Математичка гимназија Београд

МАТУРСКИ РАД

ГДЕ СЕ САСТАЈУ ГЕОМЕТРИЈА И ПОЛИНОМИ?

Кандидат:
Игор Спасојевић, IV_D

Ментор:
Ђорђе Баралић

јун 2012. Београд

Садржај

1

Увод

О математици и њеној улози у развоју човечанства је пуно тога речено и написано. Слично је са уметношћу. За математику се каже да је уметност људског ума. Шта је заједничко за математику и уметност? Обе ствара човек. Уметност изазива осећај лепог у човеку, али ово осећање није лако описати, јер свако од нас има сопствени доживљај лепог. Тако ће се математичари (а и многи други) сложити да у математици има много тога што је лепо, али не надахњују исте ствари сваког математичара на исти начин. У овом раду ће се приказати тврђења за која ћемо се вероватно сви сложити да су најпре лепа и тајанствена, а потом и видети да су и данас велика покретачка снага у математици.

Математика се развија од када и људски род. Геометрија као прва практична примена математичких знања била је развијена и код древних цивилизација. Са њом је се развијала и алгебра. Еуклидови *Елементи* били су круна геометријског знања антике. Арабљани су та знања сачували и обогатили, да бих и западна цивилизација поново открила у доба ренесансе. Од тада може се рећи траје непрекидна математичка револуција. Рене Декарт је увођењем координатног система спојио алгебру и геометрију и далекосежно повезао визуелно и апстрактно. Геометрија коју обично везујемо за визуелне објекте као што су тачке праве, кругови, ... постаје дубља и слободнија, док алгебра повезујући се са геометријом више није статична већ динамична математичка дисциплина. Математика се развијала тако да већ у XX веку постоји много математичких дисциплина које имају своје објекте и технике изучавања које се некада чине доста удаљени једни од других. Међутим овакав развој математике никада није нарушио њено јединство као науке, јер се математичке идеје препличу на неочекиване и изненађујуће начине. Тако и овде желимо да говоримо о преплитању и повезаности две фундаменталне математичке теорије геометрије и полинома.

Геометрија је свој најбржи развој имала у XIX веку. Покушаји да се докаже пети Еуклидов постулат довели су до стварања нових геометрија, која су изменила и интуицију коју је свет до тада имао о геометрији. Појавиле су се хиперболичка и пројективна геометрија. У пројективних геометрији не постоје паралелне праве, а омогућава нам једну прозрачнију слику о тврђењима за које се знало да важе и у еуклидској геомитрији као што су Паскалова, Дезаргова, Бријаншонова и Папосова теорема. Класична пројективна геометрија је свој врхунац достигла са доказом Понселеове теореме, али развој геометрији није ту стао.

Алгебра и алгебарске структуре су постале језик којим коминицира наука. Хилберт је и геометрију поставио на алгебарске основе. Богатство алгебарских структура и оно што су оне пружиле математици, учинило је да су нам многи алгебарски објекти постали природни и блиски. Такви су полиноми. Не постоји математичка дисциплина која није на директан или индиректан начин заинтересована за полиноме. Тако и

геометрија. На овај начин је се родила једна од најизазовнијих грана математике - алгебарска геометрија. У овој области је урађено много, али и данас је много отворених питања у алгебарској на које покушавају да реше математичари, па је ово сигурно од једна од дисциплина која ће се активно развијати у XXI веку.

Овде ћемо говорити о нечему што слободно можемо назвати елементарном алгебарском геометрији. Најпре ћемо дефинисати равне алгебарске криве, са акцентом на конике и кубике као објекте са којим се срећемо и током гимназијског образовања. Затим ћемо показати теорему о кавезу (Katz) која је специјалан случај чувене Безуове теореме. Применом ове теореме доказаћемо теореме везане класичне Папосове и Паскалове теореме за мистичне шестоуглове уписане у конике. Доказаћемо неке познате и неколико нових резултата за мистичне осмоуглове и $2n$-тоуглове уписане у конике који ће дати потпуно нову слику на ова тврђења. То је слика која ће открити дубоку везу између ових тврђења. На крају ћемо се дотакнути и неких отворених и озбиљних проблема за структуре Папосовог и Паскаловог типа.

Од велике помоћи у настајању овог рада био је и програмски пакет Cinderella који је развио Jürgen Richter-Gebert један од данас водећих немачких математичара. Ова тема је веома актуелна данас и њом се баве неки од светских познатих математичара, као што је S. Tabachnikov, L. Evans, G. Katz, R. Swartz и други. Недавно је изашла и књига Roberta Bixa, *Conics and cubics: an elementary introduction to the algebraic geometry* Конике и кубике: елементаран увод у алгебарску геометрију која показује да ова елементарна прича и те како привлачи пажњу научне јавности.

Jürgen Richter-Gebert

Robert Bix

Где се састају геометрија и полиноми? Тамо где почиње једна лепа и још недовољно истражена математика.

2

Алгебарске криве

2.1 Равне алгебарске криве

У овом делу ћемо се упознати са реалним и комплексним алгебарским кривама.

Дефиниција 2.1.1. *Реална алгебарска крива* $\mathcal{C}$ је подскуп од $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ који је геометријско место тачака нула полинома две променљиве $P(x, y)$ са реалним коефицијентима, тј.

$$\mathcal{C} = \left\{(x, y) \in \mathbb{R}^2 \mid P(x, y) = 0\right\}.$$

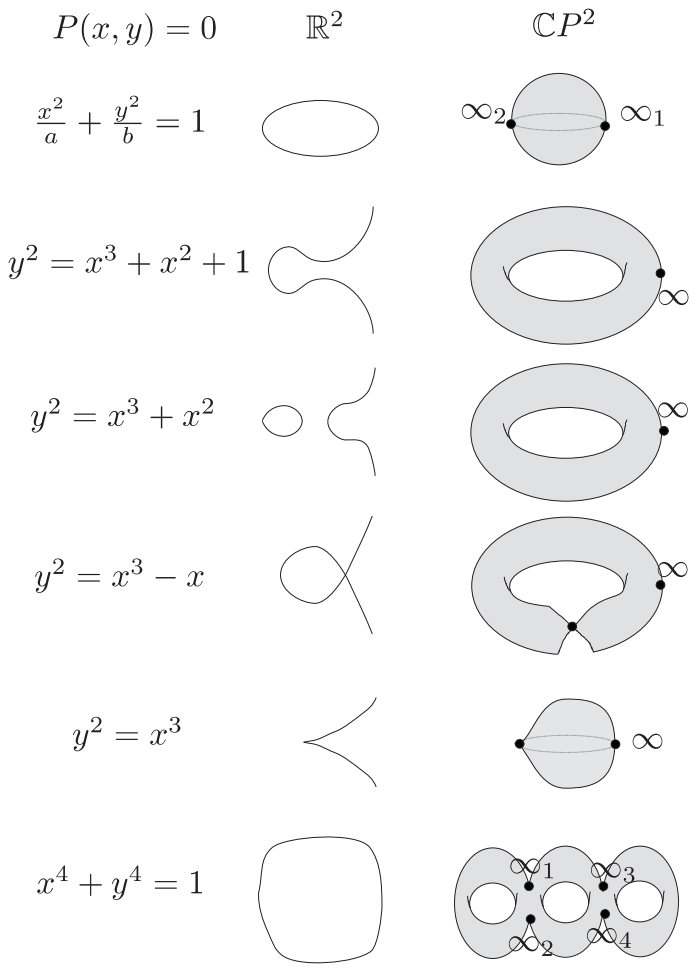
Дефиниција 2.1.2. *Комплексна алгебарска крива* $\mathcal{C}$ је подскуп од $\mathbb{C}^2 = \mathbb{C} \times \mathbb{C}$ који је геометријско место тачака нула полинома две променљиве $P(x, y)$ са комплексним коефицијентима, тј.

$$\mathcal{C} = \left\{(x, y) \in \mathbb{C}^2 \mid P(x, y) = 0\right\}.$$

На очигледан начин се свакој реалној алгебарској кривој може придружити комплексна алгебарска крива. Реалне алгебарске криве су изучаване хиљаду година раније него што су комплексне алгебарске криве признате као математички објекат иако када су се појавиле постало је јасно да су оне и једноставније и интересантније за проучавање. На пример много је лакше полином са реалним коефицијентима посматрати као полином са комплексним коефицијентима јер се у $\mathbb{C}$ сваки полином факторише и једноставније је узети само реалне нуле и одбацити остале. Комплексне алгебарске криве се могу проучавати са становишта неколико математичких дисциплина од којих се издвајају алгебра, топологија и комплексна анализа.

Реалне алгебарске криве су проучавали у старој Грчкој. Они нису знали за једначине круга, параболе, елипсе, хиперболе, али су познавали ове објекте као геометријска места тачака. Нпр. елипса је геометријско место тачака чији је збир растојања од две унапред задане тачке које називамо жижама константан. Праве и кругове је могуће конструисати помоћу шестара и лењира, док остале криве другог реда није могуће. Стари Грци су решавајући проблеме дуплирања коцке и трисекције угла конструисали инструменте којима су конструисали параболе, јер се уочили да се ови проблеми могу решити конструисањем ових кривих. Тек са развитком теорије Галоа много година касније доказано је да су ове конструкције не могу решити помоћу шестара и лењира.

Пример 2.1.1. На слици 2.1 ћемо приказати неколико алгебарских криви са њиховим једначинама и одговарајућом сликом као релном односно комплексном кривом. Слике комплексне криве заправо живе у пројективном простору $\mathbb{C}P^2$ о коме ћемо нешто касније детаљније говорити.



Слика 2.1.

Стари Грци су познавали и друге алгебарске криве као епицикличне криве којима су описиване путање планета пре откирића Кеплерових закона. Западна Европа је ова знања поново открила у ренесансном добу када су откривене и нове алгебарске криве. Леонардо да Винчи се посебно интересовао за њих проучавајући перспективу тродимензионалних облика. Античка знања западни свет је преузео од Арабљана који су имали развијен алгебарски запис математике, што је условило каснији убрзан развој математике.

Крајем XVII века, математичари су овладали идејама Декарта и Фермаа да се геометријска места тачака описују као решења једне или више једначина две променљиве по x и y. Развој диференцијалног рачуна и његова примена на алгебарске криве довела је до нових сазнања о овим објектима. Знања о алгебарске криве су се појавиле као конкретна примена математике у многим другим проблемима.

Различити облици алгебарских кривих заинтересовало је математичаре као што су Њутн за сингуларитете алгебарских кривих. Сингуларитети су тачке у којима сликовито речено крива доживљава дегенерацију тј. не изгледа "глатко". На слици 2.1 се могу уочити тачке у којима крива одступа од свог стандардног облика, где се учворава или постаје оштра. Те тачке су сингуларне и у њима долази до деформације криве, које је важно разумети.

Дефиниција 2.1.3. Тачка $(x, y) \in \mathcal{C}$ алгебарске криве $\mathcal{C}$ дефинисане полиномском једначином $P(x, y) = 0$ је *сингуларна (сингуларитет)* уколико је

$$\frac{\partial P}{\partial x}(x, y) = \frac{\partial P}{\partial y}(x, y) = 0.$$

Изучавање сигуларитета алгебарских криви је посебна област - теорија сингуларитета која има велику примену у многим областима као што је теорија чворова, топологија, комплексна анализа и др.

Како реалне алгебарске криве могу бити јако дегенерисане као нпр. крива

$$x^2 + y^2 = 0$$

која је само тачка $(0, 0) \in \mathbb{R}^2$ и

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

која представља празан скуп у $\mathbb{R}^2$ дошло је до идеје да се уместо реалних посматрају комплексна решења једначине $P(x, y) = 0$. Криве се у $\mathbb{C}^2$ много "боље"понашају, јер крива $x^2 + y^2 = 0$ представља пар комплексних правих које се секу док је крива $x^2 + y^2 = -1$ комплексна кружница.

У XIX веку се уочило да додавањем одговарајућих "тачака у бесконачности"алгебарске криве постају компактни тополошки простори. Тако се и дошло и на идеју да се криве посматрају у пројективним просторима. На компактним просторима је могуће дефинисати мероморфне и холоморфне функције па је се на комплексне алгебарске криве могла применити и комплексна анализа на $\mathbb{C}$. Одавде се развила теорија Риманових површи, које су назване по Берхарду Риману (1826-1866). Риман је био изузетан математичар XIX века који је много утицао на идеје да геометрија не треба изучавати само еуклидске просторе, већ и много генералније просторе.

Дедекинд и Вебер су 1882. показали да већи део теорије алгебарских кривих остаје на снази и над било којим пољем $\mathbb{F}$, тј. криве се више не проучавају само над пољима комплексних и реалних бројева. Тако нпр. у решавању диофантове једначине

$$P(x, y) = 0$$

у теорији бројева често се посматра ова једначина по $\mod p$ где је p прост број. Али ово није ништа друго до посматрање алгебарске криве над пољем $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ или његовим алгебарским затворењем. Ова дубока веза између алгебарских кривих и теорије бројева послужила је и Ендрију Вајлсу у доказу чувене Велике Фермаове теореме да једначина

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

нема целобројна решења у скупу природних бројева када је $n \geq 3$.

Данас доста знамо о алгебарским кривама. *Алгебарски варијетети* су дефинисани као скупови заједничких нула коначног броја полинома у коначно много променљивих и изучавање ових објеката довело је до нових идеја и рађање једне нове математичке дисциплине - *алгебарске геометрије*.

Природно је поставити питање када две алгебарске криве дефинишу исти геометријски скуп тачака. За полином кажемо да је иредуцибилан ако се не може записати као производ два полинома који су оба различита од константе. Одговор на то питање даље чувени Хилбертов Нулштележац.

Теорема 2.1.1 (Хилбертов Нулштеленжац)**.** *$P(x, y)$ и $Q(x, y)$ су полиноми такви да је*

$$\{(x, y) \in \mathbb{C}^2 \mid P(x, y) = 0\} = \{(x, y) \in \mathbb{C}^2 \mid Q(x, y) = 0\}$$

ако и само ако постоје природни бројеви m и n такви да $P \mid Q^m$ и $Q \mid P^n$ тј. ако и само ако P и Q имају исте иредуцибилне факторе.

За полином $P(x,y)$ кажемо да има дупли фактор ако постоји $Q(x,y)$ такав да $(Q(x,y))^2 \mid P(x,y)$. За полиноме који не поседују дупле факторе из Хилбертовог Нулштележаца следи:

Последица 1. *Полиноми $P(x,y)$ и $Q(x,y)$ који немају дупле факторе дефинишу исту комплексну алгебарску криву у $\mathbb{C}^2$ ако и само ако су скаларни множиоци један другог тј.*

$$P(x,y) = \lambda Q(x,y)$$

за неки скалар $\lambda \in \mathbb{C} \setminus \{0\}$.

Дефиниција 2.1.4. *Степен d алгебарске криве $\mathcal{C}$* је степен одговарајућег полинома $P(x,y)$ по x и y који је дефинише тачније степен највећег монома у полиному $P(x,y)$ тј.

$$d = \max\{i+j \mid a_{i,j} \neq 0\},$$

где је $P(x,y) = \sum_{i,j} a_{i,j} x^i y^j$.

Дефиниција 2.1.5. Алгебарска крива степена 1 се назива *права* тј. то је крива дефинисана једначином

$$ax + by + c = 0,$$

за неке комплексне коефицијенте a, b и c и где је бар један од коефицијената a и b различит од 0.

Праве су најједноставније алгебарске криве. Постоје алгебарске криве виших степена које су унија више правих. Описаћемо неке од њих.

Дефиниција 2.1.6. Полином $P(x_1,\ldots,x_n)$ степена d у n променљивих је *хомоген* уколико је за сваки скалар λ

$$P(\lambda x_1,\ldots,\lambda x_n) = \lambda^d P(x_1,\ldots,x_n)$$

или еквивалентно ако је $P(x_1,\ldots,x_n)$ облика

$$P(x_1,\ldots,x_n) = \sum_{i_1+\cdots+i_n=d} a_{i_1,\ldots,i_n} x_1^{i_1}\cdots x_n^{i_n}.$$

Сваки фактор хомогеног полинома је такође хомоген полином. Хомогени полиноми у две променљиве се факторишу на линеарне факторе што показује следећа теорема.

Теорема 2.1.2. *Нека је $P(x,y)$ хомоген ненулти полином степена d, тада се он факторише на производ линеарних полинома тј.*

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

за неке константе α_i, $\beta_i \in \mathbb{C}$.

Доказ. Запишимо

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

где су $a_0, a_1, \ldots, a_d \in \mathbb{C}$. Тада је

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

полином са комплексним коефицијентима једне променљиве $\frac{x}{y}$ који се по основном ставу алгебре потпуно растављa над $\mathbb{C}$ тј.

$$\sum_{r=0}^{d} a_r \left(\frac{x^r}{y^r}\right) = c \prod_{i=1}^{d} \left(\frac{x}{y} - \gamma_i\right)$$

за неке $c, \gamma_1, \ldots, \gamma_d \in \mathbb{C}$. Сада је

$$\begin{aligned} P(x,y) \quad &= y^d \textstyle\sum_{r=0}^{d} a_r \left(\frac{x}{y}\right)^r \quad = \\ &= y^d c \textstyle\prod_{i=1}^{d} \left(\frac{x}{y} - \gamma_i\right) \quad = \\ &= c \textstyle\prod_{i=1}^{d} (x - \gamma_i y) \quad , \end{aligned}$$

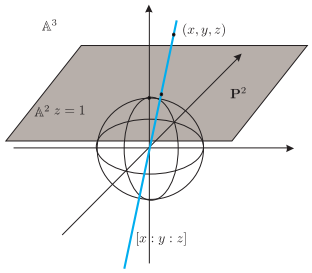
одакле следи тврђење. □

2.1.1 Комплексне пројективне криве

Комплексне алгебарске криве у $\mathbb{C}^2$ називамо афиним, како би их разликовали од пројективних алгебарских кривих. У овом делу ћемо се упознати са пројективним простором, пројективним алгебарским кривама, као и везом између афиних и пројективних кривих.

Дефиниција 2.1.7. Нека је дат афин простор $\mathbb{A}$. *Пројективни простор* $P\mathbb{A}$ је количник простор $\mathbb{A} \setminus \{O\}/\sim$ са количничком топологијом и $\sim$ је релација еквиваленција на $\mathbb{A} \setminus \{O\}$ дефинисана са $x \sim y \Leftrightarrow x = \lambda y$ за неки ненула скалар λ.

Нас специјално интересују реални $\mathbb{R}P^2$ и комплексни пројективни простор $\mathbb{C}P^2$, које ћемо оба зависно од контекста означавати $\mathbf{P}^2$. Ове просторе респективно називамо релна и комплексна пројективна раван. Они настају када се пројективизују као у дефиницији 2.1.7 простори $\mathbb{R}^3$ и $\mathbb{C}^3$. Пројективни простор није лако визуелизовати. Он локално изгледа као $\mathbb{R}^2$ односно $\mathbb{C}^2$. Тачке пројективног простора $\mathbf{P}^2$ су класе еквиваленције уређених тројки (x, y, z) различитих од $(0, 0, 0)$, при чему су две тројке $(x, y, z), (x_1, y_1, z_1) \in \mathbb{A} \setminus \{(0, 0, 0)\}$ еквивалентне $(x, y, z) \sim (x_1, y_1, z_1)$ ако и само ако је $x_1 = \lambda x, y_1 = \lambda y, z_1 = \lambda z$, где је λ ненула скалар, и ту класу еквиваленције обележавамо са $[x : y : z]$ *хомогене координате*. Геометријски гледано, $[x : y : z]$ је права кроз координатни почетак и тачку $(x, y, z) \in \mathbb{A}^3$. Увођење пројективне равни поједностављује питање пресека алгебарских, јер за разлику од равни $\mathbb{A}^2$, у $\mathbf{P}^2$ се сваке две праве секу. У $\mathbf{P}^2$ се може уочити скуп тачака $\{[x : y : 1] | x, y \in \mathbb{A}\}$



Слика 2.2.

који је хомеоморфан са $\mathbb{A}^2$. У овом скупу се налазе скоро све тачке $\mathbf{P}^2$ сем тачака $\{[x : 1 : 0] | x \in \mathbb{A}\} \cup \{[1 : 0 : 0]\}$. Зато је пројективан простор $\mathbf{P}^2$ локално као $\mathbb{R}^2$ односно $\mathbb{C}^2$, тј. то су обични $\mathbb{R}^2$ и $\mathbb{C}^2$ коме су додате "бесконачно далеке"тачке које

леже на једној правој. Интуитивно то је права на којој се налазе пресеци паралелних правих. Због ове повезаности између обичне и пројективне равни сва пројективна тврђења која су тачна у пројективној равни важе и у еуклидском случају.

Сада ћемо показати шта је равна алгебарска крива у $\mathbf{P}^2$. Уколико је равна алгебарска крива $\mathcal{C}$ у $\mathbb{C}^2$ ($\mathbb{R}^2$) задата полиномом $P(x,y) = 0$ степена d, тада је њој одговарајућа пројективна алгебарска крива $\overline{\mathcal{C}}$ задата хомогеним полиномом $\overline{P}(x,y,z) = z^d \cdot P(\frac{x}{z}, \frac{y}{z})$.

Дефиниција 2.1.8. *Пројективна алгебарска крива* $\overline{\mathcal{C}}$ у комплексној равни $\mathbb{C}P^2$ ($\mathbb{C}P^2$) је скуп тачака чије хомогене координате представљају нуле хомогеног полинома $\overline{P}(x,y,z)$, тј.

$$\overline{\mathcal{C}} = \left\{([x,y,z] \in \mathbb{C}P^2 \mid \overline{P}(x,y,z) = 0, \overline{P}(\lambda x, \lambda y, \lambda z) = \lambda^d \overline{P}(x,y,z), \lambda \in \mathbb{C}\right\}.$$

Степен пројективне алгебарске криве је као и код афине криве степен полинома који је дефинише.

Уколико нам је дата пројективна алгебарка крива $\overline{\mathcal{C}}$, а интересује нас њена афина слика $\mathcal{C}$, добићемо једноставно тако што погледамо у $\mathbb{C}^2$ ($\mathbb{R}^2$) скуп тачака $P(x,y) = \overline{P}(x,y,1) = 0$. Афина и пројективна слика јединствено одређују једна другу.

Пример 2.1.2. Праве у пројективном простору имају једначину

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

У пројективној равни се сваке две праве секу у тачно једној тачки. Пројективан простор много погоднији за проучавање алгебарских кривих. Пројективна геометрија је једна лепа математичка теорија која је доста дала математици и њеном развоју.

2.2 Конике

Дефиниција 2.2.1. Алгебарска крива степена 2 назива се *коника*.

Коника $\mathcal{C}$ је геометријско место тачака нула полинома другог степена у две промењљиве $P(x,y) = ax^2 + 2bxy + cy^2 + 2dx + 2ey + f$. У зависности од контекста, у даљем тексту ћемо се користити појмом коника или као геометријским местом тачака или као полиномом који дефинише ту конику.

Коника као скуп тачака у равни нам је добро познат. То су геометријски објекти који су нама познати као елипсе, хиперболе, параболе, парови правих који се секу, парови паралелних правих, праве (дупле), тачке и празни скупови. Ови скупови тачака се доста разликују као што се види на слици 2.3, па се поставља питање који скуп тачака представља коника задана једначином

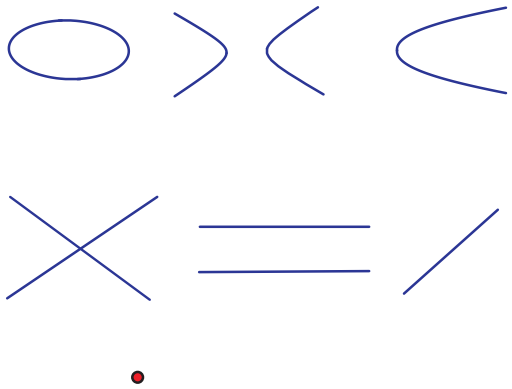
$$P(x,y) = ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0. \tag{2.1}$$

Не губећи на општости можемо претпоставити да је $a \geq 0$.

Теорема 2.2.1 (Метричка класификација коника)**.** *Нека је коника* $\mathcal{C}$ *задана једначином (2.1).*

1. *Ако је* $ac - b^2 \neq 0$ *коника је изометрична некој од крива:* $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 1$ *(елипса),* $\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} = 1$ *(хипербола),* $\frac{x^2}{\alpha^2} = \frac{y^2}{\beta^2}$ *(пар правих који се секу), тачки или празном скупу.*

2. *Ако је* $ac - b^2 = 0$ *(*$a^2 + b^2 + c^2 \neq 0$*) коника је изометрична некој од крива:* $x^2 = 2ry$ *(парабола),* $y^2 = c^2$ *(пар паралелних правих),* $y^2 = 0$ *(дупло линији) или празном скупу.*



Слика 2.3.

Доказ. *1.* Применимо транслацију $x' = x + m, y' = y + n$, и заменом у (2.1) добијамо

$$-f = a(x'-m)^2 + 2b(x'-m)(y'-n) + c(y'-n)^2 + 2(x'-m) + 2(y'-n) =$$

$$ax'^2 + 2bx'y'cy'^2 + 2(-am-bn+d)x' + 2(-bm-cn+e)y' + P(m,n) - f - 2(dm+en).$$

Решавањем система $am + bn = d, bm + cn = e$ по m и n (који због детерминанте овог система $ac - b^2 \neq 0$ има решења), и стављајући

$$g = 2(dm + en) - P(m, n),$$

редукујемо једначину конике на

$$ax'^2 + 2bx'y' + cy^2 = g.$$

Ако је $b = 0$ тада тврђење директно следи. Уколико је $b \neq 0$ ротирајмо цео систем за φ и добијамо нове променљиве

$$x = \tilde{x}\cos\varphi + \tilde{y}\sin\varphi,\ y = -\tilde{x}\sin\varphi + \tilde{y}\cos\varphi.$$

Једначине конике у новим променљивима сада изгледа

$$g = x^2(a\cos^2\varphi - 2b\cos\varphi\sin\varphi + c\sin^2\varphi) +$$

$$xy(a\cdot 2\sin\varphi\cos\varphi + 2b(\cos^2\varphi - \sin^2\varphi) - c\cdot 2\cos\varphi\sin\varphi) +$$

$$y^2(a\sin^2\varphi + 2b\sin\varphi\cos\varphi + c\cos^2\varphi).$$

Уколико изаберемо да φ буде такво да је

$$\frac{(a-c)}{2b} = -\operatorname{ctg} 2\varphi,$$

и средимо једначину доводимо је на облик

$$\frac{x^2}{\alpha^2} \pm \frac{y^2}{\beta^2} = \theta,$$

где је θ једнако 0 или 1. Одавде следи први део тврђења.

Докажимо део под *2.* По претпоставци је $ac = b^2$. Ако је $b = 0$ можемо претпоставити да је $a = 0$ па се (2.1) редукује на

$$cy^2 + 2dx + 2ey = f$$

која се одговарајућом изометријом лако доводи на тражени облик. Ако је $b \neq 0$ можемо претпоставити да су $a, c > 0$. Применимо ротацију за угао φ такав да је

$$\operatorname{tg}\varphi = \sqrt{\frac{a}{c}}.$$

Нове координате су

$$x = \tilde{x}\cos\varphi - \tilde{y}\sin\varphi,\ y = \tilde{x}\cos\varphi + \tilde{y}\cos\varphi.$$

Заменом у једначину конике због избора φ коефицијент уз $\tilde{x}^2$ ће бити 0 и после малог рачуна једначина се сведе на тражени облик. □

Коника је *недегенерисана* уколико је елипса, хипербола или парабола. Уколико је пар правих које се секу, пар паралелних правих или дупла права за конику кажемо да је *дегенерисана*.

Из доказа дела *1.* теореме 2.2.1 добијамо да је коника $\mathcal{C}$ пар правих које се секу ако и само ако систем

$$\begin{aligned} am + bn &= d,\\ bm + cn &= e,\\ dm + en &= f \end{aligned}$$

има ненулта решења. Из доказа дела под *2.* следи да се дегенерисани случај добија ако и само ако је $\frac{d}{\sqrt{a}} = \frac{e}{\sqrt{c}}$ (уз услов да је $ac = b^2$). У оба случаја добијамо да је детерминанта

$$\det\begin{vmatrix} a & b & d\\ b & c & e\\ d & e & f \end{vmatrix} = 0,$$

што је дакле потребан и довољан услов да коника буде дегенерисана.

Теорема 2.2.2. *За 5 тачака у општем положају постоји јединствена коника $\mathcal{C}$ која их садржи.*

Доказ. Без умањења општости, поставимо целу конфигурацију у раван у којој је уведен координатни систем xOy. Применимо афину трансформацију промене координата тако да један пар од тих пет тачака лежи на x-оси, а неки други пар на y-оси. Конкретно, наша афина трансформација треба да слика 5 датих тачака A, B, C, D и E на следећи начин:

$$\begin{aligned} A(x_A, y_A) &\mapsto A_1(0, y_{A_1}),\\ B(x_B, y_B) &\mapsto B_1(0, y_{B_1}),\\ C(x_C, y_C) &\mapsto C_1(x_{C_1}, 0),\\ D(x_D, y_D) &\mapsto D_1(x_{D_1}, 0),\\ E(x_E, y_E) &\mapsto E_1(x_{E_1}, y_{E_1}). \end{aligned}$$

При афиним трансформацијама се полином степена 2 преводи у полином степена 2 у новим координатама Одатле следи да се наша коника $\mathcal{C}$ слика у конику $\mathcal{C}_1(x, y) = a_1x^2 + b_1xy + c_1y^2 + d_1x + e_1y + f_1$. Коефицијенти полинома $\mathcal{C}_1$ можемо сада одредити на основу следецих једнацина:

$$Q(A_1) = 0 \Rightarrow c_1y_{A_1}^2 + e_1y_{A_1} + f_1 = 0,$$

$$Q(B_1) = 0 \Rightarrow c_1y_{B_1}^2 + e_1y_{B_1} + f_1 = 0,$$

$$Q(C_1) = 0 \Rightarrow a_1 x_{C_1}^2 + d_1 x_{C_1} + f_1 = 0,$$
$$Q(D_1) = 0 \Rightarrow a_1 x_{D_1}^2 + d_1 x_{D_1} + f_1 = 0,$$
$$Q(E_1) = 0 \Rightarrow a_1 x_{E_1}^2 + b_1 x_{E_1} y_{E_1} + c_1 y_{E_1}^2 + d_1 x_{E_1} + e_1 y_{E_1} + f_1 = 0.$$

Ових 5 једначина су независне, с обзиром да су прве две независне (Вандермондова детерминанта је различита од 0); друге две по аналогији; првих четири јер немају заједничку непознату и најзад, трећа је једина у којој се јавља непозната b_1. Тиме се гарантује да горњи систем има решење димензије један, тј. сви могући полиноми $\mathcal{C}_1$ су исти до на множење скаларом, а геометријски $\mathcal{C}_1$ и $\lambda\mathcal{C}_1$ одређују јединствену конику.

Пошто је афино пресликавање бијективно, из афине траснформације инверзне почетној, и коефицијената полинома $\mathcal{C}_1(x, y)$, ми можемо одредити коефицијенте почетног полинома $\mathcal{C}(x, y)$ који се анулира у тачкама A, B, C, D и E, чиме је тврђење доказано. □

Теорема 2.2.3. *Свака недегенерисана тј. иредуцибилна коника $\mathcal{C}$ која пролази кроз четири дате тачке A, B, C и D се може представити у облику*

$$\mathcal{C} = \lambda l_{AB} l_{CD} + \mu l_{AC} l_{BD},$$

при чему се са l_{XY} означава права која пролази кроз тачке X и Y тј. полином две променљиве степена један који се анулира на свим тачкама праве XY.

Доказ. Нека је X тачка конике $\mathcal{C}$, која се не налази на правама AB, CD, AC или BD (таква тачка постоји из иредуцибилности посматране криве). Тада је $l_{AB}(X)$, $l_{CD}(X), l_{AC}(X), l_{BD}(X) \neq 0$ одакле следи да постоје λ и μ такви да је

$$\lambda l_{AB}(X) \cdot l_{CD}(X) + \mu l_{AC}(X) \cdot l_{BD}(X) = 0.$$

Нека је сада $\mathcal{C}_1 = \lambda l_{AB} l_{CD} + \mu l_{AC} l_{BD}$. На основу избора λ и μ следи да је $\mathcal{C}_1(A) = 0$, $\mathcal{C}_1(B) = 0, \mathcal{C}_1(C) = 0, \mathcal{C}_1(D) = 0$ и $\mathcal{C}_1(X) = 0$. На основу теореме 2.2.2 постоји јединствена коника која пролази кроз тачке A, B, C, D и X, одакле је до на множење скаларом $\mathcal{C} \equiv \mathcal{C}_1$, чиме је тврђење доказано. □

2.2.1 Паскалова теорема

Теорема 2.2.4 (Паскалова теорема)**.** *Нека је дата коника $\mathcal{C}$, и тачке A, B, C, D, E и F на њој. Тада су пресеци правих AB и DE, BC и EF, AC и DF колинеарни.*

Доказ. На основу теореме 2.2.3 постоје скалари $\lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2$ и μ_3 такви да је:

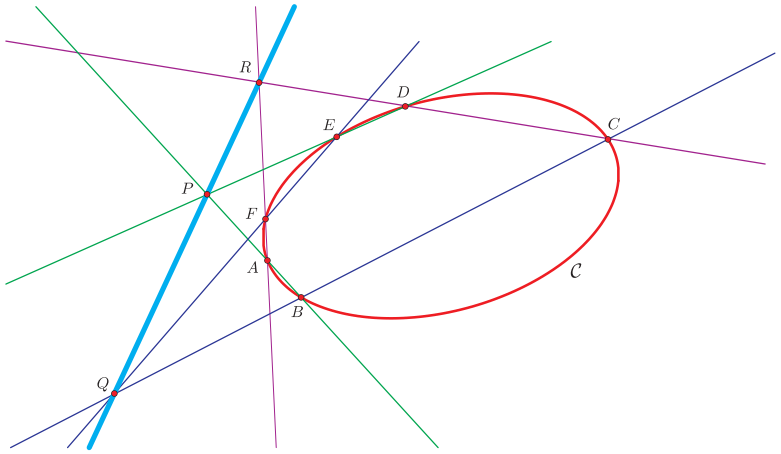
$$\mathcal{C} = \lambda_1 l_{AB} l_{CD} + \mu_1 l_{BC} l_{AD}, \tag{2.2}$$
$$\mathcal{C} = \lambda_2 l_{AF} l_{ED} + \mu_2 l_{AD} l_{EF}, \tag{2.3}$$
$$\mathcal{C} = \lambda_3 l_{BE} l_{CF} + \mu_2 l_{BC} l_{EF}. \tag{2.4}$$

Из (2.2) и (2.3) добијамо:

$$\lambda_1 l_{AB} l_{CD} - \lambda_2 l_{AF} \cdot l_{ED} = (\mu_2 l_{EF} - \mu_1 l_{BC}) \cdot l_{AD}. \qquad (\star)$$

Даље, нека је P тачка пресека правих AB и DE. Тада имамо да је $l_{AB}(P) = 0$ и $l_{ED}(P) = 0$. Замењујући тачку P, тј. њену x и y координату у полиномску једначину $(\star)$ добијамо $(\mu_2 l_{EF}(P) - \mu_1 l_{BC}(P)) \cdot l_{AD}(P) = 0$. С обзиром да P не припада l_{AD} то мора бити $(\mu_2 l_{EF}(P) - \mu_1 l_{BC}(P) = 0$ тј. да X лежи на правој $\mu_2 l_{EF} - \mu_1 l_{BC}$. Слично се добија и да пресек правих CD и AF лежи на $\mu_2 l_{EF} - \mu_1 l_{BC}$, док за пресек BC и EF тврђење очигледно важи. Тиме је теорема доказана. □

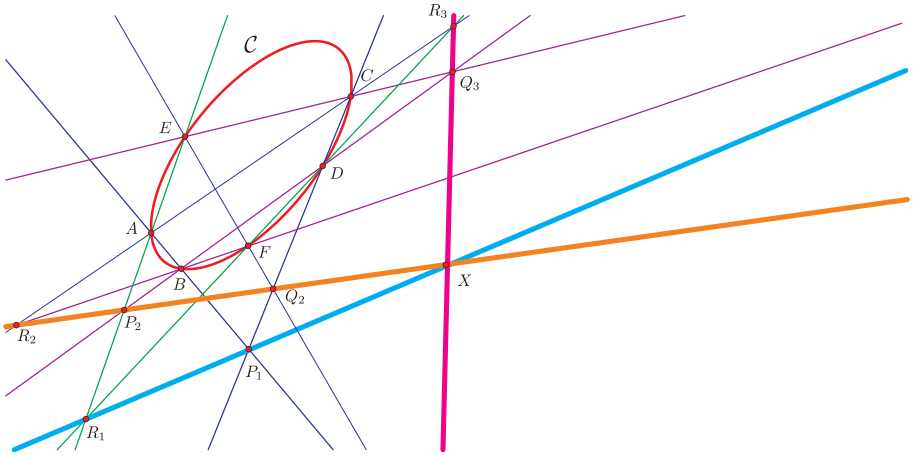
Нотацијска напомена: ово је права добијена применом Пасцалове теореме на шестоугао $ABCDEF$.



Слика 2.4.

Теорема 2.2.5. *Три праве формиране применом Паскалове теореме на шестоуглове* $ABFDCE$, $AEFBDC$ *и* $ABDFEC$ *уписане у недегенерисану конику* $\mathcal{C}$ *се секу у једној тачки.*

Доказ. Из (2.3) и (2.4), као у доказу Паскалове теореме, добијамо да тачке пресека правих AF и BE, ED и CF, AD и BC леже на правој $\mu_2 l_{AD} = \mu_3 l_{BC}$. Слично, из (2.2) и (2.3) следи да тачке пресека правих AB и CF, CD и BE, AD и EF све леже на правој $\mu_1 l_{AD} = \mu_3 l_{EF}$. Сада, остаје да се докаже да се праве $\mu_1 l_{BC} = \mu_2 l_{EF}$, $\mu_2 l_{AD} = \mu_3 l_{BC}$ и $\mu_1 l_{AD} = \mu_3 l_{AF}$ секу у једној тачки.



Слика 2.5.

Међутим, ако се прве две праве секу у тачки Y, онда је $\mu_1 l_{BC}(Y) = \mu_2 l_{EF}(Y)$ и $\mu_2 l_{AD}(Y) = \mu_3 l_{BC}(Y)$ тако да је $\mu_1\mu_2 l_{AD}(Y) = \mu_1\mu_3 l_{BC}(Y) = \mu_2\mu_3 l_{EF}(Y)$, одакле закључујемо да је

$$\mu_1 l_{AD}(Y) = \mu_3 l_{EF}(Y),$$

јер су због претпоставке о неденерисаности конике $\mathcal{C}$ сви коефицијенти $\mu_1, \mu_2, \mu_3, \lambda_1$, λ_2 и λ_3 различити од 0. Овим смо доказали да Y припада трећој правој. □

2.3 Кубике

Дефиниција 2.3.1. Алгебарска крива степена 3 назива се *кубика.*

Кубика $\mathcal{Q}$ је геометријско место тачака нула полинома две променљиве степена три. Као и код коника, у зависности од контекста, под кубиком ћемо сматрати или геометријско место тачака или сам полином.

Њутн је око 1700. потпуно класификовао кубике и описао 72 могућа случаја. Проучавао је сингуларитете кубика тј. тачке у којима крива не изгледа "глатко". Као што се може видети за тачку $(0,0)$ на кубикама $y^2 = x^3 + x$ и $y^2 = x^3$ на слици 2.1 кубика има сингуларитете типа "чвора"и "оштрице"редом. Уколико кубику посматрамо у пројективном простору, многе од ових 72 криве постану еквивалентне једна другој. Поред две поменуте кубике, пројективно гледано кубика дефинисана иредуцибилним полиномом може бити још само еквивалентна несингуларној кубици $y^2 = x(x-1)(x-\lambda)$ где је $\lambda \neq 0, 1$.

Кубике су веома значајне за модерну математику. Читава теорија елиптичких функција и елиптичких интеграла заснована је на својствима ових функција. Многи централни резултати анализе и геометрије везани су за ове криве. Главни део овог рада је управо базиран на једноставној особини кубике и како из ње произилазе неки лепи резултати елементарне геометрије.

3

Теорема о кавезу

Посматрајмо два скупа правих $H = \{h_1, \ldots, h_d\}$ и $V = \{v_1, \ldots, v_e\}$.

Дефиниција 3.0.2. Унија правих H и V $d \times e$ чини *кавез* K. $d \cdot e$ тачака пресека $H \cap V$ су *чворови* или *истакнуте* тачке кавеза.

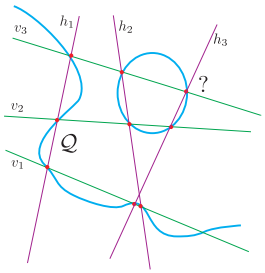
3.1 Теорема о 3×3 кавезу за кубике

Теорема 3.1.1 (Теорема о кавезу за кубике)**.** *Свака кубика која пролази кроз* 8 *истакнутих тачака* 3×3 *кавеза пролази и кроз девету тачку кавеза.*

Доказ. Нека праве h_1, h_2, h_3 и v_1, v_2, v_3 формирају 3×3 кавез. Нека је $\mathcal{Q}$ кубика која пролази кроз 8 тачака кавеза. Желимо да покажемо да ако полином $\mathcal{Q}$ има нуле у 8 тачака кавеза, тада постоје скалари λ и μ такви да је

$$\mathcal{Q} = \lambda h_1 h_2 h_3 + \mu v_1 v_2 v_3.$$

Јасно, уколико бисмо ово доказали, тврђење би било доказано, јер су све тачке кавеза (па и девета) нуле полинома $\lambda h_1 h_2 h_3$ и $\mu v_1 v_2 v_3$.



Слика 3.1.

У ту сврху, направимо пар очигледних обзервација:

1. Рестрикција полинома две промењиве степена d на некој правој је ефективно полином једне промењиве степена највише d.

   Заиста, посматрајмо у шта се слика права $ax + by + c = 0$ полиномом $P(x, y)$. Ако је $b \neq 0$, тада је $y = \frac{-ax-c}{b}$, и $P(x, y) = P(x, \frac{-ax-c}{b})$, дакле полином једне вариабле степена највише d. Ако је $b = 0$ тада је $x = \frac{-c}{a}$ константа и $P(x, y) = P(\frac{-c}{a}, y)$ што је, поново, полином једне вариабле степена највише d.

2. Ако полином једне променљиве $P(x)$ степена d има нуле $\alpha_1, \dots$ и α_d, тада је он облика $P(x) = k(x-\alpha_1)\cdots(x-\alpha_d)$, при чему је k скалар.

3. Вредност полинома $l(x,y) = ax + by + c$ у тачки $M(m_x, m_y)$ једнака је

$$l(M) = \frac{d_M}{\sqrt{a^2+b^2}},$$

где је d_M оријентисано растојање тачке M од праве l.

Орјентисано растојање d_M тачке M од праве l има абсолутну вредност исту као растојање тачке M од праве l, а знак d_m је позитиван (негативан) уколико вектор чији је почетак подножје нормале из тачке M на l, а крај у тачки M, има исти (супротан) смер од вектора (a,b).

Докажимо једну лему.

Лема 3.1.1. *Ако се полином $P(x,y)$ степена d анулира у $d+1$ колинеарних тачака, онда је он инденшички једнак нули на тој правој, а самим тим је и дељив линеарним полиномом којим је дефинисана та права.*

Доказ. Претпоставимо супротно. Обзервација 1) нам каже да је $P(x,y)$ на посматраној правој полином једне вариабле степена највисе d. Сада, на основу основног става алгебре, он може имати највише d нула на тој правој, што је у контрадикцији са нашом претпоставком да их има бар $d+1$.

Нека је $P(x,y) = a_0^d x^d + a_1^d x^{d-1}y + \cdots + a_d^d y^d + a_0^{d-1}x^{d-1} + \cdots + a_0^1 x + a_1^1 y + a_0^0$ и $l = ax + by + c$ права на којој се анулира полином $P(x,y)$. Уколико је $a = 0$ тада је права l облика $y = c$, па полином $P(x,c)$ мора бити 0 за свако x. Како $y - c \mid P(x,y) - P(x,c)$, то због $P(x,c) \equiv 0$, следи $y - c \mid P(x,y)$. Аналогно добијамо и ако је $b = 0$. Можемо претпоставити да је $a, b \neq 0$.

Приметимо да је

$P(x,y) = \frac{a_0^d}{a}x^{d-1}(ax+by+c) + \left(a_1^d - \frac{a_0^d b}{a}\right)x^{d-1}y + \cdots + a_0^0 - \frac{a_0^d c}{a} =$

$b_0^{d-1}x^{d-1}(ax+by+c) + \frac{\left(a_1^d - \frac{a_0^d b}{a}\right)}{a}x^{d-2}y(ax+by+c) + \cdots + a_0^0 - \frac{a_0^d c}{a} - \frac{\left(a_1^d - \frac{a_0^d b}{a}\right)}{a}c =$

$= Q(x,y)\cdot(ax+by+c) + R(y).$

Заправо,

$$P(x,y) = Q(x,y)\cdot(ax+by+c) + R(y),$$

где је $Q(x,y)$ полином две променљиве степена највише $d-1$ и $R(y)$ полином једне променљиве степена највише d.

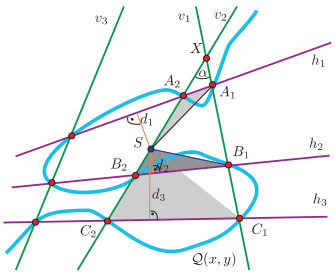
Дакле, за свако x и y такво да је $ax+by+c=0$, мора бити $R(y)=0$. То значи да се $R(y)$ анулира за свако y тј. $R(y) \equiv 0$ чиме је лема доказана. □

Вратимо се доказу теореме. Нека се праве v_1 и v_2 секу у тачки X. Нека је $h_1 \cap v_1 = A_1$, $h_1 \cap v_2 = A_2$, $h_2 \cap v_1 = B_1$, $h_1 \cap v_2 = B_2$, $h_3 \cap v_1 = C_1$, $h_3 \cap v_2 = C_2$. Нека су једначине одговарајућих правих $a_{h_i}x + b_{h_i}y + c_{h_i} = 0$, односно $a_{v_i}x + b_{v_i}y + c_{v_i} = 0$. Сада је на основу обзервације 3) за произвољну тачку S праве v_1 или праве v_2 испуњено:

$$h_1h_2h_3(S) = \sqrt{a_{h_1}^2 + b_{h_1}^2}\sqrt{a_{h_2}^2 + b_{h_2}^2}\sqrt{a_{h_3}^2 + b_{h_3}^2}\,d_1d_2d_3.$$

Међутим, из обрасца за површину троугла је

$$d_1 = \frac{P_{SA_1A_2}}{A_1A_2}, d_2 = \frac{P_{SB_1B_2}}{B_1B_2} \text{ и } d_3 = \frac{P_{SC_1C_2}}{C_1C_2},$$



Слика 3.2.

што нам даје:

$$h_1h_2h_3(S) = \sqrt{a_{h_1}^2 + b_{h_1}^2} \cdot \sqrt{a_{h_2}^2 + b_{h_2}^2} \cdot \sqrt{a_{h_3}^2 + b_{h_3}^2} \cdot \frac{P_{SA_1A_2} \cdot P_{SB_1B_2} \cdot P_{SC_1C_2}}{A_1A_2 \cdot B_1B_2 \cdot C_1C_2}.$$

Сада, уочимо да је $P_{SA_1A_2} = \frac{1}{2} \cdot SA_1 \cdot XA_2 \sin\alpha$ при чему је $\alpha = \angle A_1XA_2$. Сличне формуле важе и за преостале две површине, дајући нам следећу формулу:

$$h_1h_2h_3(S) = \frac{\sqrt{a_{h_1}^2+b_{h_1}^2}\sqrt{a_{h_2}^2+b_{h_2}^2}\sqrt{a_{h_3}^2+b_{h_3}^2}}{A_1A_2 \cdot B_1B_2 \cdot C_1C_2} \cdot SA_1 \cdot SB_1 \cdot SC_1 \cdot XA_2 \cdot XB_2 \cdot XC_2 \sin^3\alpha.$$

Сада, присетимо се прве и друге обзервације. Имамо да је кубика $\mathcal{Q}(x,y)$ на правој v_1 полином $f_1(x) = k_1(x-\alpha_1)(x-\beta_1)(x-\gamma_1)$ при чему се овај полином анулира у тачкама A_1, B_1 и C_1, док је на правој v_2 $f_2(x) = k_2(x-\alpha_2)(x-\beta_2)(x-\gamma_2)$, анулирајући се у тачкама A_2, B_2 и C_2. Уочимо да је $SA_1 \cdot SB_1 \cdot SC_1 = \frac{f(S)}{k_1}$ и да је $XA_2 \cdot XB_2 \cdot XC_2 = \frac{f(X)}{k_2}$.

Из досадашњег дела се закључује да је

$$\frac{h_1h_2h_3(S)}{f(S)} = \frac{\mathcal{Q}(X)\sqrt{a_{h_1}^2 + b_{h_1}^2}\sqrt{a_{h_2}^2 + b_{h_2}^2}\sqrt{a_{h_3}^2 + b_{h_3}^2}}{k_1k_2 \cdot A_1A_2 \cdot B_1B_2 \cdot C_1C_2},$$

израз који не зависи нити од положаја тачке S на правој v_1 нити да ли се та тачка налази на правој v_1 или v_2. Одавде се закључује да је $\frac{f(S)}{h_1h_2h_3(S)}$ исти за све тачке правих v_1 и v_2 различитих од A_1, A_2, B_1, B_2, C_1 и C_2. Дакле, постоји λ тако да се $T(x,y) = \mathcal{Q} - \lambda h_1h_2h_3$ анулира на v_1 и v_2.

Сада смо спремни да докажемо главни део тврђења. Лема 3.1.1 нам каже да је $T(x,y)$ дељив са полиномом v_1v_2, као и да је количник линеаран полином по x и y. Тај количник се анулира још у додатне две тачке кавеза по условима теореме, што нам поново на основу 3.1.1 каже да је овај полином дељив полиномом који се анулира у свим тачкама на правој кроз те две тачке. Овим је тврђење коначно доказано. □

3.1.1 Групни закон на кубици

Елиптичке криве су одиграле велику улогу у математици, поготову у теорији бројева, криптографији, и растављању природних бројева на просте чиниоце. Историјски, допринели су, за почетак, у Andrew Wiles-овом доказу Велике Fermat-ове теореме. Елиптичке криве имају пуно компликованих формула које их описују и пуно дугачких доказа који прате ове карактеризације.

Али, за почетак, шта су уопште елиптичке криве? Постоји више начина на које се оне могу дефинисати. Wolfram их је дефинисао као кубике чија решења у комплексном простору формирају скуп тополошки хомеоморфан торусу. Друга дефиниција елиптичких криви карактерише их као несингуларне кубике по две променљиве из

неког поља, наиме $f(x, y)$. Елиптичка крива над пољима као што су $\mathbb{R}$ или $\mathbb{Q}$ може бити записана у облику

$$y^2 = x^3 + ax + b \ \text{ (Weierstrass-ова једначина);}$$

такође може бити записана и у Legendr-овој форми:

$$y^2 = x(x-1)(x-\lambda).$$

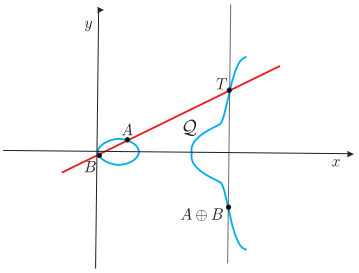
Још један начин на који се може представити елиптичка крива јесте пресек површи $z = x^3 - ay^2 + bxy^2 + cx^2y$ са равни $z = Ax + B$. Надаље, ми ћемо се бавити само елиптичким кривама над $\mathbb{R}$ или $\mathbb{Q}$.

Такође, подсетимо се шта је група. Група G је скуп на коме је дефинисана бинарна операција $\oplus$ са следећим својствима

1. *(затворености)* за свака два елемента $a, b \in G$ је $a \oplus b \in G$;
2. *(асоцијативности)* за свака три $a, b, c \in G$ важи
$$(a \oplus b) \oplus c = a \oplus (b \oplus c);$$
3. *(неутрални елемент)* постоји елемент $e \in G$, такав да је
$$a \oplus e = e \oplus a = a$$
за сваки елемент $a \in G$;
4. *(инверзни елемент)* за сваки $a \in G$ постоји $a^{-1} \in G$ такав да је
$$a \oplus a^{-1} = a^{-1} \oplus a = e;$$

Сада ћемо дефинисати сабирање на кубици и показати да оно задовољава особине групе.

Дефиниција 3.1.1. За произвољне две тачке A и B елиптичке криве $\mathcal{Q} : y^2 = x^3 + ax + b$ дефинишемо сабирање $A \oplus B$ на следећи начин: $A \oplus B$ је тачка C која је тачка симетрична тачки T која је пресек праве AB са елиптичком кривом $\mathcal{Q}$, у односу на x-осу.

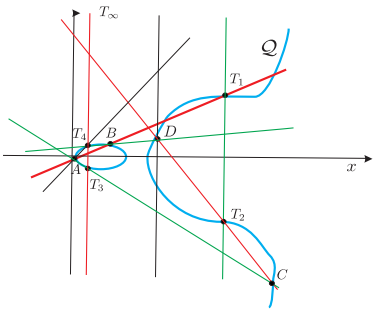


Слика 3.3.

Уверимо се сада да овако дефинисана операција на елиптичкој криви заиста чини групу:

1. *(затворености)* као прво уочимо да је рестрикција елиптичке криве, као кубике, на правој полином степена 3 или нула полином. Из тог разлога је тачка T из дефиниције добро дефинисана. Наиме, тачке A и B из дефиниције су нуле неког полинома једне променљиве степена 3. Из тог разлога он има и трећу нулу на правој AB одакле тврђење следи. Са друге стране, из једначине криве видимо да је она симтерична у односу на x-осу. Сходно томе тачка C припада елиптичкој криви, што је и требало показати.

2. *(асоцијативности)* Овај део је заправо ништа друго но замаскирана теорема о кубикама коју смо раније доказали. Наиме да бисмо се уверили да асоцијативност овакве операције важи, посматрајмо збир три тачке A, B и C тим редоследом. Даље, нека је $AB \cap \mathcal{Q} = T_1$, $A \oplus B = T_2$, $AC \cap \mathcal{Q} = T_3$, $A \oplus C = T_4$ и најзад $T_2C \cap T_4B = D$. Јасно, тражи нам се да покажемо да је у ствари сада тачка D на овој кубици. Применимо теорему о кубикама на $h_1 = D - B - T_4$, $h_2 = A - C - T_3, h_3 = T_\infty - T_1 - T_2$ и $v_1 = A - B - T_1, v_2 = D - C - T_2$, $v_3 = T_\infty - T_4 - T_3$, при чему је T_∞ тачка у бесконачности. Јасно, тачке T_∞, $A, B, C, T_1, T_2, T_3, T_4$ и T_∞ леже на кубици па у складу са теоремом лежи и тачка D.



Слика 3.4.

3. *(неутрални елемент)* Јасно, тачка у бесконачности задовољава потребне услове. Наиме пресек праве која садржи бесконачну тачку и неку тачку кубике A је нормална на x-осу и други пут сече кубику у тачки која је симетрична тачки A у односу на x-осу.

4. *(инверзни елемент)* Такође, инверз било које тачке је тачка симетрична њој у односу на x-осу.

3.2 Генерална теорема о кавезу

Сваки полином $P(x, y)$ степена d у $\mathbf{P}^2$ постаје хомоген полином по x, y и z степена d, тако што је сваком моному $x^a y^b$ у $P(x, y)$ моном $x^a y^b z^{d-a-b}$. Афина алгебарска крива у $\mathbb{A}^2$ је скуп нула полинома по x и y, док је пројективна крива у пројективном просотру $\mathbf{P}^2$ скуп нула хомогеног полинома по x, y и z. Степен криве је степен полинома који је дефинише. Такође, два пропорционална полинома дефинишу идентичну криву. Из тог разлога, видимо да је скуп класа полинома по x и y степена d до на пропорционалност бијективно кодиран скупом крива степена d у афиној равни. Слично, скуп класа пропроционалности хомогених полинома по x, y и z степена d је скуп пројективних криви степена d у $\mathbf{P}^2$.

Полином $P(x, y)$ степена не више од d има $1 + 2 + 3 + \cdots + (d + 1) = \frac{(d+1)(d+2)}{2}$ коефицијената. Такви полиноми, до на коефицијент пропорционалности који је однос

њихових водећих коефицијената, чине n-димензионални пројективни простор $\mathbf{P}^n$ где је $n = \frac{(d+1)(d+2)}{2} - 1 = \frac{d^2+3d}{2}$. Његове тачке су класе пропорционалности низа коефицијената полинома $P(x, y)$.

Када је $k < d$, полиноми по x и y степена највише k су садржани у скупу полинома степена највише d. Као последицу имамо фамилију појективних подпростора

$$\{{\mathbf{P}_*}^{\frac{k^2+3k}{2}}\}_{0 \leq k \leq d}.$$

Тако, на пример, фамилија:

$${P_*}^0 \subset {\mathbf{P}_*}^2 \subset {\mathbf{P}_*}^5 \subset {\mathbf{P}_*}^9 \subset {\mathbf{P}_*}^{14} \subset {\mathbf{P}_*}^{20}$$

одговара полиномима $P(x, y)$ степена 0 и највише $1, 2, 3, 4$ и 5, редом. Афине криве степена d у $\mathbb{A}^2$ формирају отворен скуп

$${\mathbf{P}_*}^{\frac{d^2+3d}{2}} \setminus {\mathbf{P}_*}^{\frac{(d-1)^2+3(d-1)}{2}}$$

у простору ${\mathbf{P}_*}^{\frac{d^2+3d}{2}}$. На пример, у овом моделу, кубике у $\mathbf{P}^2$ су кодиране тачкама у $\mathbf{P}^9_*$, док су кубике у $\mathbb{A}^2$ кодиране скупом $\mathbf{P}^9_* \setminus \mathbf{P}^5_*$.

Следи нам циљ да опишемо полиноме P степена d који се анулирају у чворовима датог $(d \times e)$ кавеза K, при чему је $d \geq e$. Форсирајући полином P да се анулира у датој тачки пројективне равни, ми намећемо линеарну рестрикцију над његовим коефицијентима. Више тачака, наравно, даје више ограничења које могу да смање димензију векторског простора тих полинома. Ако степени полинома нису ограничени одозго, различите тачке ће наметати независне услове. Међутим, када су степени ограничени, нове тачке често додају сувишне услове или рестрикције тј. релације које су последице претходних услова. На пример, на основу пређашње дискусије се може очекивати да полином $P(x, y)$ степена највише d и који се анулира у $\frac{d^2+3d}{2}$ тачака је потпуно одређен до на пропорционалност. Пошто $(d \times d)$ кавез има d^2 чворова, неки од њих мора да дају непотребне тј. зависне услове за коефицијенте полинома $P(x, y)$ (наравно под условом да је $d \geq 3$).

Овде се сада намеће кључно питање: који чворови $(d \times e)$ кавеза су непотребни, и како можемо описати варијитет полинома који се анулирају у датим чоровима? Неколико комбинаторних дефиниција ће нам помоћи. Као и раније, обојићемо два скупа линија које формирају кавез плавом и црвеном бојом. За било који поредак црвених линија $\{R_1, R_2, \ldots, R_d\}$ и плавих $\{B_1, B_2, \ldots, B_e\}$, ми ћемо означити са p_{ij} пресечну тачку $R_i \cap B_j$.

Дефиниција 3.2.1. За подскуп $\mathcal{A}$ скупа чворова $(d \times e)$ кавеза, казаћемо да је:

1. *тријангуларан* ако је у односу на неко преуређење црвених и плавих линија које формирају кавез $\mathcal{A}$ облика $\{p_{ij}\}_{i+j \leq d}$;

2. *квази-тријангуларан* ако кардиналност чворова у $\mathcal{A}$ који леже на плавој линији иде од d до $d - e + 1$ и узима сваку средњу вредност тачно једном;

3. *супер-тријангуларан* ако је у односу на неко преуређење црвених и плавих правих које формирају кавез $\mathcal{A}$ облика $\{p_{ij}\}_{i+j \leq d+1}$;

4. *супер-квази-тријангуларан* ако кардиналност скупа тачака у $\mathcal{A}$ које леже на плавој линији иде од d до $d - e + 2$, при чему је вреднсот d достигнута на две праве, а свака од $d - 1$ до $d - e + 2$ је достигнута тачно једном.

Сада смо спремни да реформулишемо генерализацију теореме о кубици.

Теорема 3.2.1 (Теорема о кавезу за равне криве)**.**

1. *Ако крива у* $\mathbf{P}^2$ *степена* d *пролази кроз супер-квази-троугаони скуп* $\mathcal{A}$ *чворова* $(d \times e)$*-кавеза са* $d \geq e$*, онда пролази и кроз све остале чворове кавеза.*

2. *Ни једна крива степена мањег од* e *не може да прође кроз квази-троугаони скуп чворова* $(d \times e)$*-кавеза са* $d \geq e$*.*

Доказ. Доказаћемо теорему за кавезе у $\mathbb{A}^2$. Аргумент за $\mathbf{P}^2$ је сличан. За доказ прве ставке, преуредимо плаве праве тако да прве две плаве праве садрже по d чворова, трећа $d-1$ чворова, четврта $d-2$, ..., до последње праве, која садрзи $d-e+2$ чворова.

Нека је R_i линеаран полином по x и y, чији је нула скуп права R_i и нека је B_i полином чији је нула скуп права B_i. Даље, нека је $R = \prod_{i=1}^{d} R_i$ и $B = \prod_{j=1}^{e} B_j$. Тада, било која линеарна комбинација $S_{\lambda,\mu} := \lambda R + \mu B$ се анулира у свим чворовима кавеза. Нека је $S_{[\lambda:\mu]}$ крива степена d дефинисана једначином $S_{\lambda,\mu} = 0$. Ова крива зависи од избора полинома R и B који чине кавез. Међутим, фамилија $\{S_{[\lambda:\mu]}\}$ тих криви је потпуно одређена кавезом.

Нека је P било који полином степена највише d који се анулира у чворовима из $\mathcal{A}$. Као и код доказа теореме о кубикама, циљ нам је да докажемо да за погодне бројеве λ и μ и неки полином Q, да је P облика $\lambda R + \mu B \cdot Q$, и према томе мора да се анулира у свакој тачки.

Даљи део доказа ће бити спуст по степену полинома. Упоредимо рестрикције P и $S_{\lambda,\mu}$ на плавој правој B_1. Пошто су обе рестрикције полиноми по једној вариабли степена највише d, они деле заједнички скуп од d нула, тј. чворова $p_{11}, p_{12}, \ldots, p_{1d}$. Одавде следи да морају бити пропорционални. Бирањем погодног $\lambda = \lambda_*$, ми намештамо да је $P - S_{\lambda_*,\mu}$ идентички нула на правој R_1. Пошто је B_1 иредуцубилан полином, $P - S_{\lambda_*,\mu}$ је дељив са B_1. Према томе, $P = S_{\lambda_*,\mu} + B_1 \cdot P_1$ при чему је P_1 полином степена највише $d-1$. Пошто су сви чворови скупа $\mathcal{A}$ различити, P_1 мора да се анулира у свих d чворова $A \cap B_2$, с обзиром да је B_1 ненула на $A \cap B_2$. Следи да је рестрикција P_1 на правој B_2 идентички једнака нули. Из сличних разлога као малопре, P_1 је дељиво са B_2. Исходни полином P је сада облика $P = S_{\lambda_*,\mu} + (B_1 B_2) \cdot P_2$, при чему је P_2 полином степена највише д-2. Овај поступак може да се настави све док не добијемо да је $P = S_{\lambda_*,\mu} + (B_1 B_2 \ldots B_e) \cdot P_e$ при чему је P_e степена $d-e$. Дакле, P је облика $\lambda_* R + B \cdot Q$. Такође, овде се лако уочава да у случају када је $e = d$, ми добијамо $P = S_{\lambda_*,\mu_*}$

Доказ друге ставке је још лакши. Нека је Q полином степена мањег од e који се анулира на квази-троугаоном скупу T чворова кавеза. Онда, по аргументу сличном који смо малопре изложили, његова рестрикција на било којој плавој правој мора да буде идентички једнака нули: за одговарајуће P_m, број корена на B_m премашује његов степен. Према томе, Q мора да буде дељиво са $B_1 B_2 \ldots B_e$, што је једино могуће када је Q идентички једнак нули. Контрадикција. □

3.3 Безуова теорема

Безуова теорема је суштински прво била истакнута од стране Исака Њутна у доказу 28. леме првог тома своје књиге *Principia*, где тврди да је број заједничких тачака две алгебарске криве једнак производу њихових степена. Ова теорема је касније објављена 1779. у Ètienne Bézout-овој *Théorie générale des équations algébrique*. Безу, који није имао на свом располагању модерну алгебарску нотацију за једначине са више променљивих, је дао доказ заснован на манипулацији гломазних алгебарских израза. Са модерне тачке гледишта, његова обрада овог материјала је била хеуристичка, јер

није прецизно формулисао услове под којим теорема важи. У ту сврху, започећемо овај део дефиницијом *мултиплицитета пресека*, тачније само трансверзалног пресека.

Дефиниција 3.3.1. Ако је P заједничка тачка две равне алгебарске криве $\mathcal{X}$ и $\mathcal{Y}$ која је несингуларна (нису сви парцијални изводи у тој тачки једнаки 0) за обе криве, и штавише тангентне праве на $\mathcal{X}$ и $\mathcal{Y}$ у P су различите, онда је мултиплицитет пресека 1 и ово се назива *трансверзални пресек*. Ако криве $\mathcal{X}$ и $\mathcal{Y}$ имају заједничку тангенту у P, тада је овај пресек мултиплицитета барем 2. Интуитивно, то је степен поклапања кривих $\mathcal{X}$ и $\mathcal{Y}$ у тачки P.

Сада наводимо Безуову теорему у пуној генералности, без доказа. Ова теорема је класичан резултат теорије алгебарских кривих.

Теорема 3.3.1 (Безуова теорема)**.** *Нека су $\mathcal{X}$ и $\mathcal{Y}$ две пројективне криве дефинисане над пољем $\mathbb{F}$ које немају заједничку компоненту(овај услов важи ако су и $\mathcal{X}$ и $\mathcal{Y}$ дефинисане различитим иредуцибилним полиномима). Тада је укупан број тачака пресека $\mathcal{X}$ и $\mathcal{Y}$ са координатама у алгебарски затвореном пољу $\mathbb{E}$ које садржи $\mathbb{F}$, рачунајући мултиплицитете, једнак производу степена $\mathcal{X}$ и $\mathcal{Y}$.*

Сада, наводимо једну последицу Безуове теореме, специјалан случај Безуове теореме. Њен специјалан случај је теорема о кубикама, која је толико обилато искоришћена у овом раду.

Последица 2. *Нека две пројективне криве $\mathcal{C}$ и $\mathcal{D}$ у $\mathbf{P^2}$ имају тачно n^2 тачака пресека и нека mn од њих леже на иредуцибилној криви $\mathcal{E}$ степена $m < n$. Тада преосталих $n(n-m)$ тачака леже на кривој степена највише $n-m$.*

Доказ. Нека су $\mathcal{C}$, $\mathcal{D}$ и $\mathcal{E}$ криве дефинисане хомогеним полиномима $P(x,y,z)$, $Q(x,y,z)$ и $R(x,y,z)$ редом. Нека тачка $[a:b:c]$ на $\mathcal{E}$ не лежи на $\mathcal{C}\cap\mathcal{D}$. Тада крива степена n дефинисана полиномом

$$\lambda P(x,y,z) + \mu Q(x,y,z),$$

где је $\lambda = Q(a,b,c)$, $\mu = -P(a,b,c)$, сече E у барем $mn+1$ тачака (конкретно у $[a:b:c]$ и mn тачака које леже на $C\cap D$ по претпоставци). Одавде следи, на основу обрнуте Безуове теореме, да ова крива и E морају имати заједничку компоненту, која са друге стране мора бити E, јер је E иредуцибилна. Према томе,

$$\lambda P(x,y,z) + \mu Q(x,y,z) = R(x,y,z)\cdot S(x,y,z),$$

за неки неконстантан хомоген полином $S(x,y,z)$ степена не већег од $n-m$. Према томе, ако $[u:v:w]\in\mathcal{C}\cap\mathcal{D}$ тада или је $R(u,v,w)=0$ или $S(u,v,w)=0$. Одавде следи да $n(n-m)$ тачака $\mathcal{C}\cap\mathcal{D}$ које не леже на $\mathcal{E}$ морају лежати на кривој дефинисаној полиномом $S(x,y,z)=0$. □

4

Примене теореме о кавезу

У овом поглављу ћемо осветлити дубоку везу између алгебарске геометрије равних алгебарских кривих и класичних теорема пројективне геометрије. Показаћемо и неколико нових тврђења који произилазе из тврђења теорема које смо доказали у претходним поглављама.

Blaise Pascal је 1640. као шестогодишњак уочио да шестоугао уписан у круг има својство да три тачке добијене као пресеци парова наспрамних страница увек припадају једној правој. Ово својство је назвао "Тајанствени шестоугао"и послао га је водећим математичарима тога доба. Убрзо после тога је уочио да исто својство има шестоугао који је уписан у елипсу. Овај резултат је био један од првих фундаменталних резултата који није био познат античким Грцима. За Дезарговом теоремом која је доказана четири године раније, довео је до рађања једне нове неметричке геометрије - пројективне геометрије. Пројективна геометрија у класичном смислу је достигла свој врхунац у XIX веку са чувеним Понселеовим резултатом - теореми о Понселеовом поризму, али лепота ових тврђења привлачи и даље пажњу математичке јавности и представљају мотив за истраживање у модерним математичким дисциплинама.

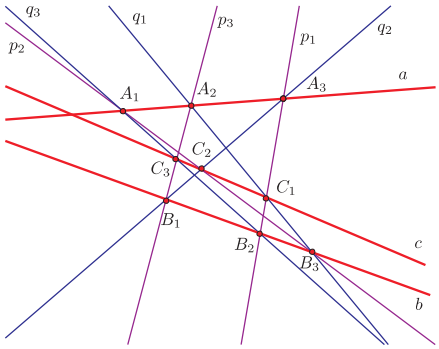
Blaise Pascal

Паскалова, Дезаргова, Бријаншонова и Папусова теорема представљају класивне теореме пројективне геометрије. Специјално, оне важе и у еуклидској равни. Постоје и докази које користећи Менелајеву и Чевијеву теорему доказују ова тврђења за еуклидски случај. Иако формулација Паскалове, Бријаншонове и Папусове теореме, као и слична техника доказа наслућују дубоку везу међу њима. Дуалност у пројективној геометрији успоставља везу међу Бријаншонове и Паскалове теореме. Пројективна геометрија и велика слобода која она даје довела је до неколико нових доказа ових тврђења. Могућност да се пројективим трансформацијама прелази из Бријаншонове, Папосове и Паскалове конфигурације пређе у неке специјалне (нпр. шестоугао са паралелним наспрамним страницама, превођење коника у кругове) је ставила ове теореме у један контекст и успоставила чвршћу везу између њих. Духовити докази Паскалове и Папосове теореме који произилазе као последица теореме о девет тачака ово теореме виде у једном јединственом светлу, као специјалне случајеве овог тврђења.

4.1 Папосова теорема

Теорема 4.1.1 (Папосова теорема)**.** *Нека су A_1, A_2 и A_3 тачке на правој a и B_1, B_2 и B_3 тачке на правој b. Праве A_1B_2 и A_2B_1 секу се у тачки C_3, праве A_2B_3 и A_3B_2 секу се у тачки C_1 и праве A_3B_1 и A_1B_3 секу се у тачки C_2. Тада су тачке C_1, C_2 и C_3 колинеарне.*

Доказ. Означимо са p_1, p_2 и p_3 праве A_3B_2, A_1B_3 и A_2B_1, а са q_1, q_2 и q_3 праве B_3A_2, B_1A_3 и B_2A_1 редом. Нека је c права C_1C_2. Подразумевамо да су и полиноми који задају одговарајуће праве означени исто као и праве. Праве p_1, p_2 и p_3 са правама q_1, q_2 и q_3 формирају кавез 3×3 чији су 9 одговарајућих тачака $A_1, A_2, A_3, B_1, B_2, B_3$, C_1, C_2 и C_3.



Слика 4.1.

Посматрајмо дегенерисану кубику $a \cdot b \cdot c = 0$. Геометријски се састоји од 3 праве a, b и c, а алгебарски је abc полином трећег степена. Ова кубика пролази кроз A_1, A_2, A_3 (права a), B_1, B_2, B_3 (права b) и C_1, C_2 (права c), тј. пролази кроз 8 тачака кавеза, а по теореми мора проћи и кроз девету, C_3. Како C_3 није ни на правој a ни на правој b то C_3 лежи на правој c. □

Приметимо да у доказу Папосове теореме нисмо нигде користили поредак тачака на правама a и b. Зато тврђење остаје на снази за било који распоред тачака. Праве које се појављују из Папосових конфигурација $A_1\ A_2\ A_3\ B_1\ B_2\ B_3$, $A_1\ A_2\ A_3\ B_2\ B_3\ B_1$ и $A_1\ A_2\ A_3\ B_3\ B_1\ B_2$ имају једно лепо својство које је исказано у следећој теореми.

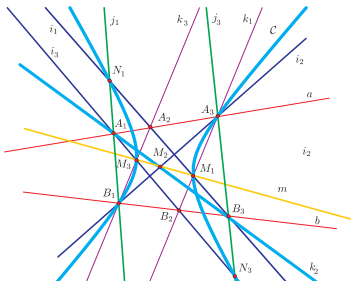
Теорема 4.1.2. *Праве које се појављују из Папосових конфигурација $A_1\ A_2\ A_3\ B_1\ B_2\ B_3$, $A_1\ A_2\ A_3\ B_2\ B_3\ B_1$ и $A_1\ A_2\ A_3\ B_3\ B_1\ B_2$ секу се у једној тачки.*

Доказ. Означимо са i_1, i_2, i_3 праве A_2B_3, A_3B_1 и A_1B_2 редом, са j_1, j_3 праве A_1B_1 и A_3B_3 редом и са k_1, k_2, k_3 праве B_2A_3, B_3A_1 и B_1A_2 као и одговарајуће полиноме који дефинишу ове праве. Нека је M_1 пресечна тачка правих i_1 и k_1, M_2 пресечна тачка правих i_2 и k_2, M_3 M_2 пресечна тачка правих i_3 и k_3, N_1 пресечна тачка правих i_1 и j_1 и тачка N_3 прсечна тачка правих i_3 и j_3. Према Папосовој теореми тачке M_1, M_2 и M_3 леже на једној правој m. Доказаћемо једну лему.

Лема 4.1.1. *Тачке M_1, M_3, N_1, N_3, A_3 и B_1 леже на једној коници.*

Доказ. Праве i_1, i_2 и i_3 са правама m, j_1 и j_3 формирају кавез 3×3 са истакнутим тачкама $M_1, M_2, M_3, N_1, N_3, A_1, A_3, B_1$ и B_3.

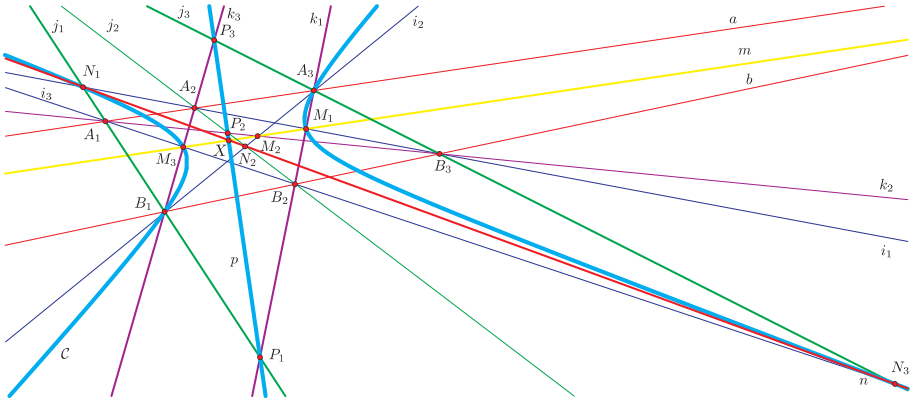
Постоји јединствена коника $\mathcal{C}$ која пролази кроз 5 тачака A_3, M_1, M_3, B_1 и N_3. Кубика $k_2 \cdot \mathcal{C} = 0$ састоји се од конике $\mathcal{C}$ и праве k_2 на којој су тачке A_1, B_3 и M_2 па



Слика 4.2.

пролази кроз 8 од 9 тачака кавеза. По теореми мора садржати и девету тачку N_1 која не припада правој k_2. Зато коника $\mathcal{C}$ пролази и кроз тачку N_1. □

Вратимо се сада тврђењу које желимо докажемо. Нека је N_2 пресечна тачка правих i_2 и j_2, P_1 пресечна тачка правих j_1 и k_1, P_2 пресечна тачка правих j_2 и k_2 и P_3 пресечна тачка правих j_3 и k_3.



Слика 4.3.

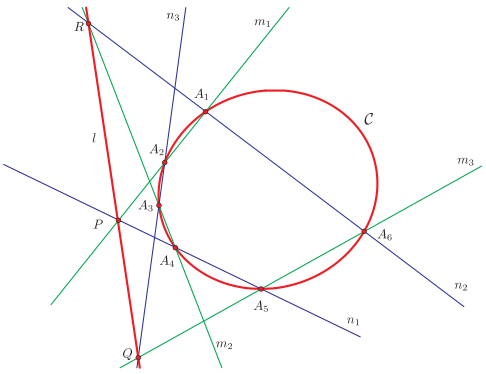
Према Папосовој теореми, тачке N_1, N_2 и N_3 леже на једној правој n, а тачке P_1, P_2 и P_3 леже на правој p. Нека се праве m и n секу у тачки X. Према леми 4.1.1 тачке M_1, M_3, N_1, N_3, A_3 и B_1 леже на једној коници, па применом Паскалове теореме на шестоугао $A_3M_1M_3B_1N_1N_3$ добијамо да су тачке P_1, P_3 и X колинеарне, тј. тачка X припада правој p. □

4.2 Паскалова теорема

Теорема 4.2.1 (Паскалова теорема)**.** *Нека су A_1, A_2, A_3, A_4, A_5 и A_6 шест тачака на конициС. Праве A_1A_2 и A_4A_5 секу се у тачки P, праве A_2A_3 и A_5A_6 секу се у тачки Q, а праве A_3A_4 и A_6A_1 секу се у тачки R. Тада су тачке P, Q и R колинеарне.*

Доказ. Нека су m_1, m_2 и m_3 праве A_1A_2, A_3A_4 и A_5A_6 редом, а n_1, n_2 и n_3 праве A_4A_5, A_6A_1 и A_2A_3 редом. Нека је l права PQ. Праве n_1, n_2 и n_3 са правама m_1, m_2 и m_3 формирају 3×3 кавез чијих су 9 одговарајућих тачака A_1, A_2, A_3, A_4, A_5, A_6, P, Q и R.

Посматрајмо кубику $l \cdot \mathcal{C} = 0$ која се састоји од праве l и конике $\mathcal{C}$. Ова кубика пролази кроз A_1, A_2, A_3, A_4, A_5 и A_6 (коника $\mathcal{C}$) и P и Q (права l), па мора проћи и кроз девету тачку R, која не припада $\mathcal{C}$. Дакле, R лежи на правој l. □



Слика 4.4.

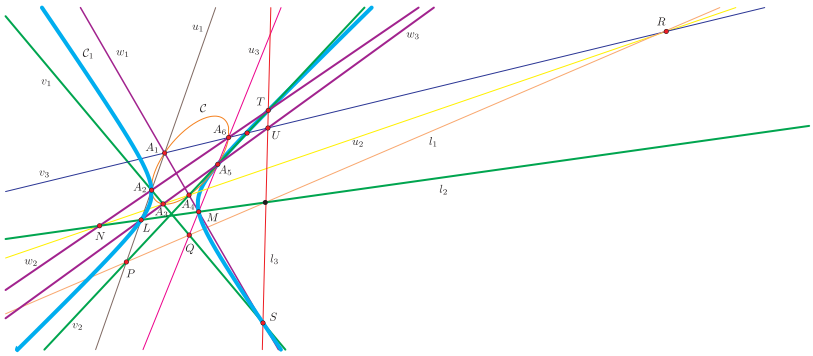
Редослед 6 тачака на коници може произвести различите праве, које називамо *Паскаловим* правама. Њих има 60, а неке од њих се секу у једној тачки. Ово смо већ видели у теореми 2.2.5, али сада ћемо га доказати на другачији начин.

Теорема 4.2.2 (Штајнерова теорема)**.** *Нека су A_1, A_2, A_3, A_4, A_5 и A_6 шест тачака на коници $\mathcal{C}$. Паскалове праве шестоуглова $A_1A_2A_3A_4A_5A_6$, $A_1A_2A_6A_5A_3A_4$ и $A_1A_4A_5A_3A_2A_6$ секу се у једној тачки.*

Доказ. Означимо са u_1, u_2 и u_3 праве A_1A_2, A_3A_4 и A_6, са v_1, v_2 и v_3 праве A_2A_3, A_4A_5 и A_6A_1, са w_1, w_2 и w_3 праве A_1A_4, A_2A_6 и A_3A_5. Означимо са P пресек u_1 и v_2, са Q пресек u_3 и v_1, са R пресек u_2 и v_3, са L пресек u_1 и w_3, са M пресек u_3 и w_1, са N пресек u_2 и w_2, са S пресек v_1 и w_1, са T пресек v_2 и w_2, са U пресек v_3 и w_3. Праве које садрже тројке тачака P, Q, R; L, M, N; S, T, U означимо редом са l_1, l_2 и l_3. Нека је X пресечна тачка правих l_2 и l_3.

Докажимо за почетак следећу лему.

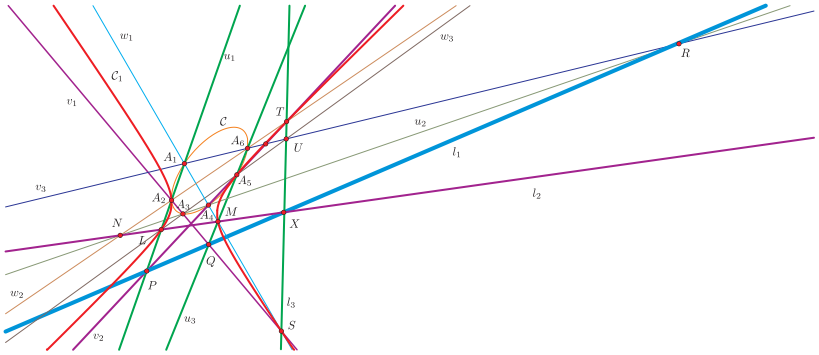
Лема 4.2.1. *Тачке A_2, A_5, L, M, S и T леже на једној коници.*



Слика 4.5.

Доказ. Праве v_1, v_2 и l_2 са правама w_1, w_2 и w_3 формирају кавез 3×3 са истакнутим тачкама $A_2, A_3, A_4, A_5, L, M, N, S$ и T. Нека је $\mathcal{C}'$ коника која пролази кроз A_5, L, M, S и T. Кубика $\mathcal{C}' \cdot u_2 = 0$ пролази кроз 8 тачака кавеза, па мора и A_2 лежати на $\mathcal{C}'$. □

Вратимо се сада тврђењу које желимо да докажемо. Праве u_1, u_3 и l_3 са правама v_1, v_2 и l_2 формирају 3×3 кавез са истакнутим тачкама $A_2, A_5, L, M, P, Q, S, T$ и X.



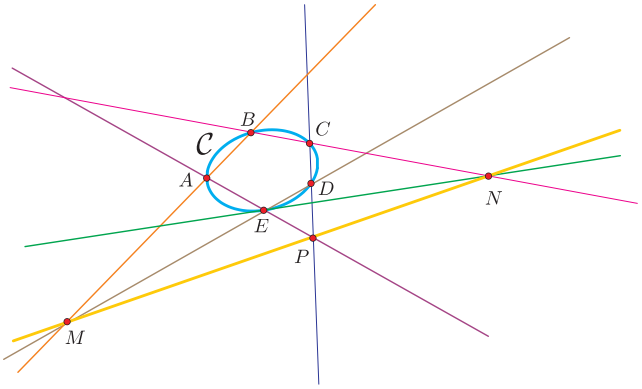
Слика 4.6.

Према леми 4.2.1 тачке A_2, A_5, L, M, S и T леже на коници $\mathcal{C}'$, па кубика $\mathcal{C}' \cdot l_1 = 0$ пролази кроз 8 тачака кавеза. Ово значи да преостала тачка X лежи на правој l_1 чиме је тврђење доказано. □

4.2.1 Дегенерисани случајеви

Паскалова теорема коју смо доказали важи за шестоуглове уписане у конику. Она је још генералнија јер ако у шестоуглу $ABCDEF$ уписаном у конику $\mathcal{C}$ тачка $F \to E$, тада права FE тежи тангенти у тачки E, тј. примена Паскалове теореме на $ABCDEF$ кад $F \to A$ се може схватити као примена на шестоугао $ABCDEE$ тј. дегерацијом добијамо следећу последицу.

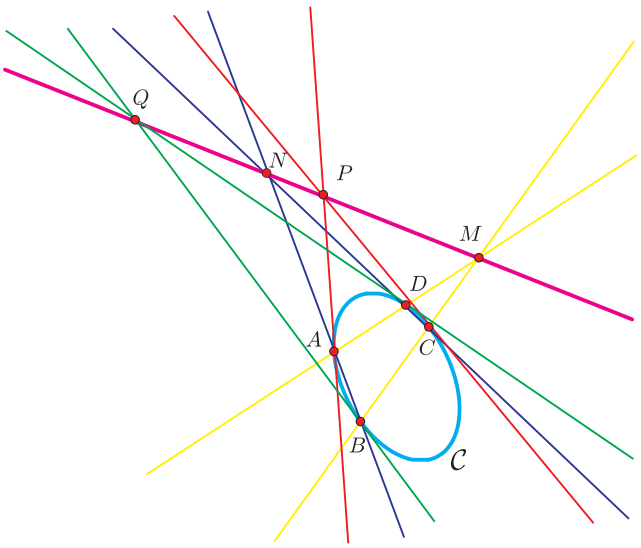
Последица 3. *Нека је $ABCDE$ петоугао уписан у конику $\mathcal{C}$ и нека је тачка M пресек правих AB и DE, тачка N пресек праве BC и тангенте на конику $\mathcal{C}$ у тачки E и тачка P пресек правих CD и AE. Тада су тачке M, N и P колинеарне.*



Слика 4.7.

Узимајући различите начине дегенерасања можемо добити различите ситуације које су опет ништа друго до дегенерација Паскалових конфигурација. Доказаћемо још две интересантне последице дегенерације шестоугла.

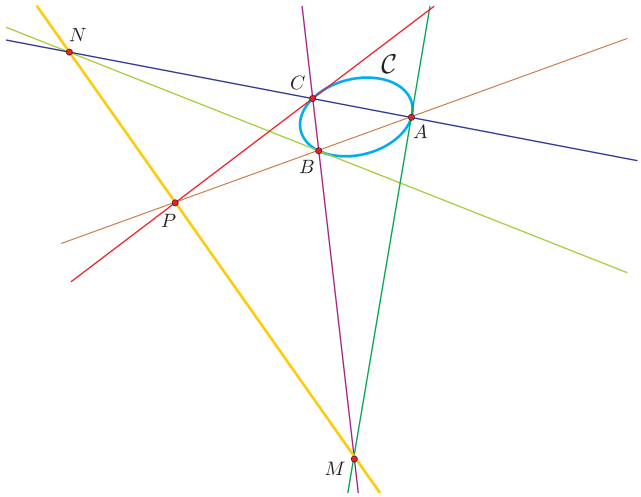
Последица 4. *Нека је $ABCD$ четвороугао уписан у конику $\mathcal{C}$ и нека је тачка M пресек правих AD и BC, тачка N пресек праве AB и праве CD, тачка пресека тангенти на конику $\mathcal{C}$ у тачкама A и C и Q тачка пресека тангенти на конику $\mathcal{C}$ у тачкама B и D. Тада су тачке M, N, P и Q колинеарне.*



Слика 4.8.

Доказ. Применом Паскалове теореме на шестоугао $AABCCD$ добијамо да су тачке M, N и P колинеарне. Применом Паскалове теореме на шестоугао $ABBCDD$ добијамо да су и тачке M, N и Q колинеарне, одакле следи тврђење. □

Последица 5. *Нека је ABC четвороугао уписан у конику $\mathcal{C}$ и нека је тачка M пресек праве AB и тангенте на конику $\mathcal{C}$ у тачки C, тачка N пресек праве BC и тангенте на конику $\mathcal{C}$ у тачки A и тачка Q пресек праве CA и тангенте на конику $\mathcal{C}$ у тачки B. Тада су тачке M, N и P колинеарне.*



Слика 4.9.

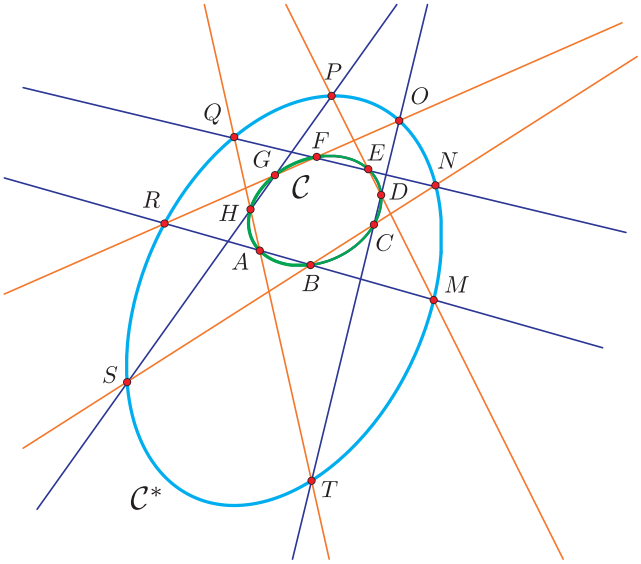
Доказ. Применом Паскалове теореме на шестоугао $AABBCC$ добијамо да су тачке M, N и P колинеарне. □

4.3 Мистични осмоугао

Природно је поставити питање да ли постоји начин да се уопште Папосова и Паскалова теорема. Постоји ли неко слично својство које би поседовале четворке тачака односно осмоугао уписан у конику? Ова питања су доста разматрана у протекла два века и још увек није стављена тачка на њих. Сада ћемо размотрити и у духу теореме о кавезу доказати тврђење за "мистични осмоугао„уписан у конику и њен дегенерисан случај који би представљао генерализацију Папосове теореме.

4.3.1 Паскалова конфигурација

Теорема 4.3.1 (Мистични осмоугао)**.** *Нека је осмоугао $ABCDEFGH$ уписан у конику $\mathcal{C}$ и нека је тачка M пресек правих AB и DE, тачка N пресек правих BC и EF, тачка O пресек правих CD и FG, тачка P пресек правих DE и GH, тачка Q пресек правих EF и HA, тачка R пресек правих FG и AB, тачка S пресек правих GH и BC и тачка S пресек правих HA и CD. Тада тачке M, N, O, P, Q, R, S и T припадају једној коници $\mathcal{C}^*$.*



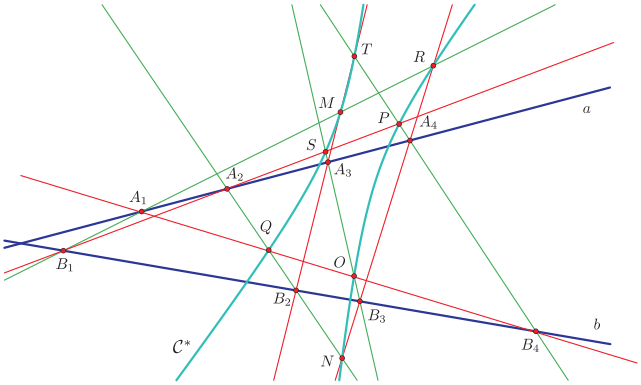
Слика 4.10.

Доказ. Нека је $\mathcal{C}^*$ коника која пролази кроз 5 тачака M, N, O, P и Q. Праве AB, CD, EF и GH са правама BC, DE, FG и HA формирају 4×4 кавез са чворовима у тачкама $A, B, C, \ldots, S$ и T. Тачке $A, B, \ldots P$ и Q формирају супра-триангуларан скуп, па крива $\mathcal{D} = \mathcal{C} \cdot \mathcal{C}^*$ која је четвртог степена пролази кроз њега. Но, према теореми о кавезу она мора проћи и кроз преостале тачке R, S и T. Крива $\mathcal{D}$ је геометријски скуп тачака две конике $\mathcal{C}$ и $\mathcal{C}^*$, а како R, S и T не леже на $\mathcal{C}$, морају припадати $\mathcal{C}^*$. □

4.3.2 Папосова конфигурација

Следећа теорема се може схватити као аналог Папосове теореме. Њу добијемо када у теореми о мистичном осмоуглу узмемо специјалну конику $\mathcal{C} = a \cdot b$ која је унија две праве a и b.

Теорема 4.3.2. *Нека су A_1, A_2, A_3 и A_4 тачке на правој a и B_1, B_2, B_3 и B_4 тачке на правој b и нека је тачка M пресек правих A_1B_1 и A_3B_2, тачка N пресек правих A_2B_2 и A_4B_3, тачка O пресек правих A_3B_3 и A_1B_4, тачка P пресек правих A_4B_4 и A_2B_1, тачка Q пресек правих A_2B_2 и A_1B_4, тачка R пресек правих A_1B_1 и A_4B_3, тачка S пресек правих A_3B_3 и A_2B_1 и тачка S пресек правих A_4B_4 и A_3B_4. Тада тачке M, N, O, P, Q, R, S и T припадају једној коници $\mathcal{C}^*$.*



Слика 4.11.

4.4 Мистични $2n$-тоуглови

Теорема 4.3.1 се природно генерализује за $2n$-тоуглове уписане у конику.

Теорема 4.4.1. *Нека је D многоугао са $2n$ страна уписан у недегенерисану конику $\mathcal{C}$, и нека су му стране обојене наизменично у две боје, црвену и плаву. Ако је K $(n \times n)$-кавез генерисан са датих n црвених и n плавих прави, тада свих $n^2 - 2n$ нових темена кавеза леже на равној криви $\mathcal{C}^*$ степена највише $n-2$.*

Доказ. С обзиром да је $\mathcal{C}$ иредуцибилна коника, следи да се на свакој правој кавеза K налазе тачно две тачке $\mathcal{C}$. Одатле следи да је могуће пренумерисати праве (и плаве и црвене) тако да тачке D чине скуп чворова p_{ij} који задовољавају услов $i + j = n \pm 1$ заједно са два "ћошка "p_{n1} и p_{1n}. Скуп D је садржан у $A = \{p_{ij}\}_{i+j \leq n+1}$, који је супер-триангуларан скуп. Његов комплементаран скуп $A \setminus D$ се садржи од

$$\left(\frac{n^2+3n}{2} - 1\right) - 2n = \frac{n(n-1)}{2} - 1$$

елемената. Желимо да проверимо да ли чворови скупа $A \setminus D$ леже на некој кривој $\mathcal{C}^*$ степена највише $n-2$. Пошто има $\frac{n(n-1)}{2} - 1$ елемената у $A \setminus D$, постојање такве криве је загарантовано неједнакостима

$$\frac{(n-2)^2 + 3(n-2)}{2} \geq \frac{n(n-1)}{2} - 1$$

и $1 \leq n-2 \leq n-1$. Према томе, тачке $A \setminus D$ леже на кривој $\mathcal{C}^*$ степена $n-2$ (прећашња неједнакост нам гарантује егзистенцију коефицијената криве $\mathcal{C}^*$ као решења хомогеног система $\frac{n(n-1)}{2} - 1$ линеарних једначина по $\frac{(n-2)^2+3(n-2)}{2}$ променљивих).

Размотримо сада криву $\mathcal{Q} = \mathcal{C} \cup \mathcal{C}^*$ степена n са иредуцибилном квадратном компонентом $\mathcal{C}$. Чворови D-а се налазе на $\mathcal{C}$, и чворови $A \setminus D$ на $\mathcal{C}^*$. Према томе,

сви чворови A се налазе на C. По теореми о кавезу за равне криве, сви чворови кавеза K морају да леже на кривој $\mathcal{Q}$. Међутим, чворови K који нису у D не могу припадати $\mathcal{C}$, зато што би ово било у контрадикцији са чињеницом да права не може сећи иредуцибилну конику у три тачке. Следи да неурачунати чворови морају да леже на $\mathcal{C}^*$, што је и требало доказати. □

Литература

[1] Gabriel Katz, *Curves in Cages: An Algebro-Geometric Zoo*, The American Mathematical Monthly, Vol. 113, No. 9 (Nov., 2006), pp. 777-791

[2] Lawrence S. Evans and John F. RigbyReviewed, *Octagrammum Mysticum and the Golden Cross-Ratio*, The Mathematical Gazette, Vol. 86, No. 505 (Mar., 2002), pp. 35-4

[3] Richard Schwartz, *PAPPUS'S THEOREM AND THE MODULAR GROUP*, preprint

[4] Frances Kirwan, *Complex Projective Space*, Cambridge University Press ISBN $0521 - 41251X$

[5] Richard Evan Schwartz and Serge Tabachnikov, *Elementary Surprises in Projective Geometry*, preprint

[6] V. V. Prasolov and V. M. Tikhomirov, *Geometry*, American Mathematical Society ISBN $0 - 8218 - 2038 - 9$

[7] Richard Hartley and Andrew Zisserman, *Multiple View Geometry in Computer Vision*, Cambridge University Press ISBN 0521 54051 8

[8] Jürgen Richter-Gebert, *Perspectives on Projective Geometry*, Springer-Verlag Berlin Heidelberg 2011 ISBN 978-3-642-17285-4

[9] Robert Bix, *Conics and cubics: an elementary introduction to the algebraic geometry*, Springer-Verlag

[10] Marcel Berger, *Geometry Revealed - A Jscob's Ladder to Modern Higher Geometry*, Springer Heidelberg Dodrecht London New York ISBN 978-3-540-70966-1