo

$$Q = O_1 * O_2,$$
$$\theta(A) = A * Q.$$

Preslikava θ je injektivna:

$$\theta(A) = \theta(B),$$
$$A * Q = B * Q,$$
$$(A * Q) * Q = (B * Q) * Q.$$

Iz lastnosti absorpcije sledi

$$A = B.$$

Preslikava θ je surjektivna:

$$A \in \mathcal{C}$$

$$\theta(A * Q) = (A * Q) * Q = (Q * A) * Q = A.$$

Preslikava θ je homomorfizem:

$$\theta(A + B) = (A + B) * Q = ((A * B) * O_1) * Q,$$

$$\theta(A) + \theta(B) = (A * Q) + (B * Q) = ((A * Q) * (B * Q)) * O_2 =$$

$$= A*((Q*O_2)*(B*Q)) = A*(O_1*(B*Q)) = A*((B*Q)*O_1) = ((A*B)*O_1)*Q.$$

Vsi vmesni koraki sledijo iz lasnosti operacije *. Sledi

$$\theta(A + B) = \theta(A) + \theta(B).$$

Dokazali smo, da je preslikava θ izomorfizem grup. □

Še posebej lep primer grupe pa dobimo, če za točko O izberemo enega od prevojev kubične krivulje. Tedaj ima aditivna operacija na točkah kubične krivulje še nekaj dodatnih lastnosti.

Lema 4.7. *Naj bo $\mathcal{C}$ gladka kubika in O njen prevoj. Potem velja:*

(1) $A + B + C = O \iff A,B,C$ *so kolinearne;*
(2) $A \neq O$ *je točka reda 2 (*$2A = O$*)* $\iff$ *tangenta v A gre skozi O;*
(3) $A \neq O$ *je točka reda 3 (*$3A = O$*)* $\iff$ *A je prevoj.*

Dokaz. (1) Predpostavimo, da velja

$$A + B + C = O.$$

Potem je

$$A + B = -C,$$

$$(A * B) * O = C * (O * O).$$

Točka $(O * O)$ je točka v preseku krivulje in tangente na O; ker pa je O prevoj, je presečna večkratnost tangente v točki O enaka vsaj 3. Zato velja $(O * O) = O$.

$$(A * B) * O = C * O,$$

$$A * B = C.$$

Iz tega sledi, da so A,B in C kolinearne.

(2) Izračunajmo

$$2A = O,$$

$$A + A = (A * A) * O = O.$$

Naj bo $B = A * A$. Potem je B točka z lastnostjo, da če skozi B in O potegnemo premico, je tretja točka v preseku s krivuljo kar O. Torej je ta premica tangenta na O. Ker pa je O prevoj, ima tangenta v tej točki presečno večkratnost enako tri, zato je edina možnost, da je $B = O$. Torej velja

$$A * A = O,$$

oziroma, tretja točka preseka tangente na krivuljo v točki A je točka O.

(3) Za točko A reda 3 velja

$$3A = O,$$
$$A + A = -A,$$
$$(A * A) * O = A * (O * O).$$

Po ugotovitvi iz točke (1) dobimo

$$(A * A) * O = A * O,$$
$$A * A = A.$$

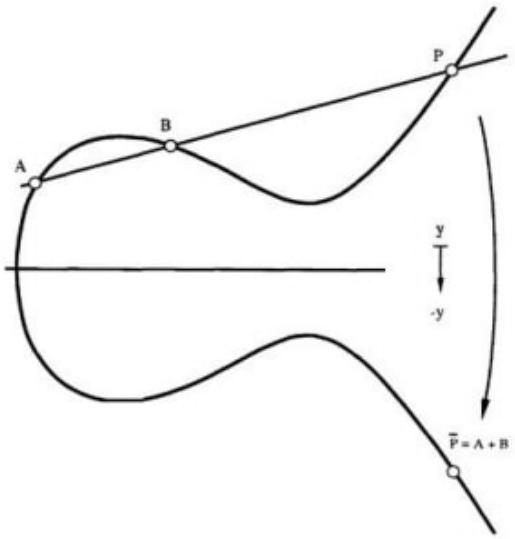
Iščemo torej točko A z lastnostjo, da je tretja točka v preseku tangente v točki A in krivulje same kar sama točka A. To pa velja natanko takrat, ko je presečna večkratnost v tej točki enaka 3, kar je natanko takrat, ko je A prevoj.

□

Aditivno grupo še poenostavimo, če opazujemo kubično krivuljo v Weierstrassovi obliki v ravnini $z = 1$. Za nevtralni element O grupe izberemo njeno prevojno točko [0,1,0], ki je za ravnino $z = 1$ točka v neskončnosti. To grupo si podrobnejše oglejmo.

Iz enačbe Weierstrassove kubike vidimo, da je ta simetrična preko abscisne osi, saj je $y^2 = (-y)^2$. Za vsako točko A predpišemo njeno inverzno točko $-A$ kar z zrcaljenjem čez x-os. Za $A = O$ pa naj bo $-A = O$.

Točko $A + B$ torej določimo tako, da najprej vzamemo tretjo točko v preseku krivulje s premico skozi točki A in B, potem pa slednjo prezrcalimo čez x-os. To je prikazano tudi na sliki 16.



Slika 16. Vsota točk A in B na kubični krivulji v Weierstrassovi obliki, kjer za O vzamemo prevojno točko [0,1,0] [7, str. 39].

Če bi bila ena od točk A,B prevojna točka O (privzemimo $B = O$), bi potem veljalo $A + O = A = O + A$, saj je O nevtralni element. Če sta si A in B simetrični pri čez x-os, bo $A + B = O$. Če pa vzamemo $A = B$, bo premica tangenta na krivuljo v točki A. V večini primerov bo tangenta sekala krivuljo v neki tretji točki (katere zrcalno nasprotna točka bo potem $A + A$). Če pa je A slučajno prevoj, je tudi tretja točka A in bo veljalo $A + A = -A$.

Abelova grupa na kubični krivulji, kot smo jo predstavili, nam bo v pomoč v naslednjih poglavjih.

5. Hessejeva konfiguracija

V tem razdelku bomo kubične krivulje predstavili kot kvocientni prostor mreže v kompleksni ravnini. Namen razdelka je vzpostavitev povezav med kubično krivuljo in njeno Abelovo grupo ter med njej ekvivalentnimi strukturami v topologiji in kompleksni analizi. Rezultat teh povezav, Hessejeva konfiguracija, nam bo omogočila, da bomo lahko dokazali rešljivost problema eksplicitnega izračuna prevojev. Dokaze večine izrekov in trditev iz tega razdelka bomo izpustili, saj bi nas ponesli predaleč stran od teme in bistva diplomskega dela. Podrobnejšo razlago in dokaze lahko najdemo v [6, poglavje 5.1].

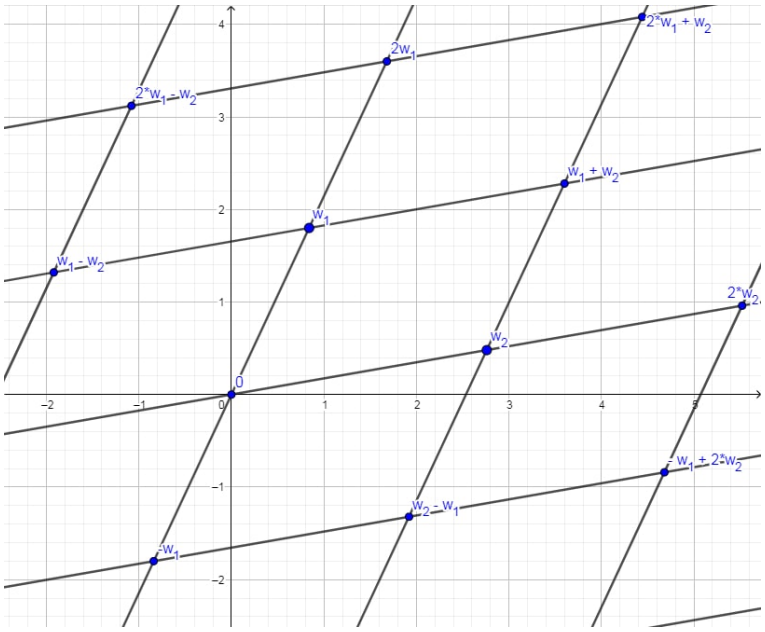
Definicija 5.1. Naj bosta w_1 in w_2 neničelni kompleksni števili, linearno neodvisni nad $\mathbb{R}$. To pomeni, da njun kvocient $\frac{w_1}{w_2}$ ni realno število.

Naj bo

$$\Lambda = \{nw_1 + mw_2; n,m \in \mathbb{Z}\}.$$

Množico Λ imenujemo *mreža* na kompleksni ravnini $\mathbb{C}$.

Mreža Λ je grupa za seštevanje, izomorfna $\mathbb{Z}^2$, hkrati pa tudi podgrupa aditivne grupe $\mathbb{C}$.



Slika 17. Mreža $\Lambda = \{nw_1 + mw_2; n,m \in \mathbb{Z}\}$. Prikazi mreže v tem poglavju ter trojic premic v poglavju 7 so izrisani s programom GeoGebra

Ker je $\mathbb{C}$ Abelova grupa za seštevanje, je vsaka njena podgrupa edinka. Ker je zato mreža Λ njena edinka, lahko definiramo kvocientno grupo.

Definicija 5.2. Če obravnavamo Λ kot podgrupo edinko v $\mathbb{C}$, lahko definiramo kvocientno grupo

$$\mathbb{C}/\Lambda = \{a + \Lambda; a \in \mathbb{C}\}.$$

V tej grupi sta dve množici $a + \Lambda$ in $b + \Lambda$ za a,$b \in \mathbb{C}$ enaki natanko tedaj, ko velja $a - b \in \Lambda$.

Poglejmo si lastnosti te grupe. Najprej uvedimo na njej topologijo, inducirano s standardno topologijo na $\mathbb{C}$.

Definicija 5.3. Naj bo

$$\begin{array}{rccc} \pi: & \mathbb{C} & \to & \mathbb{C}/\Lambda \\ & a & \mapsto & a + \Lambda \end{array}$$

surjektivna preslikava kompleksne ravnine. Potem je $U \in \mathbb{C}/\Lambda$ odprta v kvocientni topologiji na $\mathbb{C}/\Lambda$ natanko takrat, ko je njena praslika $\pi^{-1}(U)$ odprta v $\mathbb{C}$.

Naslednji lemi podajmo brez dokaza, saj gre za splošno znani dejstvi iz topologije.

Lema 5.4. *Podmnožica v $\mathbb{C}^n$ ali $\mathbb{R}^n$ je kompaktna natanko takrat, ko je zaprta in omejena.*

Lema 5.5. *Naj bo $f : X \to Y$ zvezna preslikava med topološkima prostoroma. Če je X kompakten prostor, je tudi slika $f(X)$ kompaktna.*

Naj bo množica

$$P = \{sw_1 + tw_2 : s,t \in [0,1]\}$$

zaprt paralelogram v kompleksni ravnini, določen s kompleksnima številoma w_1 in w_2.

Trditev 5.6. *Množica $\mathbb{C}/\Lambda$ je kompaktna v kvocientni topologiji.*

Dokaz. Paralelogram P je zaprta in omejena podmnožica $\mathbb{C}$, zato je kompaktna. Hkrati pa velja

$$\pi(P) = \mathbb{C}/\Lambda.$$

Slika tega paralelograma je torej kar cel prostor $\mathbb{C}/\Lambda$. Ker je π zvezna preslikava, zvezna slika kompaktnega prostora pa je kompaktna, je tudi $\mathbb{C}/\Lambda$ kompaktna. □

Izkaže se, da je kvocient $\mathbb{C}/\Lambda$ topološki torus.

V kompleksni ravnini $\mathbb{C}$ si $\mathbb{C}/\Lambda$ lahko predstavljamo kot en sam paralelogram (katerega ogljišča so v mreži) z lastnostjo: če paralelogram zapustimo na desnem robu, se na levem zvezno vrnemo vanj. Prav tako se iz zgornjega roba vrnemo na spodnji rob. Torus pa lahko identificiramo z zgoraj omenjenim paralelogramom P, ki mu zlepimo nasprotne robove; naprej levega in desnega, kar nam da neke vrste valj, z lepljenjem zgornjega in spodnjega roba pa dobimo torus. Identifikacija je prikazana na sliki 18.

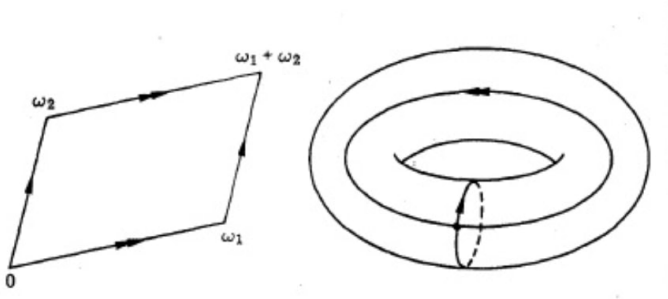
Trditev 5.7. [6, Trditev 5.10] *Na $\mathbb{C}$ obstaja meromorfna funkcija*

$$\wp(z) = z^{-2} + \sum_{w \in \Lambda - \{0\}} ((z - w)^{-2} - w^{-2})$$

z odvodom

$$\wp'(z) = (-2)z^{-3} + \sum_{w \in \Lambda} (-2)(z - w)^{-3}.$$

Opomba 5.8. Da je ta funkcija dobro definirana, je potrebno pokazati, da obe vrsti konvergirata; dokaz trditve in konvergence vrst najdemo v [6, str. 115].



SLIKA 18. Prikaz preoblikovanja paralelograma v kompleksni ravnini v torus [6, str. 122].

Definicija 5.9. [6, Definicija 5.12] Funkcijo $\wp(z)$ v odvisnosti od mreže Λ imenujemo *Weierstrassova $\wp$-funkcija.*

Weierstrassova $\wp$-funkcija ima naslednje lastnosti:

(1) Za vsaka $z \in \mathbb{C}$ in $\eta \in \Lambda$ velja $\wp(-z) = \wp(z) = \wp(z+\eta)$;
(2) Funcija je dvojno periodična in meromorfna [6, Dokaz, str. 117];
(3) Za funkcijo velja enačba

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

kjer sta

$$g_2 = g_2(\Lambda) = 60 \sum_{w\in\Lambda-\{0\}} w^{-4}$$

in

$$g_3 = g_3(\Lambda) = 140 \sum_{w\in\Lambda-\{0\}} w^{-6}.$$

Definicija 5.10. [6, Definicija 5.19] Naj bo $\mathcal{C}_\Lambda$ projektivna krivulja v $\mathcal{P}^2$, definirana s polinomom

$$q_\Lambda(x,y,z) = y^2z - 4x^3 + g_2xz^2 + g_3z^3,$$

kjer sta $g_2 = g_2(\Lambda)$ in $g_3 = g_3(\Lambda)$ definirani kot v prejšnji lemi.

Definicija 5.11. [6, str. 122] Obstaja dobro definirana preslikava

$$\begin{array}{rccc} u: & \mathbb{C}/\Lambda & \to & \mathcal{C}_\Lambda \\ & z+\Lambda & \mapsto & \begin{cases} [\wp(z),\wp'(z),1] & \text{če z} \notin \Lambda; \\ [0,1,0] & \text{če z} \in \Lambda. \end{cases} \end{array}$$

Trditev 5.12. [6, Trditev 5.22] *Preslikava $u : \mathbb{C}/\Lambda \to \mathcal{C}_\Lambda$ je homeomorfizem.*

Pojasnimo, kaj smo izvedeli iz zadnjih treh definicij in trditve. Če si ogledamo polinom krivulje $\mathcal{C}_\Lambda$ hitro ugotovimo, da je oblika krivulje zelo podobna polinomu krivulje v Weiestrassovi obliki. Od nje jo loči zgolj še koeficient 4 pred x^3. Če želimo $\mathcal{C}_\Lambda$ pretvoriti v Weierstrassovo obliko, polinom $q_\Lambda(x,y,z)$ s preprosto projektivnostjo ϕ preslikamo v polinom $p(x,y,z) = y^2z - x^3 + g_2xz^2 + g_3z^3$. Preslikava ϕ je skrčitev po spremenljivki x:

$$\phi : q_\Lambda(x,y,z) \to q_\Lambda(\frac{x}{4^{\frac{1}{3}}},y,z),$$

kjer dobimo

$$\phi(q_\Lambda(x,y,z)) = y^2z - x^3 + g_2xz^2 + g_3z^3.$$

Koeficienta a,b v dobljeni Weierstrassovi kubiki pa bosta izražena kot $a = -g_2$, $b = -g_1$.

Kubično krivuljo $q_\Lambda(x,y,z)$ smo definirali, ker preslikava u tvori direkten homeomorfizem iz kvocienta $\mathbb{C}/\Lambda$ na $\mathcal{C}_\Lambda$. Kljub temu, da ni Weierstrassova, nas od te loči le preprosta projektivnost in krivulji imata enake lastnosti. Prav tako pa že od prej vemo, da je kvocient $\mathbb{C}/\Lambda$ torus. Vse skupaj nam da ekvivalenco med tremi geometrijskimi objekti:

(1) Kvocient $\mathbb{C}/\Lambda$;
(2) Kompleksni torus;
(3) Kubična krivulja v $\mathcal{P}^2(\mathbb{C})$.

Vzemimo neko mrežo Λ. S to mrežo je natanko določen kvocient $\mathbb{C}/\Lambda$, ki ga s homeomorfizmom u slikamo v točno določeno kubiko v Weierstrassovi obliki. Kompleksna koeficienta a in b sta natanko določena z izborom mreže oziroma kompleksnih števil w_1 in w_2. Obratno pa tudi vsaki krivulji v Weierstrassovi obliki pripada neka mreža, torej določeni kompleksni števili w_1 in w_2.

Tudi za vsako krivuljo, podano v splošni polinomski obliki, velja enako. Po trditvi 2.16 namreč lahko vsako kubično krivuljo s projektivnostmi pretvorimo v Weierstrassovo obliko. Vse krivulje, ki imajo pri pretvorbi v Weierstrassovo obliko enaka koeficienta a in b, so si projektivno ekvivalentne.

Vendar pa preslikava u ne ohranja zgolj topoloških lastnosti. Tako kompleksni torus $\mathbb{C}/\Lambda$ kot nesingularno kubično krivuljo $\mathcal{C}_\Lambda$ lahko obravnavamo kot kompleksen prostor, ki mu rečemo *Riemmanova ploskev*. Če tako množici vzamemo za Riemmanovi ploskvi, ima homeomorfizem u še dodatno lastnost.

Izrek 5.13. [6, Trditev 5.43] *Homomorfizem $u : \mathbb{C}/\Lambda \to \mathcal{C}_\Lambda$ je holomorfen. Prav tako je holomorfizem njegov inverz*

$$u^{-1} : \mathcal{C}_\Lambda \to \mathbb{C}/\Lambda.$$

Tega izreka v nadaljevanju ne bomo potrebovali. Pa vendar smo dobili občutek, da preslikava u ne ohranja zgolj topoloških lastnosti, ampak mnogo več kot to: pri preslikavi se ohrani tudi sama struktura množice, zato morata imeti $\mathbb{C}/\Lambda$ in $\mathcal{C}_\Lambda$ več skupnih lastnosti.

Z razumevanjem, da obstaja holomorfna preslikava med $\mathbb{C}/\Lambda$ in neko kubiko $\mathcal{C}_\Lambda$ bomo poskušali povezati tudi njuni Abelovi grupi. Na kubični krivulji je to že opisana grupa $(\mathcal{C},+)$, na mreži pa imamo seveda kvocientno aditivno grupo $\mathbb{C}/\Lambda$.

Trditev 5.14. [11] *Naj bo $\mathcal{C}_\Lambda$ gladka kubika v $\mathcal{P}^2$ in izberimo enega izmed prevojev za točko $O \in \mathcal{C}_\Lambda$. Tedaj so prevojne točke na $\mathcal{C}_\Lambda$ natanko reda 1 ali 3 v grupi $(\mathcal{C}_\Lambda, +)$.*

Opomba 5.15. Kljub temu, da za primerjavo s kvocientom $\mathbb{C}/\Lambda$ uporabljamo kubiko $\mathcal{C}_\Lambda$, pa je rezultat veljaven tudi za projektivno ekvivalentno Weierstrassovo kubiko, in posledično po izreku 2.16 za vsako nerazcepno kubično krivuljo.

Opomba 5.16. Velja še več. Edine točke na $\mathcal{C}_\Lambda$, ki so v tej grupi reda 1 ali 3, so kar prevoji krivulje $\mathcal{C}_\Lambda$.

Vemo, da je na kubični krivulji 9 prevojev. Eden je nevtralni element grupe z redom 1, ostalih 8 prevojev pa je reda 3. Za začetek lahko poskušamo ugibati, ali so točke reda 1 in 3 na kubiki v kakšni korespondenci z točkami v aditivni grupi $\mathbb{C}/\Lambda$, ki so reda 1 ali 3. Oglejmo si kvocient in preštejmo, koliko takih točk obstaja tam:

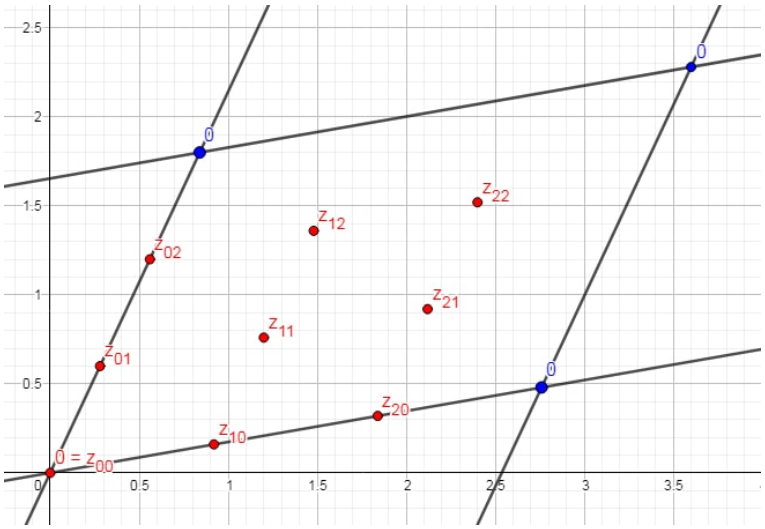
(1) točke reda 1: dobimo zgolj eno točko v kvocientni grupi, in to je

$$z_{00} = (0,0) + \Lambda;$$

(2) točke reda 3: v tej skupini so natanko točke oblike

$$z_{jk} = \frac{j}{3}w_1 + \frac{k}{3}w_2 + \Lambda,$$

kjer $k,j \in \{0,1,2\}$ in k,j nista hkrati enaka 0. Takih točk je 8.



Slika 19. Točke reda 1 in 3 v grupi $\mathbb{C}/\Lambda$.

Skupaj je teh točk ravno 9; natanko toliko, kot je prevojnih točk na kubični krivulji, šteto po Bezout-jevem izreku. Hkrati pa opazimo, da tudi redi točk pri obeh grupnih operacijah sovpadajo.

Na $\mathbb{C}/\Lambda$ množica točk reda 1 in 3 tvori Abelovo grupo $G_{\mathbb{C}/\Lambda}$ z enoto z_{00}, ki je hkrati Abelova podgrupa kvocientne aditivne grupe na $\mathbb{C}/\Lambda$. Ta grupa moči $|G_{\mathbb{C}/\Lambda}| = 9$ ima tudi sledečo lastnost: lahko jo uredimo v 3×3 tabelo na tak način, da se trije elementi v vsaki vrstici, stolpcu ali po diagonalah seštejejo v $0 + \Lambda$. Če to povemo v formalnem jeziku, je grupa izomorfna kartezičnemu produktu dveh cikličnih grup celih števil po modulu 3, grupi $\mathbb{Z}_3^2$.

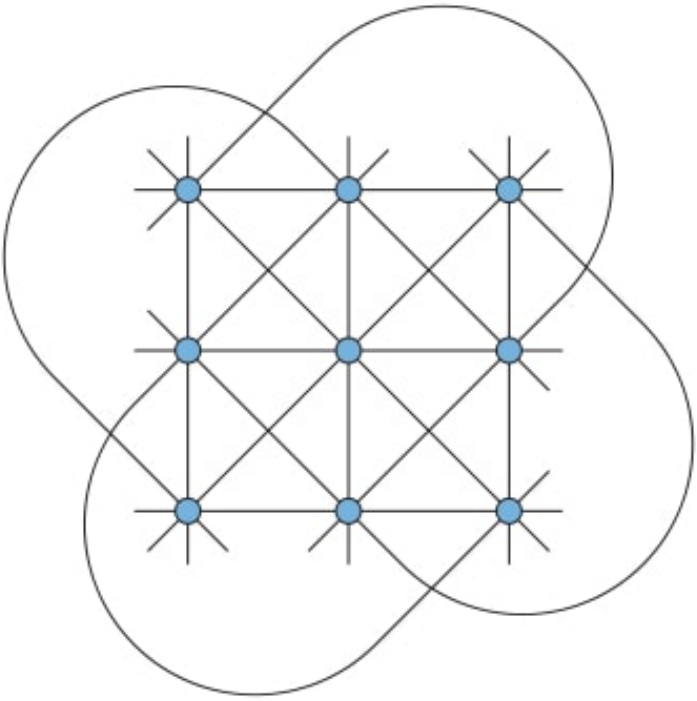
Množico vseh prevojnih točk na kubični krivulji $\mathcal{C}_\Lambda$ označimo z S.

Trditev 5.17. *Preslikava u je izomorfizem grup $G_{\mathbb{C}/\Lambda}$ in $(S,+)$.*

Trditve ne bomo dokazovali, saj ne poznamo dovolj podrobnih lastnosti preslikave u. Vendar pa si poglejmo, do kakšnih sklepov lahko na podlagi te trditve pridemo.

Ker je u izomorfizem grup, se mora pri preslikavi celotna struktura grupe $G_{\mathbb{C}/\Lambda}$ ohraniti. Ker je $G_{\mathbb{C}/\Lambda}$ izomorfna $\mathbb{Z}_3^2$, more biti po trditvi tudi Abelova grupa $(S,+)$ izomorfna $\mathbb{Z}_3^2$. Prevojne točke projektivne kubične krivulje zato lahko uredimo v 3×3 tabelo na tak način, da tri točke v kateremkoli stolpcu, vrstici ali na diagonali ležijo na isti premici v $\mathcal{P}^2$, ter je njihova vsota enaka O. Velja tudi, da premica v $\mathcal{P}^2$, ki gre skozi dva prevoja, vedno seka krivuljo še v tretjem prevoju. Tako strukturo 9 prevojev kubične krivulje in 12 premic, ki potekajo skozi te prevoje, imenujemo *Hessejeva konfiguracija*.

Kot smo že omenili, bo ravno obstoj Hessejeve konfiguracije prevojev omogočil, da jih bomo lahko tudi eksplicitno izračunali.



Slika 20. Hessejeva konfiguracija [12].

6. Galoisove grupe

Vprašanje, ali je mogoče za splošno kubično krivuljo eksplicitno izračunati njene prevoje, razdelajmo še malo bolj natančno. Kar nas v resnici zanima, je: ali je za splošno kubično krivuljo, podano s homogenim polinomom

$$p(x,y,z) = \sum_{i=0}^{3} \sum_{j=0}^{3-i} a_{ij} x^i y^j z^{3-i-j}$$

možno eksplicitno izračunati prevoje kot funkcije koeficientov a_{ij}, če na koeficientih lahko uporabljamo le osnovne algebraične operacije – množenje, deljenje, seštevanje, odštevanje, potenciranje in korenjenje. Na to vprašanje nam elegantno odgovori področje algebre, znano kot *Galoisova teorija*. Začetnik tega področja je francoski matematik Evariste Galois, ki mu je uspelo problem izračuna ničel polinoma n-te stopnje v odvisnosti od njegovih koeficientov pretvoriti na ekvivaleten problem, ali ima polinomu prirejena grupa določene lasnosti.

Prvotna motivacija za razvoj Galoisove teorije je bilo vprašanje: zakaj za splošen polinom stopnje 5 v eni spremenljivki ne obstaja eksplicitna formula za izračun njegovih ničel kot funkcij koeficientov in uporabo osnovnih algebraičnih operacij? Tudi za splošen polinom stopnje, večje od 5, velja enako; za tiste s stopnjo 4 ali manj pa je bilo že v Galoisovem času dokazano, da eksplicitne formule obstajajo.

Vzemimo nek polinom $f(x)$ stopnje n z vodilnim koeficientom 1, torej polinom oblike

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Če bi poznali njegove ničle, bi lahko iz osnovnih operacij na teh ničlah izpeljali določene algebraične enačbe. Pri koeficientih teh enačb se omejimo na neko polje.

Kljub temu, da naravno lahko vzamemo katerokoli polje, bo v našem primeru to vedno polje $\mathbb{Q}$. Tako gledamo zgolj enačbe med ničlami polinoma, ki imajo racionalne koeficiente.

Ideja Galoisove teorije je, da poiščemo take permutacije ničel polinoma, da bodo vse izpeljane enačbe po permutaciji ničel še vedno izpolnjene. Na prvi pogled se zdi, da bo takih permutacij zelo malo, pa vendar imajo polinomi poleg racionalnih tudi realne in kompleksne ničle, ki nam dajo bistveno manj enačb z racionalnimi koeficienti, manj enačbam pa bo zadoščalo več permutacij. Prav tako pa konjugirane pare kompleksnih števil vedno lahko permutiramo, brez da bi enačbe izgubile veljavnost. Permutacije, ki jih lahko izvedemo, da ohranimo veljavnost enačb, tvorijo grupo.

Zgoraj smo predpostavili, da ničle polinoma poznamo, in lahko iz njih sestavimo enačbe. Kaj pa, če poznamo enačbe med ničlami, samih ničel pa ne? Videli bomo, da lahko z Galoisovo teorijo na podlagi teh enačb že določimo, ali se bo ničle sploh dalo izraziti s koeficienti polinoma.

Definicija 6.1. Naj bo polje E razširitev polja F. *Avtomorfizem ϕ razširitve E/F* je avtomorfizem polja E, ki fiksira F; tj. avtomorfizem ϕ, pri katerem za vsak $x \in F$ velja

$$\phi(x) = x.$$

Množico vseh takih avtomorfizmov označimo z $Aut(E/F)$, to pa je grupa za komponiranje funkcij.

To definicijo sedaj uporabimo na primeru polinomov in njihovih ničel. Naj bo F polje, iz katerega jemljemo koeficiente polinoma. Polje E pa naj bo razširitev izbranega polja z ničlami polinoma $f(x)$. Množica ϕ bo tedaj množica vseh takih avtomorfizmov, ki fiksirajo polje F ter permutirajo ničle polinoma. Te ničle so generatorji razširitve E/F.

Vsakemu avtomofizmu iz $Aut(E/F)$ je enolično prirejena permutacija na ničlah polinoma. Množica permutacij, ki so prirejene vsem ustreznim avtomorfizmom, pa vsebuje ravno tiste permutacije, ki ohranjajo enačbe z racionalnimi koeficienti, ki veljajo na ničlah polinoma. Ti avtomorfizmi in permutacije so si izomorfni.

Definicija 6.2. Razširitev E/F je *Galoisova razširitev*, če je razširitev algebraična ter množica avtomorfizmov $Aut(E/F)$ fiksira množico F.

Definicija 6.3. Če je E/F Galoisova razširitev, potem grupo $Aut(E/F)$ imenujemo *Galoisova grupa* ter jo označimo z $Gal(E/F)$.

Za boljše razumevanje obravnavajmo še primer.

Primer 6.4 (prirejeno po [13])**.** Naj bo $f(x) = x^4 - 16x^2 + 4 = (x^2 - 8)^2 - 60$. Želeli bi opisati Galoisovo grupo ničel polinoma $f(x)$. Koeficienti polinoma so iz polja $\mathbb{Q}$. Njegove ničle so

$$x_1 = \sqrt{3} + \sqrt{5},$$
$$x_2 = \sqrt{3} - \sqrt{5},$$
$$x_3 = -\sqrt{3} + \sqrt{5},$$
$$x_4 = -\sqrt{3} - \sqrt{5}.$$

Ničle zadoščajo sledečim 6 enačbam z racionalnimi koeficienti

$$x_1 x_2 = -2,$$
$$x_1 x_3 = 2,$$

$$x_1 + x_4 = 0,$$
$$x_2 + x_3 = 0,$$
$$x_2 x_4 = 2,$$
$$x_3 x_4 = -2.$$

Polje koeficientov polinoma je $\mathbb{Q}$, razširjeno polje pa polje

$$\mathbb{Q}(x_1,x_2,x_3,x_4,x_5,x_6) = \mathbb{Q}(\sqrt{3},\sqrt{5}).$$

Poiskati moramo še avtomorfizme razširitve $\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}$. Ničle polinoma bi lahko permutirali na $|S_4| = 4! = 24$ načinov; vendar pa vse permutacije ne ohranjajo enačb, ki jih te ničle izpolnjujejo. Če preverimo ustreznost vseh permutacij, nam ostanejo samo 4 ustrezne. To so:

$$\delta_1 : (x_1,x_2,x_3,x_4) \to (x_1,x_2,x_3,x_4),$$
$$\delta_2 : (x_1,x_2,x_3,x_4) \to (x_2,x_1,x_4,x_3),$$
$$\delta_3 : (x_1,x_2,x_3,x_4) \to (x_3,x_4,x_1,x_2),$$
$$\delta_4 : (x_1,x_2,x_3,x_4) \to (x_4,x_3,x_2,x_1).$$

Štirje avtomorfizmi, izomorfni zgornjim permutacijam, tvorijo Galoisovo grupo polinoma $f(x)$. To so avtomorfizmi:

$$\phi_1(a + b\sqrt{3} + c\sqrt{5}) = a + b\sqrt{3} + c\sqrt{5},$$
$$\phi_2(a + b\sqrt{3} + c\sqrt{5}) = a + b\sqrt{3} - c\sqrt{5},$$
$$\phi_3(a + b\sqrt{3} + c\sqrt{5}) = a - b\sqrt{3} + c\sqrt{5},$$
$$\phi_4(a + b\sqrt{3} + c\sqrt{5}) = a - b\sqrt{3} - c\sqrt{5}.$$

Galoisova grupa polinoma $Gal(\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q})$ je izomorfna grupi $\mathbb{Z}_2^2$. ♢

Sedaj si poglejmo pojem rešljivosti grupe in nekaj izrekov ter trditev, ki so povezane s tem pojmom. Že poimenovanje rešljiva grupe nakazuje na povezavo s problemom iskanja ničel polinomov – rešljivosti polinomske enačbe. Kot bomo videli formula za ničle namreč obstaja natanko tedaj, ko je Galoisova grupa ničel polinoma rešljiva.

Definicija 6.5. [4, Definicija 6.9] Grupa G je *enostavna*, če ne vsebuje nobene netrivialne edinke.

Definicija 6.6. [4, Definicija 8.1 in definicija 8.3] *Kompozicijska vrsta* grupe G do podgrupe N je zaporedje podgrup

$$G = G_0 > G_1 > G_2 > \cdots > G_{n-1} > G_n = N,$$

kjer velja $G_{k+1} \triangleleft G_k$ in so vse G_k/G_{k+1} enostavne.

Definicija 6.7. [4, Definicija 8.3 izrek 8.5] Grupa G je *rešljiva*, če obstaja taka kompozicijska vrsta

$$G = G_0 > G_1 > G_2 > \cdots > G_{n-1} > G_n = \{e\},$$

da je vsak faktor G_k/G_{k+1} Abelova grupa.

Trditev 6.8. *Vsaka podgrupa rešljive grupe je rešljiva.*

Poglejmo si še nekaj primerov rešljivih grup.

Primer 6.9. Pokažimo rešljivost cikličnih grup $\mathbb{Z}_2$ in $\mathbb{Z}_3$, grupe simetrične permutacij treh elementov S_3 in alternirajoče grupe vseh sodih permutacij štirih elementov A_4.

Ciklična grupa $\mathbb{Z}_2$ nima nobene netrivialne edinke (je enostavna), zato je edina možna kompozicijska vrsta

$$\mathbb{Z}_2 > \{0\}.$$

Kvocientna grupa $\mathbb{Z}_2/\{0\} = \mathbb{Z}_2$ je enostavna in abelova, zato je grupa $\mathbb{Z}_2$ rešljiva. Dokaz za grupo $\mathbb{Z}_3$ je analogen.

Simetrična grupa S_3 ni enostavna. Edina edinka, ki jo vsebuje, je alternirajoča grupa A_3. Grupa A_3 netrivialnih edink nima, zato zaporedje grup lahko konstruiramo zgolj na sledeč način:

$$S_3 > A_3 > \{id\}.$$

Poglejmo si sedaj obe kvocientni grupi. Da bo zaporedje grup kompozicijsko zaporedje, morata biti obe kvocientni grupi enostavni. Da pa bo grupa S_3 rešljiva, pa morata biti obe kvocientni grupi Abelovi. Prva grupa je

$$S_3/A_3 = \{\sigma A_3, \sigma \in S_3\},$$

kjer je

$$\sigma A_3 = \begin{cases} \sigma A_3, \sigma \notin A_3, \\ A_3, \sigma \in A_3. \end{cases}$$

Ta grupa vsebuje le dve elementa, A_3 ter σA_3, kjer je σ neka liha permutacija. Tako je ta grupa izomorfna grupi $\mathbb{Z}_2$.

Grupa

$$A_3/\{id\} \cong A_3 = (\{id, \sigma = (12)(23), \sigma^2 = (23)(12)\}, \circ)$$

pa je izomorfna grupi $\mathbb{Z}_3$. Ker sta kvocientni grupi enostavni in Abelovi, je grupa S_3 rešljiva.

Tudi alternirajoča grupa A_4 sama ni Abelova. Pri njej bo kompozicijsko zaporedje

$$A_4 > \{id,(12)(34),(13)(24),(14)(23)\} > \{id,(12)(34)\} > \{id\}.$$

Preverimo, kakšni so kvocienti;

$$A_4/\{id,(12)(34),(13)(24),(14)(23)\} \cong \mathbb{Z}_2,$$
$$\{id,(12)(34),(13)(24),(14)(23)\}/\{id,(12)(34)\} \cong \mathbb{Z}_2,$$
$$\{id,(12)(34)\}/\{id\} \cong \mathbb{Z}_2.$$

Ker so kvocientne grupe enostavne in Abelove, zopet dobimo ustrezno kompozicijsko zaporedje. Grupa A_4 je zato rešljiva.

Znano je, da je grupa A_4 je v resnici kar največja rešljiva alternirajoča podgrupa, saj A_5 ni rešljiva. Grupa S_3 pa je najmanjša rešljiva grupa, ki ni Abelova. ♢

Podajmo še par izrekov, ki jih bomo potrebovali pri dokazu rešljivosti grupe v naslednjem poglavju.

Izrek 6.10 (2. izrek E. Noether)**.** [8, izrek 5.17] *Če sta $N \subseteq H$ podgrupi edinki grupe G, potem velja $G/H \cong (G/N)/(H/N)$.*

Lema 6.11. *Predpostavimo, da velja $N \triangleleft G$. Naj bo H taka podgrupa grupe G, ki vsebuje N. Za vsako tako podgrupo obstaja preslikava*

$$H \to H/N,$$

ki ohranja red in preslika podgrupe grupe G, ki vsebujejo N v podgrupe G/N.

Po izreku 6.10 velja, da se kompozicijska vrsta

$$G = G_0 > G_1 > G_2 > \cdots > G_n = N$$

preslika v vrsto

$$G/N = G_0/N > G_1/N > G_2/N > \cdots > G_n/N = N/N = \{id\}.$$

Faktorji G_i/G_{i+1} so izomorfni faktorjem $(G_i/N)/(G_{i+1}/N)$.

Trditev 6.12. [8, Izrek 12.9] *Naj bo $N \triangleleft G$. Če sta grupi N in G/N rešljivi, potem je rešljiva tudi grupa G.*

Dokaz. Ker je G/N rešljiva, poznamo njeno kompozicijsko zaporedje Abelovih grup G/N do id. Te z izomorfizmom iz leme 6.11 prevedemo v kompozicijsko vrsto G do N, od N naprej pa vrsto nadaljujemo z faktorji iz kompozicijske vrste N, saj vemo, da je grupa N rešljiva in taka vrsta obstaja. Vrsta, sestavljena iz obeh omenjenih vrst, je kompozicijska vrsta G do $\{e\}$ in grupa G je rešljiva. □

Izrek 6.13 (Osnovni izrek o izomorfizmu)**.** [4, Trditev 5.7] *Če je $\phi : G \to H$ homomorfizem grup, potem ϕ inducira izomorfizem grup*

$$G/\ker(\phi) \cong \operatorname{im}\phi.$$

V naslednjem poglavju bomo Galoisovo teorijo uporabili, da tvorimo Galoisovo grupo prevojev kubične krivulje.

7. Rešljivost problema

Vse ugotovitve v tem poglavju so povzete po Harrisovem članku [3], ki je bistven vir za ta diplomski seminar. V uvodu v članek si avtor postavi sledeče vprašanje: ali je možno iz koeficientov polinoma projektivne kubične krivulje natanko določiti, kje na krivulji se prevojne točke nahajajo, oziroma, ali obstaja specifična formula prevojev v odvisnosti od koeficientov?

Naj bo $\mathcal{C}$ kubična krivulja, podana s homogenim polinomom $p(x,y,z)$. Polinom njene Hessejeve krivulje označimo s $h(x,y,z)$. Naj bo $S = \{S_k; k \in \{1,2,...,9\}\}$ množica prevojev $\mathcal{C}$. Vsak prevoj S_k določajo projektivne koordinate $[x_k,y_k,z_k]$.

Polinoma $p(x,y,z)$ in $h(x,y,z)$ sedaj pod pogoji opombe 3.5 razvijmo po eni od spremenljivk, recimo y. Potem izračunamo rezultanto $R_{p,h}(x,z)$ obeh polinomov, ki je polinom v odvisnosti od x in z. Ker pa smo v projektivnem prostoru, lahko krivulji opazujemo v določeni afini ravnini in tako fiksiramo eno od spremenljivk. Naj bo to ravnina $z = 1$. Rezultanta je potem polinom $R_{p,h}(x,1)$, ki je stopnje 9 v spremenljivki x.

Trditev 7.1. *Naj bo $\mathcal{C}$ kubična krivulja, podana s polinomom $p(x,y,z)$ in $h(x,y,z)$ polinom njene Hessejeve krivulje. Polinoma razvijemo po spremenljivki y in izračunamo njuno rezultanto $R_{p,h}(x,z)$. Naj bo $x_k \in \mathbb{C}$ število, za katerega velja*

$$R_{p,h}(x_k,1) = 0.$$

Tedaj obstaja tak y_k, da je $S_k = [x_k,y_k,1]$ eden od prevojev kubične krivulje $\mathcal{C}$.

Dokaz. Iz enačbe

$$R_{p,h}(x_k,1) = 0.$$

po a) točki leme 3.6 sledi, da imata polinoma $p(x_k,y,1)$ ter $h(x_k,y,1)$ nekonstantni skupni faktor. Če fiksiramo koordinati x,z polinomov $p(x,y,z)$ in $h(x,y,z)$ kot $z = 1$ in $x = x_k$, sta to namreč polinoma v spremenljivki y, ki imata rezultanto enako 0.

Torej imata skupno ničlo. Drugače povedano, obstaja nek tak y_k, za katerega točka $[x_k,y_k,1]$ izpolnjuje pogoja

$$p(x_k,y_k,1) = 0$$
$$h(x_k,y_k,1) = 0,$$

torej leži na obeh krivuljah in je prevoj $\mathcal{C}$.

Ugotovili smo torej, da vsaki od ničel x_k polinoma $R_{p,h}(x,1)$ stopnje 9 v x pripada nek y_k (lahko jih je tudi več, če imajo prevoji enake x-koordinate) in dobljene točke $[x_k,y_k,1]$ so prevoji krivulje $\mathcal{C}$.

□

Za izračun prevojev torej želimo poiskati ničle polinoma $R_{p,h}(x,1)$. Za splošen polinom 9. stopnje velja, da njegovih ničel v odvisnosti od koeficientov ni možno izračunati. Pokazali pa bomo, da je polinom $R_{p,h}(x,1)$ poseben. To, kar vemo o njem, bomo zdaj prevedli v jezik Galoisove teorije.

Polje koeficientov polinoma $R_{p,h}(x,1)$ želimo razširiti z njegovimi ničlami in določiti njegovo Galoisovo grupo. Najprej omenimo, da so koeficienti polinoma $h(x,y,z)$ preko izračuna determinante Hessejeve matrike odvisni od koeficientov a_{ij} polinoma $p(x,y,z)$. Prav tako pa so tudi koeficienti rezultante $R_{p,h}(x,1)$ posredno odvisni od koeficientov a_{ij} v $p(x,y,z)$, rezultanta je namreč funkcija koeficientov $p(x,y,z)$ in $h(x,y,z)$. To lahko povemo tudi drugače: koeficienti rezultante so elementi *polja* $\mathbb{C}(a_{ij})$ *racionalnih funkcij* desetih kompleksnih koeficientov a_{ij}. Naša rezultanta bo torej oblike

$$R_{p,h}(x,1) = \sum_{k=0}^{9} f_k(a_{ij})x^k$$

za neke racionalne funkcije $f_k(a_{ij})$.

Polje koeficientov rezultante, ki ga želimo razširiti, je torej polje $\mathbb{C}(a_{ij})$. To polje razširimo na polje $\mathbb{C}(a_{ij}, x_k)$ za vse $k \in \{1,2,...,9\}$ in tiste i,j, ki določajo koeficiente polinoma $p(x,y,z)$. Polje $\mathbb{C}(a_{ij}, x_k)$ pa je polje racionalnih funkcij v koeficientih polinoma in x-koordinatah prevojev. Razširitev $\mathbb{C}(a_{ij}, x_k)/\mathbb{C}(a_{ij})$ je končna algebraična razširitev.

Sedaj naravno pridemo do naslednje trditve.

Trditev 7.2. [3, str. 686] *Formula za koordinate x_k prevojev S_k za $k \in \{1,2,\ldots,9\}$ v odvisnosti od koeficientov a_{ij} polinoma $p(x,y,z)$ obstaja natanko tedaj, ko je Galoisova grupa $Gal(\mathbb{C}(a_{ij}, x_k)/\mathbb{C}(a_{ij}))$ rešljiva.*

Če torej dokažemo rešljivost grupe $Gal(\mathbb{C}(a_{ij}, x_k)/\mathbb{C}(a_{ij}))$, se bomo prepričali, da prevoje lahko eksplicitno izrazimo v odvisnosti od koeficientov. *Galoisova grupa prevojev kubične krivulje*, ki jo označimo z $Gal(\mathbb{C}(a_{ij}, x_k)/\mathbb{C}(a_{ij}))$ je grupa avtomorfizmov, ki fiksirajo racionalne funkcije iz $\mathbb{C}(a_{ij})$.

Ker se izkaže, da je Galoisova grupa prevojev v tem primeru težko izračunljiva, se avtor članka [3] problema loti tako, da izkoristi izomorfnost Galoisovih grup prevojev in tako imenovanih *monodromijskih grup* [3, str. 689]. S slednjimi se mi ne bomo ukvarjali, saj je za njihovo razumevanje potrebno poglobljeno znanje drugih področij matematike. Prav tako pa avtor v članku dokaže izomorfnost monodromijske grupe in *afine specialne linearne grupe* $ASL_2(\mathbb{Z}_3)$ [3, str. 694]. Zato si bomo ogledali samo slednjo grupo.

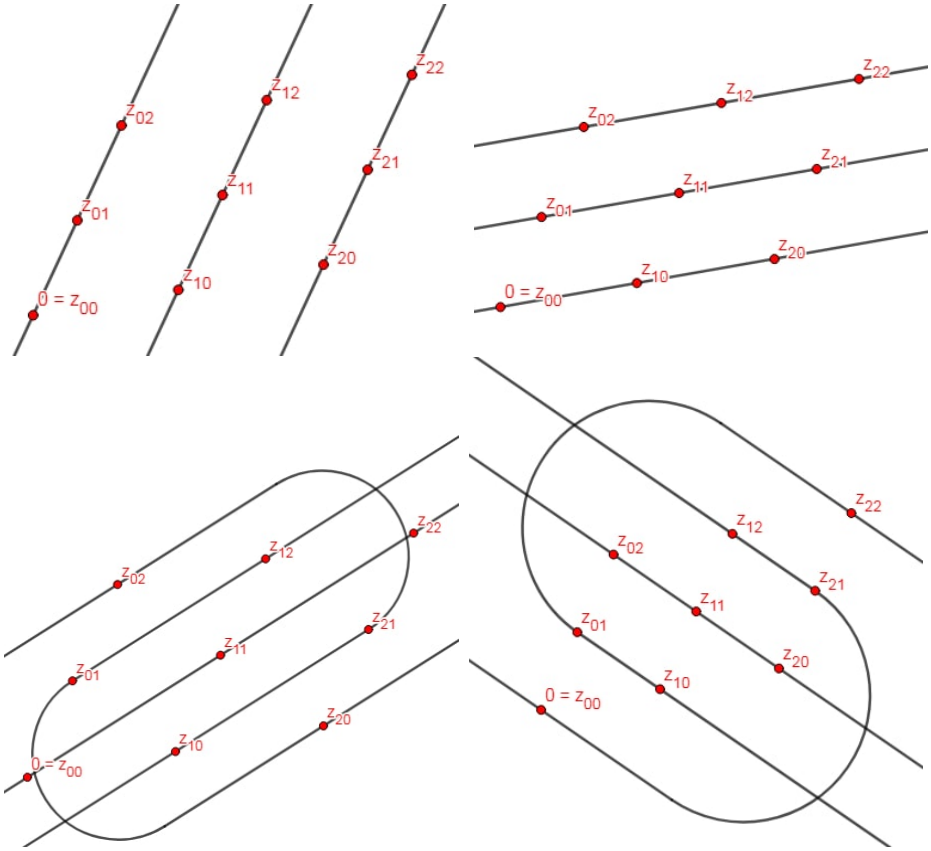
Grupa $ASL_2(\mathbb{Z}_3)$ je podgrupa obrnljivih afinih transformacij na $\mathbb{Z}_3$. Generirata jo dve vrsti elementov:

- Translacije dvodimenzionalnega vektorskega prostora nad poljem $\mathbb{Z}_3$ za nek vektor v.
- Elementi splošne linearne grupe $SL_2(\mathbb{Z}_3)$. To so vse linearne transformacije dvodimenzionalnega vektorskega prostora nad poljem $\mathbb{Z}_3$, ki jih lahko zapišemo kot 2×2 matrike s koeficienti $\mathbb{Z}_3$ in determinanto 1.

Ker je Galoisova grupa razširitve $Gal(\mathbb{C}(a_{ij}, x_k)/\mathbb{C}(a_{ij}))$ izomorfna grupi $ASL_2(\mathbb{Z}_3)$, je problem rešljivosti grupe $Gal(\mathbb{C}(a_{ij}, x_k)/\mathbb{C}(a_{ij}))$ ekvivalenten problemu rešljivosti grupe $ASL_2(\mathbb{Z}_3)$.

Trditev 7.3. *Grupa $ASL_2(\mathbb{Z}_3)$ je rešljiva.*

Dokaz. Spomnimo se, da prostor $\mathbb{Z}_3^2$ opisuje strukturo Hessejeve konfiguracije devetih prevojev kubične krivulje. Definirajmo $V = \mathbb{Z}_3^2$ kot dvodimenzionalni vektorski podprostor nad obsegom $\mathbb{Z}_3$. Vsaka premica, ki gre skozi tri točke prostora V ima še dve vzporednici, ki gresta vsaka skozi tri druge točke, skupaj pa tri premice pokrijejo celoten prostor V. Po definiciji 2.13 je projektivni prostor $\mathcal{P}(V)$ vektorskega prostora V množica vseh njegovih enorazsežnih vektorskih podprostorov. Točke $\mathcal{P}(V)$ so torej kar premice vektorskega prostora V. Ta vsebuje 4 trojice vzporednih premic. Vsaka od teh trojic nam bo dala zgolj eno točko v $\mathcal{P}(V)$, saj sta tisti dve premici, ki nista vektorska podprostora, zgolj translaciji prve. Zato celoten prostor $\mathcal{P}(V)$ vsebuje le 4 točke. Na sliki 21 si te točke lahko ogledamo.



Slika 21. Točke prostora $\mathcal{P}(V)$, ki jih predstavljajo štiri trojice vzporednih premic.

Izkaže se, da translacije prostora V za poljuben vektor $v = (v_1,v_2) \in \mathbb{Z}_3^2$ ohranijo $\mathcal{P}(V)$. Translacija bo namreč vsako točko $\mathcal{P}(V)$ preslikala nazaj vase. Drugače

povedano, translacija povzroči zamenjavo točk prostora V, vendar se premice v vsaki posamezni trojici, tj. točki $\mathcal{P}(V)$ med seboj le permutirajo. Za lažjo predstavo si lahko zopet pomagamo s sliko 21. Tudi involucija $-I$ na V ima enak učinek in povzroči zgolj permutacijo premic. Pri involuciji je sicer to malce manj očitno, pa vendar s kratkim izračunom delovanja na točkah hitro vidimo, da to drži.

Sedaj definirajmo homomorfizem grup

$$\varphi_1 : ASL_2(\mathbb{Z}_3) \to S_4,$$

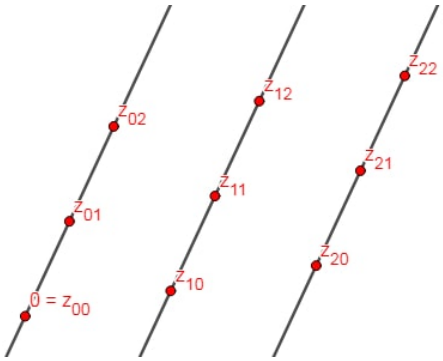
kjer je S_4 simetrična grupa vseh permutacij 4 elementov. Vsakemu elementu grupe $ASL_2(\mathbb{Z}_3)$ s tem homomorfizmom priredimo ustrezno permutacijo točk iz $P(V)$. Homomorfizem množico translacij in involucijo $-I$ preslika v identiteto, saj te fiksirajo vse trojice premic. Zato je jedro $G_1 = \ker(\varphi_1)$ generirano s translacijami in involucijo. Slika $\operatorname{im}\varphi_1$ pa je kar alternirajoča grupa A_4 sodih permutacij, saj nobena preslikava v $ASL_2(\mathbb{Z}_3)$ ne inducira lihe permutacije med trojicami premic. Očitno obstajajo zgolj preslikave, ki trojice premic ohranijo, ter take, ki na trojicah inducirajo permutacijo, ki je produkt dveh disjunktnih ciklov.

Jedro G_1 homomorfizma φ_1 je podgrupa edinka grupe $ASL_2(\mathbb{Z}_3)$, po izreku 6.13 pa velja

$$ASL_2(\mathbb{Z}_3)/G_1 \cong A_4.$$

Uporabimo lahko še izrek 6.12 iz prejšnjega poglavja. Če dokažemo, da sta tako jedro homomorfizma $\ker\varphi_1$ kot tudi njegova slika $\operatorname{im}\varphi_1$ rešljivi, potem je tudi sama grupa $ASL_2(\mathbb{Z}_3)$ rešljiva.

Kot smo že omenili, je slika preslikave enaka A_4, to pa je rešljiva grupa, kar smo dokazali v prejšnjem poglavju. Tudi jedro G_1 je rešljiva grupa. To dokažimo tako, da tvorimo nov homomorfizem φ_2, ki bo vsakemu elementu iz G_1 priredil njegovo delovanje na točno določeni trojici premic. Brez škode za splošnost lahko vzamemo trojico na sliki 22, premice zaporedno iz leve strani označimo z l_1,l_2 in l_3.



Slika 22. Preslikava φ_2 opazuje permutacijo premic pri delovanju preslikav iz jedra G_1.

Vemo, da bo vsaka afina transformacija iz G_1 trojico premic preslikala v enako trojico, vendar bo φ_2 vsaki taki transformaciji priredil permutacijo teh treh premic. Dobimo surjekcijo

$$\varphi_2 : G_1 \to S_3.$$

Njeno jedro je $G_2 \cong \mathbb{Z}_3$. Edine afine transformacije, ki premic ne permutirajo, so identiteta ter dve translaciji vzdolž premic (v primeru 22 sta to translaciji (0,1) ter (0,2)). Te tri preslikave tvorijo ciklično grupo $\mathbb{Z}_3$ s praštevilskim redom, ki je rešljiva. Slika te preslikave pa je kar S_3, saj je generirana z involucijo (na primeru 22 bo to

$(l_2 l_3)$), ki permutira dve premici, ter vsemi možnimi translacijami, ki generirajo vse cikle dolžine 3 v S_3. V prejšnjem poglavju smo dokazali, da je S_3 rešljiva grupa.

Ker sta jedro G_2 in slika S_3 preslikave φ_2 rešljivi, je rešljiva tudi sama grupa G_1. Ker pa sta jedro G_1 in slika A_4 preslikave φ_1 rešljivi, je rešljiva tudi $ASL_2(\mathbb{Z}_3)$ in dokaz je končan. □

Podajmo še nekaj dodatnih pojasnil, zakaj je tak rezultat smiselen. Rezultanta, ki smo jo opazovali, je bila polinom 9. stopnje v x. Ničle splošnega polinoma 9. stopnje med seboj niso povezane - če bi želeli poiskati Galoisovo grupo avtomorfizmov takega polinoma, ne bi imeli za avtomorfizme nobenega pogoja v obliki enačb, ki bi jih ničle morale izpolnjevati. Zato jih lahko poljubno permutiramo in Galoisova grupa avtomorfizmov polinoma 9. stopnje bo enaka S_9. Ta grupa pa ni rešljiva.

Vendar pa v našem primeru obstajajo določene relacije med ničlami našega polinoma – rezultante $R_{p,h}(x,1)$. To je natanko sistem Hessejeve konfiguracije. Tudi po permutaciji ničel morajo te še vedno ostati v takem sistemu; vsaka ničla mora biti vsota 4 parov drugih ničel (tistih, s katerimi leži na skupni premici). To pa je dovolj močen pogoj, da niso vse permutacije iz S_9 ustrezne. Ustrezne so natanko tiste permutacije, ki ležijo v Galoisovi grupi, izomorfni $ASL_2(\mathbb{Z}_3)$, to so namreč edine permutacije, ki Hessejevo konfiguracijo ohranjajo. Ker pa smo dokazali, da je ta grupa rešljiva, je tudi naš problem rešljiv. S tem smo s pomočjo Galoisove teorije dokazali, da se prevoje da izraziti kot funkcijo koeficientov polinoma.

V naslednjem poglavju nas čaka le še izpeljava postopka za njihov izračun.

8. Izračun prevojev kubične krivulje

Sedaj pa se lotimo našega problema eksplicitnega izračuna prevojev kubične krivulje, podane s polinomom

$$p(x,y,z) = \sum_{i=0}^{3} \sum_{j=0}^{3-i} a_{ij} x^i y^j z^{3-i-j}.$$

Tudi to poglavje je v celoti povzeto po članku [3].

Iz prejšnjih poglavij se spomnimo, da so prevoji kubične krivulje urejeni v Hessejevi konfiguraciji s strukturo ciklične grupe $\mathbb{Z}_3^2$. Vemo, da vsaka premica dvodimenzionalnega prostora $V = \mathbb{Z}_3^2$ vsebuje tri točke iz prostora, ki se seštejejo v 0. Točka Φ^i v $\mathcal{P}(V)$ pa naj označuje eno trojico premic $\{l_1^i, l_2^i, l_3^i\}$, ki skupaj pokrijejo vse točke v V; ena točka Φ^i torej skupno vsebuje vseh 9 prevojev. Vemo, da so take točke natanko 4.

Definicija 8.1. Naj bo kubična krivulja $\mathcal{C} \in \mathcal{P}^2$ podana s homogenim polinomom $p(x,y,z)$. Kubična krivulja $\mathcal{C}_\lambda$ je krivulja, podana s polinomom

$$p_\lambda(x,y,z) = p(x,y,z) + \lambda h(x,y,z),$$

kjer je $h(x,y,z)$ polinom Hessejeve krivulje. Množica polinomov $\{p_\lambda(x,y,z); \lambda \in \mathbb{C}\}$ v odvisnosti od λ podaja *šop,* oziroma 1-dimenzionalno linearno družino krivulj.

Opazimo, da tako definirana množica krivulj vsebuje vse prevoje kubične krivulje $\mathcal{C}$, saj so ti ničle tako polinoma $p(x,y,z)$, kot tudi $h(x,y,z)$. Krivulje se zvezno spreminjajo s spreminjanjem λ, pa vendar 9 prevojnih točk ostane na vsaki krivulji v tej družini krivulj.

Primer 8.2 (Hessejev šop)**.** V teoriji pogosto zasledimo t.i. *Hessejev šop.* Kot lahko sklepamo že iz imena, v tem primeru za krivuljo $\mathcal{C}$ vzamemo Hessejevo krivuljo, ki

jo že poznamo iz prejšnjih zgledov. Šop kubične krivulje $\mathcal{C}$ je potem enak množici krivulj, podanih s polinomi

$$p_\lambda(x,y,z) = x^3 + y^3 + z^3 + 6^3\lambda xyz, \lambda \in \mathbb{C}.$$

$\diamondsuit$

Točke Φ^i smo definirali kot trojice premic v $\mathcal{P}(V)$; sedaj pa te premice predstavimo v projektivni ravnini $\mathcal{P}^2(\mathbb{C})$. Točke v V bodo od sedaj naprej prevoji $\mathcal{C}$. Množico n premic na projektivni ravnini $\mathcal{P}^2$ podaja homogen polinom n-te stopnje, ki je razcepen na linearne faktorje. Torej bo naša trojica premic podana z razcepnim kubičnim polinomom in je zato razcepna kubična krivulja. Za vsako točko – trojico premic $\Phi^i \in \mathcal{P}(V)$ obstaja neka razcepna kubična krivulja, ki jo podaja. Krivuljo za Φ^i označimo z $\mathcal{C}^i = l_1^i l_2^i l_3^i \in \mathcal{P}^2(\mathbb{C})$. Ker je $\{\mathcal{C}_\lambda; \lambda \in \mathbb{C}\}$ množica krivulj, ki grejo skozi vseh 9 prevojev, hkrati pa grejo tudi trojice premic skozi vse prevoje, velja $\mathcal{C}^i \in \mathcal{C}_\lambda$. Zato bodo obstajali taki λ_i, za katere bodo polinom p_{λ_i} razcepni in bodo produkti treh linearnih homogenih polinomov.

Motivacija iskanja $\mathcal{C}_i$ je sledeča: izmed krivulj $\{\mathcal{C}_i; i \in \{1,2,3,4\}\}$ želimo določiti dve razcepni kubični krivulji (najti njun polinom). S podanima polinomoma bo zelo enostavno izračunati njun presek. V tem preseku pa bodo natanko prevojne točke krivulje $\mathcal{C}$, saj vemo, da te točke ležijo na vsaki krivulji iz šopa, ki ga tvori $\mathcal{C}$. Lotimo se torej izračuna $\mathcal{C}^i$.

Naj bo

$$h(x,y,z) = \det(H_p) = \sum_{i=0}^{3}\sum_{j=0}^{3-i} b_{ij}x^i y^j z^{3-i-j}$$

polinom Hessejeve krivulje. Koeficienti b_{ij} tega polinoma so že podani kot racionalne funkcije koeficientov a_{ij}, saj jih dobimo iz determinante Hessejeve matrike. Izračunajmo determinanto Hessejeve matrike za šop kubik

$$p_\lambda(x,y,z) = p(x,y,z) + \lambda h(x,y,z).$$

Dobimo polinom Hessejeve krivulje,

$$h_\lambda(x,y,z) = \det H_{p_\lambda},$$

v katerem parameter λ nastopa kubično. Da dobimo rezultanto polinomov $p_\lambda(x,y,z)$ in $h_\lambda(x,y,z)$, ju najprej razvijemo po eni izmed koordinat, recimo x, pri čemer upoštevamo pogoje 3.5. Rezultanta R_{p_λ,q_λ} je polinom v odvisnosti od drugih dveh spremenljivk (v našem primeru y in z) ter λ, v katerem je λ stopnje 12. Označimo

$$\Delta(\lambda) = R_{p_\lambda,h_\lambda}(y,z).$$

Če polinom $\Delta(\lambda)$ razvijmo po λ, dobimo

$$\Delta(\lambda) = \sum_{i=0}^{12} c_i(y,z)\lambda^i.$$

Naj bo $\lambda = w_i$ ničla $\Delta(\lambda)$. Potem bosta imela polinoma p_{w_i} in h_{w_i} skupni homogeni faktor stopnje 1 ali več. Torej imamo tri možnosti:

- Polinom p_{w_i} podaja kubiko in krivulja ima s kubiko polinoma h_{w_i} nerazcepni skupni faktor stopnje tri.
- Polinom p_{w_i} podaja unijo kvadrike in premice in ima z h_{w_i} bodisi nerazcepni faktor stopnje 2 (kvadriko) ali nerazcepni faktor stopnje 1 (premico).
- Polinom p_{w_i} je produkt treh homogenih faktorjev stopnje 1, ter ima z h_{w_i} vsaj en skupen nerazcepni faktor stopnje 1.

Sedaj pa se problema lotimo iz druge strani.

Trditev 8.3. *Če je kubična krivulja $\mathcal{C}$ razcepna ter je unija treh premic, je njena Hessejeva krivulja je podana s polinomom $\mathcal{H}_\mathcal{C}$ enaka prvotni krivulji $\mathcal{C}$.*

Dokaz. Naj bo $\mathcal{C}$ razcepna kubična krivulja, sestavljena kot unija treh premic in torej podana s homogenim polinomom, ki je produkt treh linearnih polinomov

$$p(x,y,z) = l_1 l_2 l_3 = (a_1x + a_2y + a_3z)(b_1x + b_2y + b_3z)(c_1x + c_2y + c_3z)$$

za neke $a_i,b_i,c_i \in \mathbb{C}, i \in \{1,2,3\}$. Ko izračunamo Hessejevo matriko in njeno determinanto, dobimo

$$h(x,y,z) = k(a_1x + a_2y + a_3z)(b_1x + b_2y + b_3z)(c_1x + c_2y + c_3z),$$

kjer je $k = 2(a_3b_2c_1 - a_2b_3c_1 - a_3b_1c_2 + a_1b_3c_2 + a_2b_1c_3 - a_1b_2c_3)^2$. Ta polinom podaja enako krivuljo kot polinom $p(x,y,z)$; krivulji $\mathcal{C}$ in $\mathcal{H}_\mathcal{C}$ sta torej enaki. □

V nadaljevanju torej želimo dokazati, da je p_λ produkt treh linearnih faktorjev. To storimo tako, da izločimo ostali dve možnosti.

Trditev 8.4. *Polinom $p_\lambda(x,y,z)$ za ničle w_1,w_2,w_3,w_4 rezultante $\Delta(\lambda)$ podaja razcepno kubično krivuljo, ki je produkt treh premic l_1, l_2 in l_3.*

Dokaz. Recimo, da to ne drži, in velja ena od drugih dveh možnosti. Naj imata polinoma p_{w_i} in h_{w_i} nerazcepni skupni faktor stopnje tri (sta enaki kubični krivulji). Ker je torej p_{w_i} nerazcepen, po [1, Izrek 4.5] dobimo protislovje, saj se krivulja brez premic nikoli ne ujema s pripadajočo Hessejevo krivuljo.

Naj sedaj polinom p_{w_i} podaja unijo kvadrike in premice. V tem primeru bi šla premica skozi 3 prevoje krivulje, kvadrika pa skozi ostalih 6. Specifična kvadrika, ki poteka skozi ostalih 6 prevojev krivulje, je unija dveh premic, kjer gre vsaka premica skozi 3 točke. Kvadrike pa so enolično določene že s 5 točkami, zato je to tudi edina možna kvadrika. Ker pa je po naši predpostavki polinom kvadrike nerazcepen, ponovno pridemo do protislovja. □

Ugotovili smo, da bo za ničle w_i rezultante $\Delta(\lambda)$ šop kubik podajal unijo treh premic. Polinom $\Delta(\lambda)$ je stopnje 12 v λ, in ker vsebuje še člene odvisne od y in z se zdi, da izračun njegovih ničel v odvisnosti od λ ne bo mogoč. Vendar pa ima ta polinom dve dodatni lastnosti. Kot prvo, so vse ničle tega polinoma trojne. To je smiselno, saj obstajajo natanko 4 taki koeficienti λ, pri katerih bo p_λ razcepen do linearnih faktorjev in tako podajal unijo treh premic. Kot drugo pa je možno polinom zapisati kot

$$\Delta(\lambda) = f(y,z)g(\lambda)$$

za neki funkciji f,g. Tako se spremenljivki ločita od λ in dobimo polinom 12 stopnje zgolj v λ. Zaradi trojnih ničel $g(\lambda)$ lahko izračunamo njegov minimalni polinom, ki je četrte stopnje, potem pa polinome četrte stopnje razstavimo na linearne člene. Tako dobimo štiri ničle $\Delta(\lambda)$, ki jih označimo z w_1,w_2,w_3 in w_4. Koeficienti minimalnega polinoma

$$\Delta_m(\lambda) = \prod_{i=1}^{4}(\lambda - w_i) = \sum_{i=0}^{4} d_i\lambda^i.$$

so racionalne funkcije koeficientov polinoma $\Delta(\lambda)$.

Na tem koraku pojasnimo, kaj smo pravzaprav dosegli z uvedbo šopa $p_\lambda(x,y,z)$. Ta šop gre skozi vse prevoje kubične krivulje $\mathcal{C}$. Zavedamo se, da šop vsebuje tudi štiri razcepne krivulje $\mathcal{C}^i, i \in \{1,2,3,4\}$, ki gredo prav tako skozi vse prevoje. Ko

prosti parameter λ preteče $\mathbb{C}$, polinom $p_\lambda(x,y,z)$ pri določenih štirih vrednostih w_i podaja singularne krivulje – trojice premic, ki potekajo skozi prevojne točke $\mathcal{C}$. Te vrednosti najdemo kot ničle polinoma $\Delta(\lambda)$. Pri teh štirih vrednostih p_λ ne bo več nerazcepen kubični polinom, pač pa produkt homogenih polinomov prve stopnje.

Tako dobimo enačbe za razcepne kubične polinome

$$g_i(x,y,z) = p(x,y,z) + w_i h(x,y,z),$$

ki podajajo trojice premic $\mathcal{C}^i$.

Zgled 8.5. Sedaj pa ponazorimo postopek izračuna ustreznih $w_i, i \in \{1,2,3,4\}$ na primeru krivulje v Weierstrassovi obliki. Pri splošni polinomski obliki bi seveda imeli več členov, vendar postopek tam ostane enak. Vsi izračuni v tem diplomskem seminarju so narejeni v programu Mathematica. Naj bo

$$p(x,y,z) = y^2z - x^3 - axz^2 - bz^3$$

polinom krivulje v Weierstrassovi obliki v odvisnosti od kompleksnih koeficientov a in b. Njena Hessejeva krivulja je

$$h(x,y,z) = 8(3xy^2 + 3ax^2z + 9bxz^2 - a^2z^3).$$

Polinom $p_\lambda(x,y,z)$ je torej

$$p_\lambda(x,y,z) = -x^3 + y^2z - axz^2 - bz^3 + 8(3xy^2 + 3ax^2z + 9bxz^2 - a^2z^3)\lambda,$$

polinom $h_\lambda(x,y,z)$ pa

$$\begin{aligned} h_\lambda(x,y,z) = 8(&3xy^2+3ax^2z+9bxz^2-a^2z^3+72ax^3\lambda-72ay^2z\lambda+72a^2xz^2\lambda+72abz^3\lambda- \\ &-5184bx^3\lambda^2 + 1728axy^2\lambda^2 + 1728a^2x^2z\lambda^2 + 5184by^2z\lambda^2 - 576a^3z^3\lambda^2- \\ &-5184b^2z^3\lambda^2 - 13824a^2x^3\lambda^3 - 41472bxy^2\lambda^3 - 41472abx^2z\lambda^3+ \\ &+13824a^2y^2z\lambda^3 - 13824a^3xz^2\lambda^3 - 124416b^2xz^2\lambda^3). \end{aligned}$$

Rezultanto teh dveh polinomov nam Mathemathica poenostavi kot

$$R_{p_\lambda,h_\lambda}(y,z) = k(y,z)(-1 - 1152a\lambda^2 + 55296b\lambda^3 + 110592a^2\lambda^4)^3,$$

kjer je

$$k(y,z) = -512z(27y^8 + 216by^6z^2 + 18(4a^3 + 27b^2)y^4z^4 - (4a^3 + 27b^2)^2z^8).$$

Opazimo, da smo dobili kub polinoma 4. stopnje, iz katerega lahko z uporabo formule za faktorizacijo polinomov 4. stopnje dobimo ustrezne $\lambda = w_i$, za katere bo ta rezultanta enaka 0. Taki λ so seveda odvisni od koeficientov a in b, ki nastopata v polinomu. Torej smo za vse Weierstrassove kubike dobili kar direktno formulo za $w_i, i \in \{1,2,3,4\}$. Tudi te vrednosti imajo obsežno formulo, zato zapišimo samo eno izmed njih:

$$\begin{aligned} w_1 = &-\frac{b}{8a^2} - \frac{1}{24}\sqrt{\frac{1}{a} + \frac{9b^2}{a^4} + \frac{(-4a^3-27b^2)^{\frac{1}{3}}}{2^{\frac{2}{3}}a^2}} - \\ &-\frac{1}{2}\sqrt{\frac{1}{72a} + \frac{b^2}{8a^4} - \frac{(-4a^3-27b^2)^{\frac{1}{3}}}{144(2^{\frac{2}{3}})a^2} - \frac{3(-\frac{b}{48a^3} - \frac{b^3}{8a^6})}{\sqrt{\frac{1}{a} + \frac{9b^2}{a^4} + \frac{(-4a^3-27b^2)^{\frac{1}{3}}}{2^{\frac{2}{3}}a^2}}}}. \end{aligned}$$

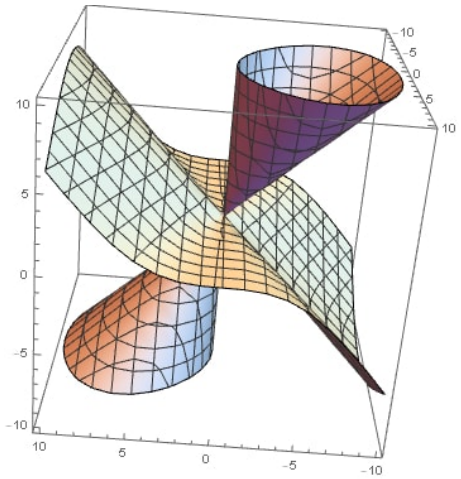
Ta izraz ni definiran za $a = 0$, zato tak primer obravnavamo ločeno. Kot vidimo iz rezultante $R_{p_\lambda,h_\lambda}(y,z)$, bi v tem primeru dobili kub polinoma stopnje 3 in tako zgolj tri koeficiente λ. ♢

V posebnih primerih se lahko pri postopku pojavi težava, da polinom $\Delta(\lambda)$ ni stopnje 12, ampak manj. Tak primer je tudi Fermatova kubika, pri kateri dobimo polinom stopnje zgolj 9. Tako dobimo tri ustrezne w_i, kar pa nam za izračun prevojev prav tako zadošča.

Primer 8.6. Naredili bomo izračun koeficientov $w_i, i \in \{1,2,3,4\}$ za kubično krivuljo $\mathcal{C}$, podano s polinomom

$$p(x,y,z) = y^2z - x(x-z)(x+z).$$

Ker je $\mathcal{C}$ v Weiestrassovi obliki, bi lahko za izračun uporabili zgoraj izpeljano formulo, vendar pa za namen aplikacije na specifični kubiki ponovimo postopek. Hessejeva



Slika 23. Kubična krivulja $p(x,y,z) = y^2z - x(x-z)(x+z)$.

matrika krivulje je matrika

$$H_p = \begin{pmatrix} -6x & 0 & 2z \\ 0 & 2z & 2y \\ 2z & 2y & 2x \end{pmatrix},$$

polinom Hessejeve krivulje pa je potem enak

$$h(x,y,z) = \det H_p = 8(3xy^2 - 3x^2z - z^3).$$

Šop kubičnih krivulj v odvisnosti od λ je podan s polinomi

$$p_\lambda(x,y,z) = y^2z - x(x-z)(x+z) + 8(3xy^2 - 3x^2z - z^3)\lambda,$$

njihova Hessejeva krivulja pa s polinomom

$$h_\lambda(x,y,z) = 8(3xy^2 - 3x^2z - z^3 - 72x^3\lambda + 72y^2z\lambda + 72xz^2\lambda - 1728xy^2\lambda^2 +$$

$$+1728x^2z\lambda^2 + 576z^3\lambda^2 - 13824x^3\lambda^3 + 13824y^2z\lambda^3 + 13824xz^2\lambda^3).$$

Polinoma $p_\lambda(x,y,z)$ in $h_\lambda(x,y,z)$ razvijemo po potencah x in izračunamo rezultanto $R_{p_\lambda,h_\lambda}(x)$. Ta je enaka

$$\det\begin{pmatrix} z(y^2-8z^2\lambda) & z^2+24y^2\lambda & -24z\lambda & -1 & 0 & 0 \\ 0 & z(y^2-8z^2\lambda) & z^2+24y^2\lambda & -24z\lambda & -1 & 0 \\ 0 & 0 & z(y^2-8z^2\lambda) & z^2+24y^2\lambda & -24z\lambda & -1 \\ A & B & C & D & 0 & 0 \\ 0 & A & B & C & D & 0 \\ 0 & 0 & A & B & C & D \end{pmatrix},$$

kjer označimo

$$\begin{aligned} A &= 8z(72y^2\lambda(1+192\lambda^2)+z^2(-1+576\lambda^2)), \\ B &= 24(y^2(1-576\lambda^2)+24z^2\lambda(1+192\lambda^2)), \\ C &= 24z(-1+576\lambda^2), \\ D &= -576(\lambda+192\lambda^3). \end{aligned}$$

Determinanta te matrike nam porodi polinom stopnje 12 v λ. Po poenostavljanju dobimo

$$R_{p_\lambda,h_\lambda}(x) = 512z(-27y^8+72y^4z^4+16z^8)(-1+1152\lambda^2+110592\lambda^4)^3.$$

Vidimo, da nam je uspelo v polinomu člene, ki so odvisni od y in z, ločiti od tistih, odvisnih od λ. Preko formule za faktorizacijo polinomov 4. stopnje potem izračunamo ničle rezultante. To so

$$\begin{aligned} w_1 &= -0.028385418276383887, \\ w_2 &= -0.105936i, \\ w_3 &= 0.105936i, \\ w_4 &= 0.028385418276383887. \end{aligned}$$

Te ničle nam enolično točno določijo štiri trojice premic, ki gredo skozi prevojne točke kubične krivulje. Njihove enačbe so

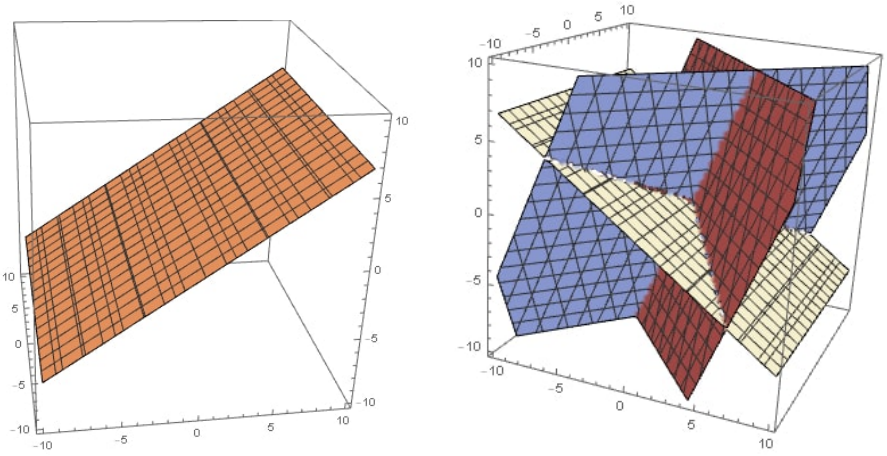
$$\begin{aligned} g_1(x,y,z) &= p_{w_1}(x,y,z) = y^2z - x(x-z)(x+z) + 8(-0.0283854)(3xy^2-3x^2z-z^3), \\ g_2(x,y,z) &= p_{w_2}(x,y,z) = y^2z - x(x-z)(x+z) + 8(-0.105936i)(3xy^2-3x^2z-z^3), \\ g_3(x,y,z) &= p_{w_3}(x,y,z) = y^2z - x(x-z)(x+z) + 8(0.105936i)(3xy^2-3x^2z-z^3), \\ g_4(x,y,z) &= p_{w_4}(x,y,z) = y^2z - x(x-z)(x+z) + 8(0.0283854)(3xy^2-3x^2z-z^3). \end{aligned}$$

Zavedati se moramo, da so nekatere premice realne, nekatere pa ne. V resnici tako za w_2 kot za w_3 ne dobimo nobene realne premice; pri w_1 je realna zgolj ena, pri w_4 pa vse tri, kot je prikazano na sliki 24.

♢

Kljub temu, da sedaj za polinome $g_i(x,y,z)$ vemo, da so produkti treh linearnih faktorjev, pa smo obtičali s polinomi tretje stopnje v treh spremenljivkah, ki jih ne znamo razcepiti. Zato se bo potrebno lotiti še tega problema.

Tri premice krivulje $\mathcal{C}_i$ se paroma sekajo v treh točkah, vsak par premic v eni. Te točke pa so singularne točke $\mathcal{C}$. Če nam jih uspe izračunati, bodo premice z njimi enolično določene kot premice skozi dve posamezni točki. Torej se najprej posvetimo računanju teh singularnih točk.



Slika 24. Realni del singularnih krivulj ozroma trojic premic, podanih s polinomoma g_1 ter g_4.

Izračunajmo parcialne odvode polinoma $g_i(x,y,z)$. V ustreznih singularnih točkah bo moralo veljati, da

$$\nabla g_i(x,y,z) = \left(\frac{\partial g_i(x,y,z)}{\partial x}, \frac{\partial g_i(x,y,z)}{\partial y}, \frac{\partial g_i(x,y,z)}{\partial z}\right) = (0,0,0).$$

Ker pri odvajanju po katerikoli spremenljivki izgubimo eno stopnjo, nam v gradientu ostanejo polinomi 2. stopnje. Ti pa podajajo vsaka svojo *kvadriko* oziroma projektivno algebraično krivuljo 2. stopnje. Označimo jih z Q_1^i, Q_2^i in Q_3^i, njihove polinome pa z $q_1^i(x,y,z), q_2^i(x,y,z)$ in $q_3^i(x,y,z)$. Točke, kjer bodo vsi parcialni odvodi 0 so natanko tiste, ki ležijo na vseh treh kvadrikah, zato moramo poiskati njihov presek.

Avtor članka [3] to doseže z uporabo posebne rezultante za tri polinome v več spremenljivkah. Ta je drugačna, kot smo jo definirali mi, podrobno pa je opisana v [2, poglavje 13]. V tem delu zgolj omenimo, da preko nje izračunamo presečne točke treh kvadrik – to so ničle te rezultante. Tvorimo jo tako, da vse tri polinome kvadrik razvijemo po eni spremenljivki, ter za vsak polinom v eno vrstico 3×3 matrike po vrsti dodamo tri koeficiente pri različnih potencah spremenljivke. Za polinome

$$\begin{aligned} q_1^i(x,y,z) &= r_{10}(y,z) + r_{11}(y,z)x + r_{12}(y,z)x^2, \\ q_2^i(x,y,z) &= r_{20}(y,z) + r_{21}(y,z)x + r_{22}(y,z)x^2, \\ q_3^i(x,y,z) &= r_{30}(y,z) + r_{31}(y,z)x + r_{32}(y,z)x^2, \end{aligned}$$

bo taka rezutanta enaka

$$R_{q_1^i,q_2^i,q_3^i} = \det \begin{pmatrix} r_{10}(y,z) & r_{11}(y,z) & r_{12}(y,z) \\ r_{20}(y,z) & r_{21}(y,z) & r_{22}(y,z) \\ r_{30}(y,z) & r_{31}(y,z) & r_{32}(y,z) \end{pmatrix}.$$

To je homogen kubični polinom v spremenljivkah y in z, ki ga po lemi 2.12 lahko razcepimo na produkt treh polinomov. Ko ga izenačimo z 0, dobimo tri linearne zveze med spremenljivkama y in z. Izberimo eno od teh zvez ter se vrnimo k prvotni krivulji $g_i(x,y,z)$. Če eno od spremenljivk v enačbi izrazimo z drugo, nam ostaneta dve spremenljivki; ker pa smo v projektivnem prostoru, lahko brez škode za splošnost izberemo $x = 1$. Vstavimo še to v $g_i(x,y,z)$ in dobimo kubični polinom v eni spremenljivki, recimo y. Ničle tega polinoma nam podajajo 3 možne rešitve za

preostalo spremenljivko, in tako skupno dobimo 3 projektivne točke, od katerih pa je zgolj ena prava. Za vsako točko $[x,y,z]$ je tako potrebno preveriti, ali v njej velja $\nabla g_i(x,y,z) = 0$. To bo držalo zgolj pri eni točki, ki je naša prva singularna točka. Drugi dve dobimo na enak način, s tem da v rezultanti $R_{q_1^i,q_2^i,q_3^i}$ ločeno obravnavamo še drugi dve linearni zvezi med y in z.

Da potrdimo ustreznost postopka iskanja singularnih točk, postavimo naslednjo trditev.

Trditev 8.7. *Naj bo $\mathcal{C}$ razcepna kubika, ki je unija treh premic in podana s polinomom*

$$g(x,y,z) = (o_1x + o_2y + o_3z)(m_1x + m_2y + m_3z)(n_1x + n_2y + n_3z),$$

kjer so $o_i,m_i,n_i \in \mathbb{C}$. Singularni preseki

$$s_1 = [o_3m_2 - o_2m_3, o_1m_3 - o_3m_1, o_2m_1 - o_1m_2]$$
$$s_2 = [o_3n_2 - o_2n_3, o_1n_3 - o_3n_1, o_2n_1 - o_1n_2]$$
$$s_3 = [m_3n_2 - m_2n_3, m_1n_3 - m_3n_1, m_2n_1 - m_1n_2]$$

dveh premic polinoma $g(x,y,z)$ so natanko točke v preseku treh kvadrik, ki jih podajajo parcialni odvodi polinoma $g(x,y,z)$.

Dokaz. Poiskali bomo presečne točke treh kvartik in pokazali, da ležijo na $\mathcal{C}$. Izračunajmo parcialne odvode polinoma $g(x,y,z)$,

$$\nabla g(x,y,z) = \left(\frac{\partial g(x,y,z)}{\partial x}, \frac{\partial g(x,y,z)}{\partial y}, \frac{\partial g(x,y,z)}{\partial z}\right).$$

Odvod po spremenljivki x je enak

$$\begin{aligned}\frac{\partial g(x,y,z)}{\partial x} = \quad & o_1(m_1x + m_2y + m_3z)(n_1x + n_2y + n_3z) + \\ & +n_1(m_1x + m_2y + m_3z)(o_1x + o_2y + o_3z) + \\ & +m_1(n_1x + n_2y + n_3z)(o_1x + o_2y + o_3z),\end{aligned}$$

odvoda po drugih dveh spremenljivkah pa izračunamo analogno z odvajanjem y ali z. Ti parcialni odvodi nam določijo $q_1^i(x,y,z), q_2^i(x,y,z)$ in $q_3^i(x,y,z)$. Izraze nato razvijemo po spremenljivki x, vstavimo v 3×3 matriko in izračunamo njeno determinanto. Ta je enaka

$$\begin{aligned}R_{q_1^i,q_2^i,q_3^i} \quad = \quad & k(m_2n_1y - m_1n_2y + m_3n_1z - m_1n_3z) \\ & (m_2o_1y - m_1o_2y + m_3o_1z - m_1o_3z) \\ & (-n_2o_1y + n_1o_2y - n_3o_1z + n_1o_3z),\end{aligned}$$

kjer je

$$k = (-m_3n_2o_1 + m_2n_3o_1 + m_3n_1o_2 - m_1n_3o_2 - m_2n_1o_3 + m_1n_2o_3).$$

Najprej se osredotočimo na prvi člen $(o_2m_1y - o_1m_2y + o_3m_1 - o_1m_3)$. V afini ravnini $z = 1$ je y-koordinata iskane točke enaka

$$y = \frac{(o_3m_1 - o_1m_3)}{-o_2m_1 + o_1m_2}.$$

To vrednost y vstavimo v polinome kvadrik, in če upoštevamo še $z = 1$, dobimo polinome v spremenljivki x. Vsak od treh polinomov je druge stopnje in ga tako lahko razcepimo na linearne faktorje. Iskana vrednost x je tista, ki se pojavi v

razcepu vseh treh polinomov. Vsak od njih mora imeti namreč v iskani točki $[x,y,z]$ vrednost 0. V našem primeru je to vrednost

$$x = \frac{o_3m_2 - o_2m_3}{o_2m_1 - o_1m_2}.$$

Prva iskana singularna točka je torej točka

$$\left[\frac{o_3m_2 - o_2m_3}{o_2m_1 - o_1m_2}, \frac{o_3m_1 - o_1m_3}{-o_2m_1 + o_1m_2}, 1\right],$$

zaradi homogenosti koordinat pa to točko lahko preprosteje zapišemo kot

$$[o_3m_2 - o_2m_3, -o_3m_1 + o_1m_3, o_2m_1 - o_1m_2].$$

Če to točko vstavimo v enačbe premic

$$l_1(x,y,z) = o_1x + o_2y + o_3z,$$
$$l_2(x,y,z) = m_1x + m_2y + m_3z,$$
$$l_3(x,y,z) = n_1x + n_2y + n_3z,$$

dobimo

$$l_1(m_2o_1 - o_1m_2, -o_3m_1 + o_1m_3, o_2m_1 - o_1m_2) = 0,$$
$$l_2(m_2o_1 - o_1m_2, -o_3m_1 + o_1m_3, o_2m_1 - o_1m_2) = 0,$$
$$l_3(m_2o_1 - o_1m_2, -o_3m_1 + o_1m_3, o_2m_1 - o_1m_2) \neq 0.$$

Točka s_1 je torej v preseku dveh premic krivulje $\mathcal{C}$. Za drugi dve točki je postopek analogen.

□

Iz singularnih točk, ki smo jih pridobili po zgornjem postopku, želimo sedaj izračunati vse tri premice l_1,l_2 in l_3. Vemo, da so projektivne premice podane z enačbo

$$ax + by + cz = 0.$$

Če paroma izbiramo dve od treh izračunanih točk, ter ju vstavimo v dve taki enačbi, bomo prišli do vseh treh premic krivulje $\mathcal{C}^i$.

Na tak način določimo polinoma dveh izmed kubičnih krivulj $\mathcal{C}^1, \mathcal{C}^2, \mathcal{C}^3$ ali $\mathcal{C}^4$. Vemo, da so prevoji natanko točke v presečiščih dveh trojic premic iz šopa. Zato lahko z izračunom presekov dveh trojic premic dobimo natanko 9 prevojev kubične krivulje $\mathcal{C}$.

Zgornji algoritem ponazorimo na primeru.

Primer 8.8. Nadaljujmo postopek na kubični krivulji $\mathcal{C}$ iz prejšnjega primera, podani s

$$p(x,y,z) = y^2z - x(x - z)(x + z).$$

Pri njej smo že izračunali polinome g_1,g_2,g_3 in g_3. Obravnavajmo dve razcepni krivulji podani s polinomoma

$$g_1 = y^2z - x(x - z)(x + z) + 8(-0.0283854)(3xy^2 - 3x^2z - z^3)$$

in

$$g_2 = y^2z - x(x - z)(x + z) + 8(-0.105936i)(3xy^2 - 3x^2z - z^3).$$

Njuna gradienta sta

$$\nabla g_1 = (q_{11},q_{12},q_{13}) = (-x(x - z) - x(x + z) - (x - z)(x + z) - 0.227083(3y^2 - 6xz),$$
$$-1.3625xy + 2yz, y^2 - x(x - z) + x(x + z) - 0.227083(-3x^2 - 3z^2))$$

in

$$\nabla g_2 = (q_{21},q_{22},q_{23}) = (-x(x-z) - x(x+z) - (x-z)(x+z) - 0.847487i(3y^2 - 6xz),$$
$$-5.08492ixy + 2yz, y^2 - x(x-z) + x(x+z) - 0.847487i(-3x^2 - 3z^2)).$$

Parcialne odvode potem razvijemo po spremenljivki x in jih vstavimo v rezultanti

$$R_{q_{11},q_{12},q_{13}} = \det \begin{pmatrix} -0.68125y^2 + z^2 & 1.3625z & -3 \\ 2yz & -1.3625y & 0 \\ y^2 + 0.68125z^2 & 2z & 0.68125 \end{pmatrix},$$

$$R_{q_{21},q_{22},q_{23}} = \det \begin{pmatrix} -2.54246iy^2 + z^2 & 5.08492iz & -3 \\ 2yz & -5.08492iy & 0 \\ y^2 + 2.54246iz^2 & 2z & 2.54246i \end{pmatrix}.$$

Rezultanti izračunamo ter dobimo

$$R_{q_{11},q_{12},q_{13}}(y,z) = -3.45516y^3 - 17.5692yz^2,$$
$$R_{q_{21},q_{22},q_{23}}(y,z) = -48.1242iy^3 + 65.5692yz^2.$$

Osredotočimo se najprej na prvi primer za $g_1(x,y,z)$ in rezultanto $R_{q_{11},q_{12},q_{13}}(y,z)$. Ta mora biti enaka 0, zato lahko y z z izrazimo na tri načine,

$$y_1 = 0,$$
$$y_2 = -2.25498iz,$$
$$y_3 = 2.25498iz.$$

Nato fiksiramo $x = 1$, in ko vstavimo $y = 0$ in $x = 1$ v prvotno enačbo naše krivulje, dobimo polinom v eni spremenljivki

$$g_1(1,0,z) = -(1-z)(1+z) - 0.227083(-3z - z^3),$$

katerega rešitve so

$$z_{1,2} = -2.54246,$$
$$z_3 = 0.68125.$$

Sedaj moramo določiti še, katera rešitev je prava. Iščemo tako točko, da so v njej parcialni odvodi g_1 vsi enaki 0. Izračunamo

$$\nabla g_1(1,0,-2.54246) = (1.77636 \times 10^{-15},0,0),$$
$$\nabla g_1(1,0,0.68125) = (-1.6077,0,2.35992).$$

Očitno je, da je prava rešitev $z_{1,2} = -2.54246$. Zaradi numeričnega računanja sicer dobimo določeno zaokrožitveno napako, vendar je vrednost odvoda v tej točki zanemarljivo majhna in vemo, da gre za pravo rešitev. Prva singularna točka, ki smo jo dobili, je torej točka

$$s_1 = [1,0,-2.54246].$$

Postopek ponovimo za $y = -2.25498zi$ ter dobimo

$$g_1(1,-2.25498zi,z) = -1 + 0.68125z + 4.4641z^2 - 4.85784z^3$$

z rešitvami

$$z_{1,2} = 0.68125,$$
$$z_3 = -0.443552.$$

Gradienta

$$\nabla g_1(1,-1.5362i,0.681250) = (-1.77636 \times 10^{-15}, 4.44089 \times 10^{-16}i, 4.44089 \times 10^{-16}),$$
$$\nabla g_2(1,1.0002i,0.443552) = (-2.72608,-2.25005i,-1.07222).$$

nam pokažeta, da je druga iskana točka

$$s_2 = [1, -1.5362i, 0.681250].$$

Na enak način iz $y = 2.25498iz$ dobimo

$$s_3 = [1, 1.5362i, 0.681250].$$

Sedaj, ko nam je uspelo dobiti singularne točke, v katerih se premice sekajo, lahko iz njih izračunamo vse tri projektivne premice krivulje $\mathcal{C}^1$. Za l_1^1 rešimo sistem

$$a + (-2.54246)c = 0,$$

$$a + -1.5362ib + 0.681250c = 0,$$

kjer dobimo zvezi za dva koeficienta v odvisnosti od tretjega, in tako projektivno premico

$$x - 0.825379iy + 0.39332z = 0.$$

Iz dveh preostalih parov pa izračunamo še premici l_2^1 in l_3^1, ki imata enačbo

$$x - 1.46789z = 0,$$

$$x + 0.825379iy + 0.39332z = 0.$$

Na analogen način obravnavamo drugo rezultanto. Po vseh potrebnih izračunih dobimo, da so projektivne premice l_1^2, l_2^2 in l_3^2 podane z enačbami

$$x + (-1.127488 + 1.127488i)y + 1.467890iz = 0,$$

$$x + 0.393320iz = 0,$$

$$x + (1.127488 - 1.127488i)y - 1.467890iz = 0.$$

Preostane nam še izračun preseka $\mathcal{C}^1$ in $\mathcal{C}^2$, torej presekov premic l_i^1 z l_j^2 za $i,j \in \{1,2,3\}$. To naredimo tako, da v enačbi premice preprosto izrazimo eno spremenljivko, in jo vstavimo v enačbo druge premice, kar nam da pogoj za eno koordinato v preseku. Če upoštevamo še $z = 1$,$y = 1$ ali $x = 1$, ter oboje vstavimo v enačbe ene od premic, dobimo točko v homogenih koordinatah. Koeficiente, manjše od 1×10^{-15} bomo zaokrožili na 0, saj gre za posledico zaokrožitvenih napak pri numeričnem računanju.

Tako izračunamo vseh 9 točk v preseku krivulj $\mathcal{C}_1$ in $\mathcal{C}_2$, to pa so

$$S_1 = [1, -1.21157 - 1.21157i, -2.54246i],$$

$$S_2 = [1, 0.886927, 0.68125],$$

$$S_3 = [1, 0.886927i, -0.68125],$$

$$S_4 = [1, 1.21157 - 1.21157i, 2.54246i],$$

$$S_5 = [0, 1, 0],$$

$$S_6 = [1, -0.886927i, -0.68125],$$

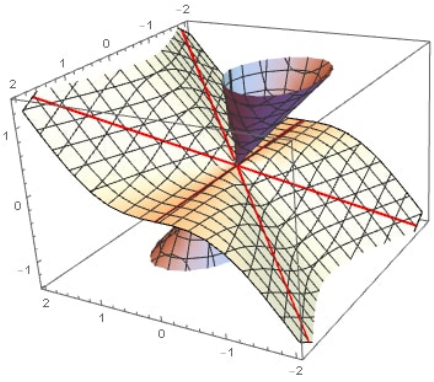
$$S_7 = [1, -1.21157 + 1.21157i, -0.68125],$$

$$S_8 = [1, -0.886927, 0.68125],$$

$$S_9 = [1, 1.21157 + 1.21157i, -2.54246i].$$

To je natanko devet prevojnih točk krivulje $\mathcal{C}$. ♢

Kot se je izkazalo, je opisan algoritem za izračun že pri enostavni kubični krivulji računsko kar zahteven. Kljub temu pa vrne eksplicitno izražene prevoje za poljubno kubično krivuljo.



Slika 25. Kubična krivulja, podana s polinomom $p(x,y,z) = y^2z - x(x-z)(x+z)$ ter njeni trije realni prevoji.

Slovar strokovnih izrazov

affine space afin prostor
composition series kompozicijska vrsta
field extension razširitev polja
flex prevoj, prevojna točka
Hessian Hessejeva krivulja
intersection presek
intersection multiplicity presečna večkratnost
irreducible nerazcepen
kernel jedro
lattice mreža
zero locus of a polynomial množica ničel polinoma
map preslikava
monodromy group monodromijska grupa
normal subgrup normalna podgrupa, edinka
pencil of cubics šop kubičnih krivulj
projective space projektivni prostor
projectivity projektivnost
reducible razcepen
solvable group rešljiva grupa

Literatura

[1] G. Fischer, *Plane algebraic curves,* Student Mathematical Library **15**, American Mathematical Society, Providence, RI, 2001.
[2] I.M. Gelfand, M.M Kapranov, A.V. Zelevinsky, *Discriminants, resultants and multidimensional determinants,* Modern Birdhauser Classics, Birkhauser Boston, 1994.
[3] J. Harris, *Galois groups of enumerative problems,* Duke Math. J., **46** no. 4,(1979), 685–724.
[4] T.W. Hungerford, *Algebra,* Holt, Rinehart and Winston, Inc., New York-Montreal, Que.-London, 1974.
[5] N. Jacobson, *Lectures in abstract algebra, Vol III: Theory of fields and Galois theory,* D. Van Nostrand Co., Inc., Princeton, N.J.-Toronto, Ont.-London-New York 1964.
[6] F. Kirwan, *Complex algebraic curves,* London Mathematical Society, Student Texts **23**, Cambridge University Press, Cambridge, 1992.
[7] M. Reid, *Undergraduate algebraic geometry,* London Mathematical Society Student Texts **12**, Cambridge University Press, Cambridge, 1988.
[8] L. Rowen, *Algebra: Groups, rings and fields,* A K Peters, Ltd., Wellesley, MA, 1994.

[9] J.H. Silverman in J.T. Tate, *Rational points on elliptic curves,* 2nd ed., Undergraduate Texts in Mathematics. Springer, Cham, 2015.
[10] A. Vavpetič, *Afina in projektivna geometrija,* prva izdaja, samozaložba Aleš Vavpetič, Ljubljana, 2011, dostopno na `https://www.fmf.uni-lj.si/~vavpetic/APG/APG.pdf`.
[11] *Zapiski s predavanja pri predmetu Algebraične krivulje,* Tomaž Košir, študijsko leto 2015/2016.
[12] *Hesse configuration*, v: Wikipedia, The Free Encyclopedia, [ogled 21.1.2018], dostopno na `https://en.wikipedia.org/wiki/Hesse_configuration`.
[13] *Galois group*, v: Wikipedia, The Free Encyclopedia, [ogled 21.1.2018], dostopno na `https://en.wikipedia.org/wiki/Galois_group`.
[14] *Galois theory*, v: Wikipedia, The Free Encyclopedia, [ogled 28.1.2018], dostopno na `https://en.wikipedia.org/wiki/Galois_theory`.
[15] *Solvable group*, v: Wikipedia, The Free Encyclopedia, [ogled 28.1.2018], dostopno na `https://en.wikipedia.org/wiki/Solvable_group`.
[16] *Traintracks*, v: Askmathematician.com, [ogled 21.3.2018], dostopno na `http://www.askamathematician.com/wp-content/uploads/2011/04/traintracks.jpg`.