FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Radek Olšák

Applications of algebraic geometry in mathematical contests

Department of Algebra

Supervisor of the bachelor thesis: doc. RNDr. Jan Šťovíček, Ph.D.
Study programme: Computer Science
Study branch: General Computer Science

Prague 2022

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In .... date ....
Author's signature

I would like to thank my supervisor, doc. RNDr. Jan Šťovíček, Ph.D., for helping me with the thesis. He's been giving me the algebraic point of view on most stated topics.

Title: Applications of algebraic geometry in mathematical contests

Author: Radek Olšák

Department: Department of Algebra

Supervisor: doc. RNDr. Jan Šťovíček, Ph.D., Department of Algebra

Abstract: The thesis presents different algebraic approaches to solving high school geometry problems. In particular, it shows the use of circle pencils, Desargues involution, the Method of Animation, and elliptic curves. It contains selected problems with solutions to show how these techniques can solve different problems.

Keywords: Animation, Desargues Involution, circles, conics, resultants, algebraic geometry, projective geometry, elliptic curve

Contents

Introduction . . . 2

1 **Algebraic definitions** . . . 3
- 1.1 Fields . . . 3
- 1.2 Projective space . . . 3
- 1.3 Linear transformations . . . 4

2 **Basics of Angle chasing** . . . 5

3 **Resultants** . . . 6

4 **Conics** . . . 8

5 **Complex circles** . . . 10
- 5.1 Introduction to circles . . . 10
- 5.2 Power of a point . . . 11
- 5.3 Radical axis . . . 12

6 **Desargues involution** . . . 15

7 **Animation** . . . 17
- 7.1 Degree bounding . . . 17
- 7.2 Degree preserving mappings . . . 19

8 **Cubic curves** . . . 22

Conclusion . . . 27

Bibliography . . . 28

Introduction

This thesis shows different non-traditional approaches to solving high school olympiad geometry problems. These olympiad problems are usually stated in standard euclidian space $\mathbb{R}^2$. However, for convenience, we will usually extend this to the projective space $\mathbb{PR}^2$ or even into $\mathbb{PC}^2$. We show example problems with solutions. These problems are selected to best show the possibilities of the presented techniques. Their solutions are combinations of different posts from [8] and my contribution.

In the first chapters, we introduce algebraic notation and conics and give a projective characterization of circles.

In the chapter about Desargues involution, we show a known result about the linearity of the Desargues involution. We present an elementary proof of that result, and we show an example of how to use it. More about this in [5].

In the animation section, we write about the Method of Animation from [1]. This technique uses curve parametrizations to solve geometric problems. We show an elementary proof using resultants of a known result regarding the degree of such a parametrized curve.

The last chapter shows how to use group operation on an elliptic curve to solve challenging problems.

1 Algebraic definitions

1.1 Fields

Proposition 1.1. Let K be UFD and Q its field of fractions. Then $p \in K[x]$ has non-constant factor in $K[x]$ if and only if it has a non-constant factor in $Q[x]$.
Proof. It's a corollary of **1.16.** in [4].

Proposition 1.2. Let p, be a homogenous polynomial in $\mathbb{C}[x, y]$ with degree d. Then it factors into d linear terms of a form $(ax - by)$, where (b, a) is a root of p.
Proof. It sufficies to find one such divisor. The rest will be given by induction on the degree of p. We distinguis two cases.

- $y \mid p$. Then we have such a divisor.
- $y \nmid p$. Then we substitute $y = 1$ to get a polynomial q in $\mathbb{C}[x]$ with the same degree. From Fundamental theorem of algebra tris polynomial has some root r and therefore is divisible by $(x - r)$. Thus we write $q = (x - r)q'$ for some $q' \in \mathbb{C}[x]$. Then we homogenize q' by adding y to get $p' \in \mathbb{C}[x, y]$. Then we have gotten a factorization of p as $p = (x - ry)p'$. □

1.2 Projective space

Definition. Let K be a field. Then the *projective space* of dimension n over field K is a set of all $(n + 1)$-tuples $(a_1, a_2, a_3, \ldots, a_n, a_{n+1}) \in K^{n+1}/\{(0, 0, \ldots, 0)\}$ up to equivalence $(a_1, a_2, a_3, \ldots, a_n, a_{n+1}) \sim (ka_1, ka_2, ka_3, \ldots, ka_n, ka_{n+1})$, for every $k \in K/\{0\}$. We denote it by $\mathcal{P}K^n$. For the equivalence class containing $(a_1, a_2, a_3, \ldots, a_n, a_{n+1})$ we use notation $[a_1, a_2, a_3, \ldots, a_n, a_{n+1}]$.

Note. When talking about $(n + 1)$-tuples from K^{n+1} we will look at K^{n+1} as having a structure of a vector space.

Definition. Let p be a homogenous polynomial in $K[x_1, x_2, x_3, \ldots, x_n, x_{n+1}]$ with degree d. Then $X = [a_1, a_2, a_3, \ldots, a_n, a_{n+1}] \in \mathcal{P}K^n$ is the *zero* of p if it holds that $p(a_1, a_2, a_3, \ldots, a_n, a_{n+1}) = 0$. This is well defined, because p is homogenous polynomial, we have that

$$p(ka_1, ka_2, ka_3, \ldots, ka_n, ka_{n+1}) = k^d p(a_1, a_2, a_3, \ldots, a_n, a_{n+1}).$$

Definition. Let p be a polynomial in $K[x_1, x_2, x_3, \ldots, x_n, x_{n+1}]$. Then we may uniquely write it as sum $p_1 + p_2 + p_3 + \cdots + p_m$ of homogenous polynomials. We say that point $X \in \mathcal{P}K^n$ is a *zero* of p if it a zero of all $p_1, p_2, p_3, \ldots, p_m$.

Definition. Let Q be a set of polynomials. Then we denote $V(Q)$ the set of all points S in $\mathcal{P}K^n$ such that $\forall p \in Q$ and $\forall s \in S$ we have that s is the zero of p.

Definition. For a set of points S in $\mathcal{P}K^n$ we define $I(S)$ the set of all polynomials Q such that $\forall p \in Q$ and $\forall s \in S$ we have that s is the zero of p.

Definition. Let I be an ideal in R. Then we denote by $\mathrm{Rad}(I)$ the set of all $r \in R$ such that there exists $n \in \mathbb{N}$ for which $r^n \in I$.

Theorem 1.3 (Projective Nullstellensatz). Let L be a homogenous ideal in $K[x_1, x_2, x_3, \ldots, x_n, x_{n+1}]$. If $V(L) \neq \emptyset$, then $I(V(L)) = \mathrm{Rad}(L)$
Proof. For proof see page 46. of [3].

Corollary 1.4. Let p be an polynomial from $K[x_1, x_2, x_3, \ldots, x_n, x_{n+1}]$ and g some ireducible factor of p such that $V(p) = V(g)$. Then for some $n \in \mathbb{N}, c \in K$ it holds that $p = cg^n$.

Proof. Because g is ireducible, we have $g = \mathrm{Rad}(\{g\})$. Thus from $V(g) = V(p)$, we have that $g = \mathrm{Rad}(\{g\}) = I(V(g)) = I(V(p)) = \mathrm{Rad}(\{p\})$. Hence $p = cg^n$ for some $n \in \mathbb{N}, c \in K$. □

Definition. Let $p_1, p_2, p_3, \dots, p_{n+2} \in \mathcal{P}K^n$ be points. Then we say that they are in general position if no subset of $(n+1)$ of their representants lie in less then $(n+1)$ dimensional vector space.

1.3 Linear transformations

Definition. Consider a projective space $\mathcal{P}K^n$ and a regular matrix $M \in K^{(n+1)\times(n+1)}$. Then this gives us a transformation $\mathcal{P}K^n \to \mathcal{P}K^n$, such that for $X = [a_1, a_2, a_3, \dots, a_n, a_{n+1}] \in \mathcal{P}K^n$ we transform it to equivalence class of

$$M(a_1, a_2, a_3, \dots, a_n, a_{n+1})^T.$$

This is well defined, because from linearity

$$M(ka_1, ka_2, ka_3, \dots, ka_n, ka_{n+1})^T = kM(a_1, a_2, a_3, \dots, a_n, a_{n+1})^T.$$

We call this the *linear transformation* given by matrix M.

Observation 1.5. Multiplying a matrix of a linear transformation of $\mathcal{P}K^n$ by a constant gives the same linear transformation.

Proposition 1.6. For given $n+2$ points p_i in general position and $n+2$ points q_i in general position in $\mathcal{P}K^n$. There exists exactly one linear transformation mapping $p_i \mapsto q_i$ for all i.

Proof. Let $a, a_1, a_2, \dots, a_n, a_{n+1} \in K^{n+1}$ be some representants of equivalences p_i. Analogously let $b, b_1, b_2, \dots, b_n, b_{n+1} \in K^{n+1}$ be some representants of q_i. Then for every nonzero $\lambda_1, \lambda_2, \dots, \lambda_n, \lambda_{n+1}$ there exists a unique linear transformation f of K^{n+1} mapping $a_i \mapsto \lambda_i b_i$. As p_i and q_i are in general position, there are unique linear combinations with nonzero coefficients

$$a = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n + \alpha_{n+1} a_{n+1}$$
$$b = \beta_1 b_1 + \beta_2 b_2 + \dots + \beta_n b_n + \beta_{n+1} b_{n+1}.$$

From linearity we have that

$$\begin{aligned} f(a) &= f(\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n + \alpha_{n+1} a_{n+1}) = \\ &= \alpha_1 f(a_1) + \alpha_2 f(a_2) + \dots + \alpha_n f(a_n) + \alpha_{n+1} f(a_{n+1}) = \\ &= \alpha_1 \lambda_1 \beta_1 + \alpha_2 \lambda_2 \beta_2 + \dots + \alpha_n \lambda_n \beta_n + \alpha_{n+1} \lambda_{n+1} \beta_{n+1}. \end{aligned}$$

This has to equal a multiple of b. Thus from uniqueness of linear combination for b, we have that, up to a scalar multiple $\lambda_i = \frac{\beta_i}{\alpha_1}$. Such a scalar multiple just multiplies the whole matrix by the same scalar. Thus from construction there is an unique linear transformation mapping $p_i \mapsto q_i$. □

2 Basics of Angle chasing

We will be working in $\mathbb{R}^2$.

Definition. We say that a set of points S is *concyclic* if there exists a circle passing through all of them.

Definition. Four points A, B, C, D form a *cyclic* quadrilateral, if they are concyclic.

Definition. Let p be a line, we will denote $\vec{p}$ the direction of p in degrees modulo $180°$.

Definition. Let p, q be two lines, we denote $\angle(p,q)$ the angle by which we have to rotate p counterclockwise to be parallel with q. We take this angle modulo $180°$. Hence we can also get it as $\vec{q} - \vec{p}$

Definition. Let A be a point on a circle ω with center O, then $\overrightarrow{A_\omega}$ is the direction of the ray OA modulo $360°$.

Proposition 2.1. Let ω be a circle with center O. Line p intersects circle at points A, B. If p is tangent, then $A = B$. Then

$$\vec{p} = \frac{\overrightarrow{A_\omega} + \overrightarrow{B_\omega}}{2} + 90°$$

Proof.

- If $A \neq B$, then as O is the center, we have that triangle OAB is isosceles $OA = OB$. Hence the internal angle bisector of OAB is perpendicular to AB.
- If $A = B$. Then p is a tangent. Hence it's perpendicular to OA. □

Theorem 2.2 (Circumscribed angle). Let A, B, C, D be four points in a general position. Then $ABCD$ is cyclic if and only if $\angle(AB, AC) = \angle(DB, DC)$.

Proof.

- $\Rightarrow$: Denote ω the circumcircle. Then from 2.1 we have

$$\angle(AB,AC) = \left(\frac{\overrightarrow{A_\omega} + \overrightarrow{C_\omega}}{2} + 90°\right) - \left(\frac{\overrightarrow{A_\omega} + \overrightarrow{B_\omega}}{2} + 90°\right) = \frac{\overrightarrow{C_\omega} - \overrightarrow{B_\omega}}{2} =$$

$$= \frac{\overrightarrow{C_\omega} - \overrightarrow{B_\omega}}{2} = \left(\frac{\overrightarrow{D_\omega} + \overrightarrow{C_\omega}}{2} + 90°\right) - \left(\frac{\overrightarrow{D_\omega} + \overrightarrow{B_\omega}}{2} + 90°\right) = \angle(DB,DC)$$

- $\Leftarrow$: Let ω be a circumcircle of ABC and let D' be the second intersection of DB with ω. Then from the first part we have that $\angle(AB,AC) = \angle(D'B, D'C) = \angle(DB,DC)$, hence $\overrightarrow{DC} = \overrightarrow{D'C}$ and as both lines pass through the same point C, they coincide. Hence $D = D'$. ■

Definition. We denote the value of $\overrightarrow{C_\omega} - \overrightarrow{B_\omega}$ as the *central angle* of arc BC.

3 Resultants

Let K be UFD and let $p = a_{\deg p}x^{\deg p} + \cdots + a_1x + a_0$, $q = b_{\deg q}x^{\deg q} + \cdots + b_1x + b_0$ be two polynomials in $K[x]$ and denote Q the field of fractions of K. Then from Gauss lemma 1.1 p, q have a non-constant common factor iff they have a common factor in $Q[x]$. And they have a common factor in $Q[x]$ iff $\deg(\mathrm{LCM}(p,q)) < \deg(p) + \deg(q)$. And that is iff there exists some polynomials $c_p, c_q \in Q[x]$ satisfying

$$\deg(c_p) < \deg(q)$$
$$\deg(c_q) < \deg(p)$$

$$c_p p + c_q q = 0$$

Which is iff there exists nontrivial linear combination of vectors

$$p, xp, x^2p, \ldots, x^{\deg(q)-1}, q, xq, x^2q, \ldots, x^{\deg(p)-1}$$

that equals zero. Which is iff determinant of this $(\deg(p) + \deg(q)) \times (\deg(p) + \deg(q))$ matrix of coefficients is equal to zero.

$$\begin{pmatrix}
a_0 & a_1 & a_2 & \cdots & a_{\deg(p)} & 0 & \cdots & 0 \\
0 & a_0 & a_1 & \cdots & a_{\deg(p)-1} & a_{\deg(p)} & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \vdots \\
0 & \cdots & 0 & a_0 & \cdots & \cdots & a_{\deg(p)-1} & a_{\deg(p)} \\
b_0 & b_1 & b_2 & \cdots & b_{\deg(q)} & 0 & \cdots & 0 \\
0 & b_0 & b_1 & \cdots & b_{\deg(q)-1} & b_{\deg(q)} & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \vdots \\
0 & \cdots & 0 & b_0 & \cdots & \cdots & b_{\deg(q)-1} & b_{\deg(q)}
\end{pmatrix}$$

Definition. The determinant of this matrix given by polynomials p and q in variable x is the *resultant* of p and q and we denote it $\mathrm{res}_x(p,q)$. And we look at it as a polynomial in coefficients of p and q.

Observation 3.1. From construction we have that $\mathrm{res}_x(p,q)$ is zero iff p and q have a non-constant common factor.

For last observations in this section we define p_x for homogenous polynomial $p \in K[x,y]$ the polynomial we get by substituting $y = 1$ in p. Even if this substitution lowered the degree, we would view p_x as having the same degree with some leading coefficients being zero. Similarly we define p_y as polynomial we get by substituting $y = 1$.

Observation 3.2. Let p, q be two homogenous polynomials in $K[x,y]$ of the same degree. Then $\mathrm{res}_x(p_x,q_x) = \pm\mathrm{res}(\mathrm{res}_y(p_y,q_y))$. Consequently $\mathrm{res}_x(p,q) = 0 \Leftrightarrow \mathrm{res}_y(p,q) = 0$

Proof. The matricies we get for $\mathrm{res}_x(p_x,q_x)$ and $\mathrm{res}_y(p_y,q_y)$ differ only by a permutation of rows and columns, hence the determinant differs by a multiple of ± 1. □

Proposition 3.3. Let p, q be two homogenous polynomials in $K[x,y]$. Then p, q have a common factor in $K[x,y]$ if and only if $res_x(p_x,q_x) = 0$.

Proof.

- $\Rightarrow$: If they have a common factor, then if this factor contains x, then it it also a factor of p_X and q_x after substitution $y = 1$, hence $res_x(p_x, q_x) = 0$. If it does not contain x, it has to contain y. So after substituting $x = 1$ it is a factor of p_y and q_y. And from 3.3 we have that $res_x(p_x, q_x) = \pm res_y(p_y, q_y) = 0$.
- $\Leftarrow$:
  - If neither p nor q is divisible by y. Then polynomials p_x and q_x have no leading zeroes, thus if $res_x(p_x, q_x) = 0$ then p_x and q_x have a common factor. Homogenizing by adding y we get a factor of p and q.
  - If both p and q are divisible by y. Then polynomials p_x and q_x both start with zero. Thus the corresponding matrix will have the first column full of zeroes. Hence its determinant will be zero.
  - If WLOG p is divisible by y and q is not. Denote k the maximum number such that $y^k \mid p$. Look at matrix corresponding to p_x and q_x. The top right $k \times d$ block will be zero. Thus using ellimination we can transform first k columns of rows d to $d + k$ into identity matrix. From that we see, that any nontrivial combination of rows that equals zero must not utilize these k rows, hence the determinant is zero iff $\mathrm{res}(p'_x, q_x)$ is zero, where p'_x is p_x with removed leading zeros. Thus we have a common factor of p'_x and q_x, which after homogenization using y gives us a common factor of p and q. □

Definition. We denote $\mathrm{res}_{xy}(p, q) = \mathrm{res}_x(p_x, q_x)$.

4 Conics

Definition. A *conic* is a homogenous quadratic form; hence it has a general form

$$Ax^2 + By^2 + Cz^2 + 2Dyz + 2Ezx + 2Fxy$$

We can write it as a matrix form

$$\begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} A & D & E \\ D & B & F \\ E & F & C \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

Definition. When the matrix is regular, we say that the conic is *nondegenerate.*

Definition. We denote the *polar* of a point $[P_x, P_y, P_z]$ with respect to a nondegenerate conic γ with matrix M as the line given by

$$\begin{pmatrix} P_x & P_y & P_z \end{pmatrix} M \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

Proposition 4.1. For every line ℓ and a nondegenerate conic γ, there is precisely one point P such that ℓ is polar of P with respect to γ.

Proof. The line is given by some equation $Ax + By + Cz = 0$, hence we are solving

$$\begin{pmatrix} P_x & P_y & P_z \end{pmatrix} M = \begin{pmatrix} A & B & C \end{pmatrix}$$

which has exactly one solution, as the matrix M is regular. Any k-multiple of $\begin{pmatrix} A & B & C \end{pmatrix}$ gives the same line. But from linearity it generates the same point.

Definition. We denote this point the *pole* of line ℓ with respect to γ.

Note. When talking about poles and polars without the conic, we refer to them as if the matrix of a conic is the identity matrix.

Theorem 4.2 (Principle of duality). Let γ be any conic, P some point and ℓ some line. And denote by p the polar of P and by L the pole of ℓ. Then $P \in \ell$ if and only if $L \in p$.

Proof. Let M be matrix associated with γ. Then

$$P \in \ell \Leftrightarrow L^T M P = 0 \Leftrightarrow P^T M^T L = 0^T \Leftrightarrow P^T M L = 0 \Leftrightarrow L \in p.$$

■

Observation 4.3. Let P be a point lying on some nondegenerate conic γ. Let p be its polar with respect γ. Then p is tangent to γ at P.

Proof. From definition $P \in p$. Now suppose that p and γ intersect at some other point $Q \neq P$. Then polar of Q from definition passes through Q and from 4.2 passes through P. But then both P and Q are the poles of p. Which is contradicts unique construction of the pole. □

Observation 4.4. Let P be a point and p its polar with respect to some nondegenerate conic γ. Then p intersects γ at two distinct points if and only if $P \notin \gamma$.

Proof. From previous observation we have that if $P \in \gamma$ then p does not intersects γ at two different points. Now if p intersects γ at one point Q. Then from have that p is the polar of Q, as at each point of γ there is an unique tangent.

Observation 4.5. Let T be a regular matrix of some linear transformation and M be a matrix of some conic. Then $T^{-T}MT^{-1}$ is the matrix of M transformed by T.

Proposition 4.6. Let T be a regular matrix of any linear transformation and M matrix of some conic. Then if p is the polar of P with respect to M then Tp is polar of TP with respect to conic $T^{-T}MT^{-1}$.
Proof. Let us take any point $X \in p$. Then

$$(TX)^T T^{-T}MT^{-1}TP = X^T MP.$$

Thus Tp is the polar of TP. □

5 Complex circles

5.1 Introduction to circles

The circle in $\mathbb{R}^2$ with center (c_x, c_y) and radius r is a set of points satisfying equation

$$(x - c_x)^2 + (y - c_y)^2 + r = 0.$$

After multiplying above equation out we get that the circle equation has form

$$Ax^2 + Ay^2 + 2B_1x + 2B_2y + C = 0$$

for some numbers A, B_1, B_2 and C. As we will be working in $\mathbb{PC}^2$ we will homogenize this equation.

Definition. Any polynomial of a form

$$\omega = Ax^2 + Ay^2 + 2B_1xz + 2B_2yz + Cz^2$$

is a *circle polynomial.* And the set $V(\{\omega\})$ is the *circle.*

Observation 5.1. We may write circle polynomial in a matrix form as follows

$$x^T \begin{pmatrix} A & 0 & B_1 \\ 0 & A & B_2 \\ B_1 & B_2 & C \end{pmatrix} x = 0$$

Definition. If $A = 1$ we have circle polynomial in form

$$x^2 + y^2 + B_1xz + B_2yz + Cz^2.$$

We denote this as the *normalized polynomial* of a circle.

Definition. Let ω be a circle. Then the *center* of ω is the pole of the infinity line with respect to ω.

Observation 5.2. Center of a circle does not lie on the infinity line.

Proposition 5.3. Let ω be a circle. And denote $O = [a, b, 1]$ its center. Then point reflection by O maps ω onto itself.

Proof. Let M be the matrix of ω with following entries

$$\begin{pmatrix} 1 & 0 & B_1 \\ 0 & 1 & B_2 \\ B_1 & B_2 & C \end{pmatrix}$$

. That O is the pole of the infinity line means, that $O^T M = [0, 0, 1]$. Hence we get that $a + B_1 = 0 = b + B_2$. The point reflection by O is given by the matrix

$$T = \begin{pmatrix} -1 & 0 & 2a \\ 0 & -1 & 2b \\ 0 & 0 & 1 \end{pmatrix}.$$

Thus the transformed conic is given by the following matrix. We will use observed conditions $a + B_1 = 0 = b + B_2$ to simplify expansion.

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 2a & 2b & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & B_1 \\ 0 & 1 & B_2 \\ B_1 & B_2 & C \end{pmatrix} \begin{pmatrix} -1 & 0 & 2a \\ 0 & -1 & 2b \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} -1 & 0 & -B_1 \\ 0 & -1 & -B_2 \\ -B_1 & -B_2 & 2B_1a + 2B_2b + C \end{pmatrix} \begin{pmatrix} -1 & 0 & 2a \\ 0 & -1 & 2b \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 & B_1 \\ 0 & 1 & B_2 \\ B_1 & B_2 & -2B_1a - 2B_2b + 2B_1a + 2B_2b + C \end{pmatrix} = \begin{pmatrix} 1 & 0 & B_1 \\ 0 & 1 & B_2 \\ B_1 & B_2 & C \end{pmatrix} = M$$

Thus for every point P we have that P lies on ω if and only if $T(P)$ lies on ω. □

Definition. We denote points complex points $[1, i, 0]$ and $[1, -i, 0]$ the *circle points.*

Proposition 5.4. Conic is a circle if and only if it passes through both circle points.
Proof. From circle polynomial it's trivial, that all circles pass through these points. So we will proceed to the other implication. General conic is given by matrix equation

$$x^T \begin{pmatrix} A & B & C \\ B & D & E \\ C & E & F \end{pmatrix} x = 0$$

Pluging in the two points we get

$$A + 2Bi - D = 0$$
$$A - 2Bi - D = 0.$$

Subtracting these gives us $4Bi = 0$, hence $B = 0$, and adding them gives $A = D$. Hence we get a matrix of a circle. □

5.2 Power of a point

Definition. For a circle ω, we denote its normalized polynomial as $\mathcal{P}_\omega$. It is also known as the *power of a point* with respect to ω.

Definition. Let ω, resp. Ω be circles. Then we denote the affine space generated by $\mathcal{P}_\omega$ and $\mathcal{P}_\Omega$ as *pencil* generated by ω and Ω. This is set of all polynomials of form $\lambda_1 \mathcal{P}_\omega + \lambda_2 \mathcal{P}_\Omega$ for $\lambda_1 + \lambda_2 = 1$.

Proposition 5.5. All polynomials in pencil of two circles are normalized circle polynomials.
Proof. Let ω and Ω be two circles. The coefficient at x^2 and y^2 is 1 in both $\mathcal{P}_\omega$ and $\mathcal{P}_\Omega$. Hence it will be 1 in any affine combination. □

Observation 5.6. Let ω and Ω be two circles and $k \in \mathbb{C}$ and $k \neq 1$. All points X satisfying

$$\frac{\mathcal{P}_\omega(X)}{\mathcal{P}_\Omega(X)} = k$$

lie on some circle from the pencil generated by ω and Ω.
Proof. We rewrite the equation as

$$\frac{1}{1-k} \cdot \mathcal{P}_\omega(X) + \frac{-k}{1-k} \cdot P_\Omega(X) = 0.$$

This is an polynomial for some circle from the pencil generated by ω and Ω. □

Corollary 5.7. Let ω and Ω be two circles and X, Y be two points such that

$$\frac{\mathcal{P}_\omega(X)}{\mathcal{P}_\Omega(X)} = \frac{\mathcal{P}_\omega(Y)}{\mathcal{P}_\Omega(Y)} \neq 1,$$

then X and Y lie on the same circle from the pencil generated by ω and Ω.

Observation 5.8. Let ω and Ω be two circles and γ be a circle from the pencil generated by ω and Ω. And let $[x, y, z]$ be a point such that $\mathcal{P}_\omega(x, y, z) = \mathcal{P}_\Omega(x, y, z)$, then $\mathcal{P}_\gamma(x, y, z) = \mathcal{P}_\omega(x, y, z) = \mathcal{P}_\Omega(x, y, z)$.

Corollary 5.9. When X is one of the intersections of ω and Ω, it lies on all circles from their pencil.

5.3 Radical axis

Definition. For circles ω and Ω, we look at the polynomial $\mathcal{P}_\omega - \mathcal{P}_\Omega$. As both $\mathcal{P}_\omega$ and $\mathcal{P}_\Omega$ are normalized the terms x^2 and y^2 cancel out we are left with a polynomial of the form $z \cdot Q(x, y, z)$, where Q is linear. We denote Q the *radical axis polynomial* of ω and Ω and $V(\{Q\})$ as the *radical axis* of ω and Ω.

Proposition 5.10. Let ω and Ω be two circles. The radical axis is the same for any pair of circles from the pencil generated by ω and Ω.
Proof. Let $c_1 = \lambda_1\mathcal{P}_\omega + (1-\lambda_1)\mathcal{P}_\Omega$ and $c_2 = \lambda_2\mathcal{P}_\omega + (1-\lambda_2)\mathcal{P}_\Omega$ for $\lambda_1 \neq \lambda_2$. Then radical axis polynomial of c_1 and c_2 is

$$\lambda_1\mathcal{P}_\omega + (1-\lambda_1)\mathcal{P}_\Omega - \lambda_2\mathcal{P}_\omega - (1-\lambda_2)\mathcal{P}_\Omega = (\lambda_1 - \lambda_2)(\mathcal{P}_\omega - \mathcal{P}_\Omega).$$

As $\lambda_1 - \lambda_2$ is nonzero, this radical axis polynomial is always a scalar multiple of $\mathcal{P}_\omega - \mathcal{P}_\Omega$, hence the radical axis does not depend on λ_1, λ_2.

Theorem 5.11. For three circles ω, Ω, and γ not lying on one pencil, their pairwise radical axes are concurrent.
Proof. Denote $\ell(c_1, c_2)$ the radical axis of circles c_1 and c_2. We distinguish two cases

- $\ell(\omega, \Omega)$ and $\ell(\Omega, \gamma)$ are not parallel, hence they are not concurrent with the infinity line. Then denote by R their intersection point. From the definition of radical axis we have that $\mathcal{P}_\omega(R) = \mathcal{P}_\Omega(R) = \mathcal{P}_\gamma(R)$, hence R is a zero of $\mathcal{P}_\gamma - \mathcal{P}_\omega$. And as it does not lie on the infinity line, it has to lie on the radical axis of γ and ω.
- $\ell(\omega, \Omega)$ and $\ell(\Omega, \gamma)$ intersect on the infinity line at point R. Then for contradiction suppose, that $\ell(\gamma, \omega)$ intersects $\ell(\omega, \Omega)$ at a point Q different from R. Then Q does not lie on the infinity line, hence from the first part all three radical axes pass through Q, hence a contradiction. ■

Definition. We denote the intersection of radical axes of three circles not lying on one pencil the *radical center* of the three circles.

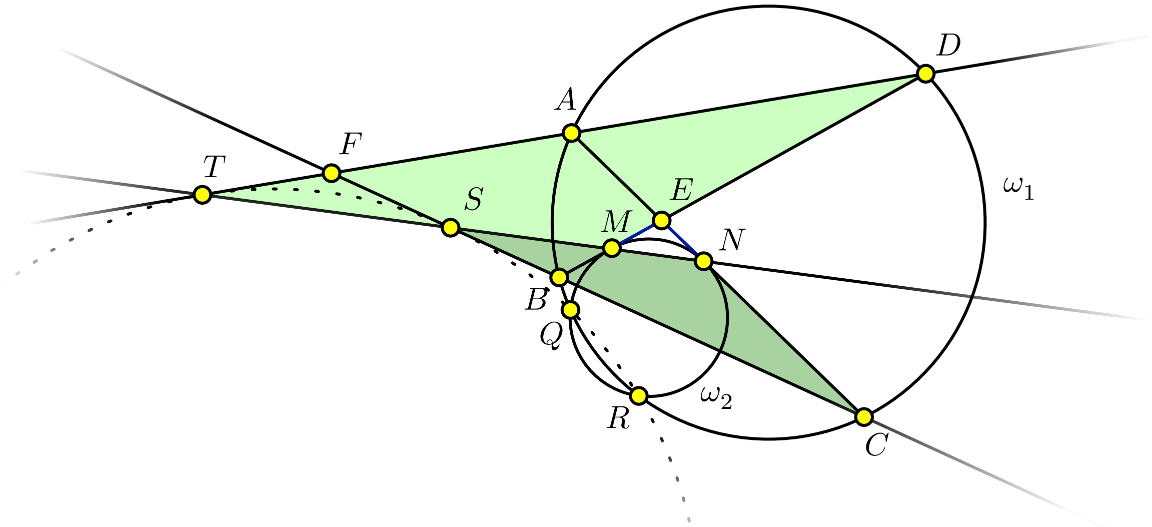
Proposition 5.12. Let X be a point and ω a circle, both in $\mathbb{R}^2$. A line ℓ passing through X intersects the circle at two points Z_1, Z_2. Then after substituting $z = 1$ into $\mathcal{P}_\omega$ we have $\mathcal{P}_\omega X = XZ_1 \cdot XZ_2$, where distances are directed.
Proof. Denote O the point $[0, 0, 1]$. Let M be a matrix for the circle polynomial of ω. Len N be an composition of rotation matrix in $\mathbb{R}^2$ with translation matrix such that it maps $y = 0$ onto ℓ and point O onto X. Then

$$\mathcal{P}_\omega X = X^T M X = O^T N^T M N O.$$

In N the top right 2×2 submatrix is an rotational matrix; thus an orthonormal matrix. Furthermore from that M is normalized, we have that its top right 2×2 submatrix is identity matrix. Thus the final matrix $N^T M N$ has the top right 2×2

submatrix the identity matrix; hence is a normalized circle polynomial. Denote Q the circle polynomial given by matrix $N^T M N$ after substituting $z = 1$ and $y = 0$. Thus $Q \in \mathbb{R}[x]$. Denote Z_1' and Z_2' points of intersection of line $y = 0$ with circle given by $N^T M N$ and denote z_1 and z_2 their x-coordinates respectively. As rotation and translation preserves distances, we have that $XZ_1 = OZ_1' = z_1$ and $XZ_2 = OZ_2' = z_2$. As z_1 and z_2 are roots of Q and Q has leading coefficient 1, we have from Vieta formulas that $\mathcal{P}_\omega X = Q(0) = z_1 z_2 = XZ_1 \cdot XZ_2$. □

Problem 5.1 (CGMO 2017/7). Let the $ABCD$ be a cyclic quadrilateral with circumcircle ω_1. Lines AC and BD intersect at point E, and lines AD, BC intersect at point F. Circle ω_2 is tangent to segments EB, EC at points M, N respectively, and intersects with circle ω_1 at points Q, R. Lines BC, AD intersect line MN at S, T respectively. Show that Q, R, S, T are concyclic.

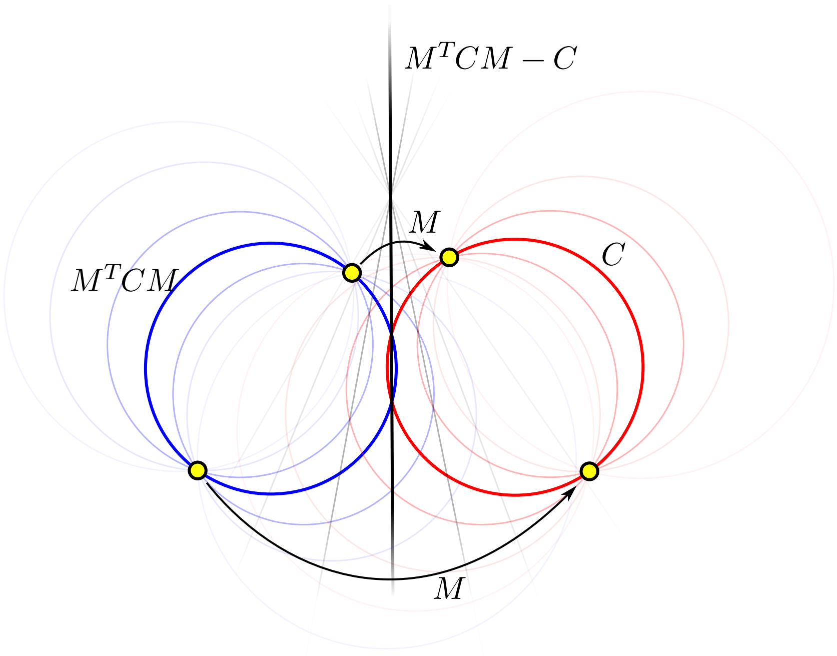


Solution. From symmetry we have that triangle EMN is isosceles, hence $\angle(EM, MN) = \angle(MN, EN)$. And because $ABCD$ is cyclic, we conclude that $\angle(BC, CA) = \angle(BD, DA)$, hence $\triangle SCN \sim \triangle TDM \Rightarrow \frac{SN}{TM} = \frac{SC}{TD}$. Analogously $\triangle SBM \sim TAN \Rightarrow \frac{SM}{TN} = \frac{SB}{TA}$. Thus

$$\frac{P_{\omega_1}(S)}{P_{\omega_2}(S)} = \frac{SC \cdot SB}{SN \cdot SM} = \frac{TD \cdot TA}{TN \cdot TM} = \frac{P_{\omega_1}(T)}{P_{\omega_2}(T)}.$$

Hence S and T both lie on the same circle γ from pencil generated by ω_1 and ω_2. Thus all points Q, R, S, T lie on γ.

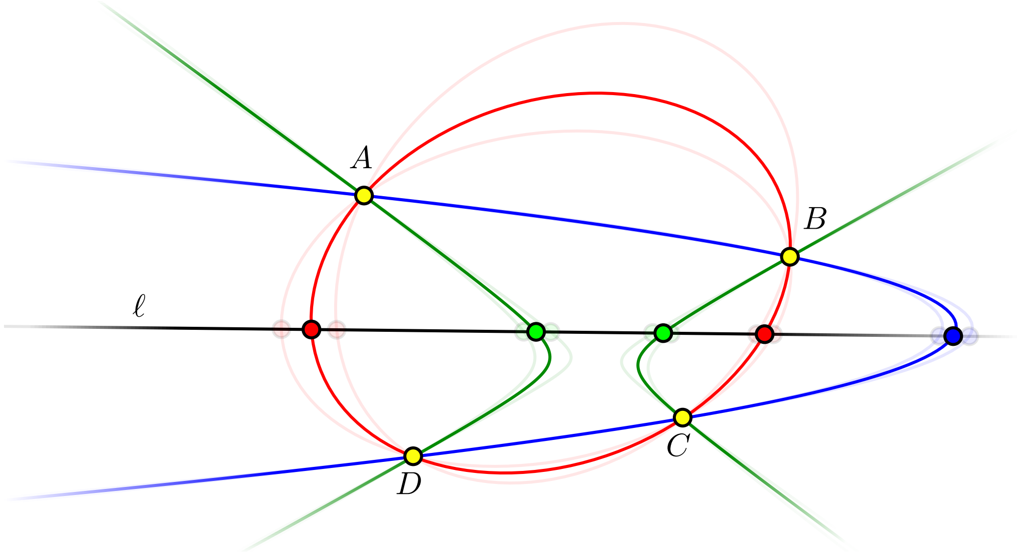
Problem 5.2. Let AB and XY be two segments in a plane. Let ω be an arbitrary circle passing through AB and construct ω' passing through XY such that $\omega \cup AB$ is directly similar to $\omega' \cup XY$. Prove that the radical axis of ω and Ω pass through a fixed point, not depending on the choice of ω.



Solution. All circles passing through XY form a pencil. Denote C matrix of some circle ω' from this pencil. As $\omega' \cup XY$ is directly similar to $\omega \cup AB$, there exists a fixed linear mapping with the matrix M such that it maps $A \mapsto X$, $B \mapsto Y$ and $\omega \mapsto \omega'$. Hence we get that matrix for ω is M^TCM. Now the conic defined by $M^TCM - C$ is the radical axis polynomial of ω and ω' multiplied by the infinity line. As $M^TCM - C$ is a linear mapping of C, these polynomials will again form a pencil. Hence for any two radical axes p, q we can express any other radical axes as $\lambda_1 p + \lambda_2 q$ for $\lambda_1 + \lambda_2 = 1$. Thus if two of the radical axes p, q intersect on a point P not lying on the infinity line, all the radical axes are zero at this point. Hence they all pass through a fixed point.

6 Desargues involution

Definition. Let A, B, C, D be four points in a general position and ℓ a line not passing through any of them. Then we construct a mapping $\pi\colon \ell \to \ell$ as follows. Take a point X on ℓ, then construct the conic passing through A, B, C, D, X and find it's second intersection X' with ℓ. Then $\pi(X) = X'$. We call this the *Desargues involution* on ℓ given by A, B, C, D.



Observation 6.1. Desargues involution is an involution.

Theorem 6.2. Desargues involution is a linear mapping on ℓ.

Proof. Using projective transformation we may assume that ℓ is given by equation $z = 0$. All conics passing through A, B, C, D form one dimensional affine space. Take two conics passing through A, B, C, D and substitute $z = 0$ to get

$$\begin{aligned} \omega_1 &= a_1x^2 + b_1xy + c_1y^2 \\ \omega_2 &= a_2x^2 + b_2xy + c_2y^2 \end{aligned}.$$

As all conics from statement are part of one dimensional affine space, we can get them as linear combination of ω_1 and ω_2. For given $[x_0, y_0]$ denote

$$\omega = \omega_1(x_0, y_0)\omega_2 - \omega_2(x_0, y_0)\omega_1.$$

Then ω is a conic from given pencil, that passes through $[x_0, y_0]$. We claim that the involution π is given by

$$[x, y] \mapsto [(a_1c_2 - a_2c_1)x + (b_1c_2 - b_2c_1)y, (b_1a_2 - b_2a_1)x + (c_1a_2 - c_2a_1)y].$$

To check it is the Desargues involution, it sufficies to show that ω equals

$$\begin{aligned} (y_0x - x_0y)\Big(((b_1a_2 - b_2a_1)x_0 + (c_1a_2 - c_2a_1)y_0)x- \\ -((a_1c_2 - a_2c_1)x_0 + (b_1c_2 - b_2c_1)y_0)y\Big) \end{aligned}$$

as then it has roots $[x_0, y_0]$ and $\pi([x_0, y_0])$. So we collect coefficients for x^2, xy and y^2. Coefficient for x^2 is

$$\begin{aligned} y_0((b_1a_2-b_2a_1)x_0+(c_1a_2-c_2a_1)y_0) &= b_1a_2x_0y_0+c_1a_2y_0^2-(b_2a_1x_0y_0+c_2a_1y_0^2) = \\ &= a_2(b_1x_0y_0 + c_1y_0^2) - a_1(b_2x_0y_0 + c_2y_0^2) = \\ &= a_2(a_1x_0^2 + b_1x_0y_0 + c_1y_0^2) - a_1(a_2x_0^2 + b_2x_0y_0 + c_2y_0^2) = \\ &= a_2\omega_1(x_0, y_0) - a_1\omega_2(x_0, y_0), \end{aligned}$$

which is exactly the coefficient for x^2 in ω. Analogously coefficient for y^2 is

$$x_0((a_1c_2-a_2c_1)x_0+(b_1c_2-b_2c_1)y_0) = a_1c_2x_0^2+b_1c_2x_0y_0-(a_2c_1x_0^2+b_2c_1x_0y_0) =$$
$$= c_2(a_1x_0^2+b_1x_0y_0) - c_1(a_2x_0^2+b_2x_0y_0) =$$
$$= c_2(a_1x_0^2+b_1x_0y_0+c_1y_0^2) - c_1(a_2x_0^2+b_2x_0y_0+c_2y_0^2) =$$
$$= c_2\omega_1(x_0,y_0) - c_1\omega_2(x_0,y_0),$$

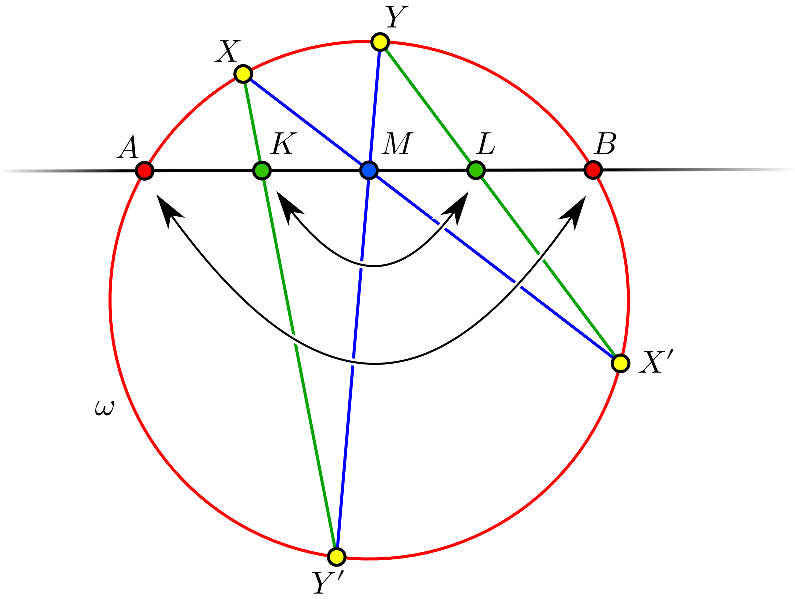
which is exactly the coefficient for y^2 in ω. And finally coefficient for xy is

$$-((b_1a_2-b_2a_1)x_0+(c_1a_2-c_2a_1)y_0)x_0-((a_1c_2-a_2c_1)x_0+(b_1c_2-b_2c_1)y_0)y_0 =$$
$$= b_2a_1x_0^2+c_2a_1x_0y_0+a_2c_1x_0y_0+b_2c_1y_0^2-(b_1a_2x_0^2+c_1a_2x_0y_0+a_1c_2x_0y_0+b_1c_2y_0^2) =$$
$$= b_2(a_1x_0^2+c_1y_0^2) - b_1(a_2x_0^2+c_2y_0^2) =$$
$$= b_2(a_1x_0^2+b_1x_0y_0+c_1y_0^2) - b_1(a_2x_0^2+b_2x_0y_0+c_2y_0^2) =$$
$$= b_2\omega_1(x_0,y_0) - b_1\omega_2(x_0,y_0),$$

which is exactly the coefficient for xy in ω. ■

Problem 6.1 (Butterfly theorem). Let ω be a circle and $A, B, X, Y \in \omega$ points on it. Denote M the midpoint of AB. Denote X' the second intersection of XM with ω and Y' the second intersection of YM with ω. Denote $K = Y'X \cap AB$ and $L = X'Y \cap AB$. Prove that M is the midpoint of KL.

Solution. Denote ϕ the involution on AB given by reflection by M. This involution clearly swaps (A, B), (M, M). Now let π be the Desargues involution given by conics passing through X, Y, X', Y' on AB. This swaps (A, B), as ω is one such conic, then it swaps (M, M) as $XX' \cup YY'$ is another such conic, and finally, it swappes (K, L) as $XY' \cup YX'$ is another such conic. As π and ϕ are linear they coincide on images of M, A, and B, they are the same involution. Hence M is the midpoint of KL.



7 Animation

Definition. We define a *moving point* as a polynomial mapping $\mathbb{P}^1 \to \mathbb{P}^2$. Hence it's given by three coprime homogenous polynomials of the same degree. We denote this degree as the *degree of a moving point.* For a moving point X, we denote its polynomials as X_p, X_q, X_r.

Definition. We define *moving line* as the polar of some moving point. And we denote *degree of a moving line* the degree of its pole.

7.1 Degree bounding

Proposition 7.1. Let A and B be two moving points with degrees d_a and d_b. If they coincide for k different values, then the degree of line AB is at most $d_a + d_b - k$.
Proof. Pole of line connecting two points is calculated using the cross product of given points, hence the moving line is given by

$$[A_qB_r - B_qA_r, A_rB_p - A_pB_r, A_PB_q - A_qB_p],$$

hence it has degree at most $d_a + d_b$. But for every $t = [t_1, t_2] \in \mathbb{P}^1$ such that

$$[A_p(t), A_q(t), A_r(t)] = [B_p(t), B_q(t), B_r(t)],$$

we get that

$$\begin{aligned}(A_qB_r - B_qA_r)(t) &= 0,\\ (A_rB_p - A_pB_r)(t) &= 0,\\ (A_PB_q - A_qB_p)(t) &= 0.\end{aligned}$$

Hence all these three polynomials share a common factor $(x_2t_1 - x_1t_2)$. Thus for every such t, we lower the degree by one. Hence the final bound is that the degree is at most $d_a + d_b - k$. □

Observation 7.2. As a dual we get that for two moving lines ℓ_1, ℓ_2 with degrees d_1, d_1, that coincide for k values, their intersection has degree at most $d_1 + d_2 - k$.

Proposition 7.3. Let A, B, C be three moving points with degrees at most d_a, d_b, d_c. Then if they are collinear for $d_a + d_b + d_C + 1$ choices of $t \in \mathbb{P}^1$, they are always collinear.
Proof. Three points are collinear if they are linearly dependent, hence when

$$\det\begin{pmatrix} A_p & A_q & A_r \\ B_p & B_q & B_r \\ C_p & C_q & C_r \end{pmatrix} = 0$$

But that is a polynomial of degree at most $d_1 + d_2 + d_3$, hence if it's nonzero, it has at most $d_1 + d_2 + d_3$ zeroes. □

Proposition 7.4. Let A, B be two moving points with degrees d_A and d_B respectively. If they coincide on $d_A + d_B + 1$ different values, they are the same moving point.
Proof. To check that point $[a, b, c]$ equals point $[x, y, z]$ we have to check that their cross product is zero

$$(bz - cy, cx - az, ay - bx) = (0, 0, 0)$$

That consists of three polynomials of degrees $d_A + d_B$. Hence if they are zero for $d_A + d_B + 1$ different values, they are always zero. ■

Theorem 7.5. Let X be a moving point with a degree $d_X > 0$, then image of X is a curve of degree d such that $d \mid d_X$.

Proof. Let the homogenous polynomials X_p, X_q, X_r be in $K[t, s]$. Then for points $k = [t_0, s_0]$ such that $X_r(k)$ is nonzero we have that image $X(k)$ is

$$\left[\frac{X_p(k)}{X_r(k)}, \frac{X_q(k)}{X_r(k)}, 1\right].$$

Thus a point $[a, b, 1]$ is in the image iff

$$\begin{aligned} X_p(k) - X_r(k)a &= 0 \\ X_q(k) - X_r(k)b &= 0 \end{aligned}$$

for some k. Which is equivalent to $X_p - X_r a$ and $X_q - X_r b$ having a common factor. Hence after homogenization we get that a point $[a, b, 1]$ is in the image iff

$$\operatorname{res}_{ts}(X_p c - X_r a, X_q c - X_r b)([a, b, 1]) = 0.$$

We denote

$$\pi'_{ab} = \operatorname{res}_{ts}(X_p c - X_r a, X_q c - X_r b).$$

Observe, that for points $[a, b, 0]$ the polynomials $-X_r a, -X_r b$ share a nontrivial factor X_r, hence $\pi'_{ab}[a, b, 0] = 0$. We will take a look how exactly π'_{ab} looks. So let

$$\begin{aligned} X_p &= p_0 s^d + p_1 s^{d-1} t + p_2 s^{d-2} t^2 + \cdots + p_{d-2} s^2 t^{d-2} + p_{d-1} s t^{d-1} + p_d t^d \\ X_q &= q_0 s^d + q_1 s^{d-1} t + q_2 s^{d-2} t^2 + \cdots + q_{d-2} s^2 t^{d-2} + q_{d-1} s t^{d-1} + q_d t^d \\ X_r &= r_0 s^d + r_1 s^{d-1} t + r_2 s^{d-2} t^2 + \cdots + r_{d-2} s^2 t^{d-2} + r_{d-1} s t^{d-1} + r_d t^d \end{aligned}$$

and look a the matrix

$$M = \begin{pmatrix} p_0 c - r_0 a & p_1 c - r_1 a & p_2 c - r_2 a & \cdots & p_d c - r_d a & 0 & \cdots & 0 \\ 0 & p_0 c - r_0 a & p_1 c - r_1 a & \cdots & p_{d-1} c - r_{d-1} a & p_d c - r_d a & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & p_0 c - r_o a & \cdots & \cdots & p_{d-1} c - r_{d-1} a & p_d c - r_d a \\ q_0 c - r_0 b & q_1 c - r_1 b & q_2 c - r_2 b & \cdots & q_d c - r_d b & 0 & \cdots & 0 \\ 0 & q_0 c - r_0 b & q_1 c - r_1 b & \cdots & q_{d-1} c - r_{d-1} b & q_d c - r_d b & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & q_0 c - r_o b & \cdots & \cdots & q_{d-1} c - r_{d-1} b & q_d c - r_d b \end{pmatrix}$$

We want to calculate it's determinant, so we will use the Leibniz formula. Denote indices of the first d_X rows as $v_1, v_2, \ldots, v_{d_X}$ and the indeces of the remaninig rows as $w_1, w_2, w_3 \ldots, w_{d_X}$. Suppose we want to calculate a term in the final determinant, that contains $c^{d'}$, where $d' < d_X$. We get it as a sum of some products of some permutations. Take a look at one such permutation ρ. As all terms are linear in c, to get $c^{d'}$ we had to not take the linear term in c from exactly $2d - d' > d$ terms. From Pidgeonhole principle we have some i such that we've not taken the linear term from terms on positions $(v_i, \rho(v_i))$, $(w_i, \rho(w_i))$. Suppose that i is the smallest such i. Then by altering ρ to ρ' such that $\rho'(v_i) = \rho(w_i)$ and $\rho'(w_i) = \rho(v_i)$ we get the same term in the result, but with a different sign. Thus we got a bijection on terms containing $c^{d'}$ that cancels them out. Hence the final result is a multiple of c^{d_X}. So we denote $\pi_{ab} = \pi'_{ab}/c^{d_X}$. Analogously we define π_{bc} and π_{ca}.

From construction we have that the image of X coincides with $V(\{\pi_{ab}\})$ on all points such that $c \neq 0$. Analogously the image of X coincides $V(\{\pi_{bc}\})$ on all points such that $a \neq 0$. And finally the image of X coincides with $V(\{\pi_{ca}\})$ on all points such that $b \neq 0$.

Let us look at the matrix for π_{bc}:

$$M_0 = \begin{pmatrix} q_0a - p_0b & q_1a - p_1b & q_2a - p_2b & \cdots & q_da - p_db & 0 & \cdots & 0 \\ 0 & q_0a - p_0b & q_1a - p_1b & \cdots & q_{d-1}a - p_{d-1}b & q_da - p_db & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & q_0a - p_ob & \cdots & \cdots & q_{d-1}a - p_{d-1}b & q_da - p_db \\ r_0a - p_0c & r_1a - p_1c & r_2a - p_2c & \cdots & r_da - p_dc & 0 & \cdots & 0 \\ 0 & r_0a - p_0c & r_1a - p_1c & \cdots & r_{d-1}a - p_{d-1}c & r_da - p_dc & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & r_0a - p_oc & \cdots & \cdots & r_{d-1}a - p_{d-1}c & r_da - p_dc \end{pmatrix}$$

We will transform M_0 into M. First, we swap the first d rows with the second d rows, and we multiply the new first d rows by -1 to get

$$M'_0 = \begin{pmatrix} p_0c - r_0a & p_1c - r_1a & p_2c - r_2a & \cdots & p_dc - r_da & 0 & \cdots & 0 \\ 0 & p_0c - r_0a & p_1c - r_1a & \cdots & p_{d-1}c - r_{d-1}a & p_dc - r_da & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & p_0c - r_oa & \cdots & \cdots & p_{d-1}c - r_{d-1}a & p_dc - r_da \\ q_0a - p_0b & q_1a - p_1b & q_2a - p_2b & \cdots & q_da - p_db & 0 & \cdots & 0 \\ 0 & q_0a - p_0b & q_1a - p_1b & \cdots & q_{d-1}a - p_{d-1}b & q_da - p_db & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & q_0a - p_ob & \cdots & \cdots & q_{d-1}a - p_{d-1}b & q_da - p_db \end{pmatrix}.$$

This multiplied the determinant by ± 1. Next for every $0 < i \leq d_X$ we replace row w_i with combination of rows $\frac{c}{a}w_i + \frac{b}{a}v_i$. This multiplies the determinant by $\frac{c}{a}$ for every i, thus overall we multiplied the determinant by $\pm\left(\frac{c}{a}\right)^{d_X}$. Hence we have that $c^{d_x}\pi_{ab} = \pm\left(\frac{c}{a}\right)^{d_X} \cdot a^{d_x}\pi_{bc}$. From this we conclude that $\pi_{ab} = \pm\pi_{bc}$ and analogously equals $\pm\pi_{ca}$. We know that for every point at least one of $V(\{\pi_{ab}\})$, $V(\{\pi_{bc}\})$, $V(\{\pi_{ca}\})$ coincides with the image of X, hence we get that $V(\{\pi_{ab}\})$ coincides with image of X on all points. And degree of π_{ab} is d_X.

Suppose that $\pi_{ab} = g_1 g_2 g_3 \cdots g_m$ for some nonconstant ireducible polynomials g_i. Then suppose that $V(g_i)$ is a proper subset of $V(\pi_{ab})$. Define W the set of all points $w \in \mathcal{P}^1$ such that $X(w) \in V(g_i)$; the preimage of W in X. Then W is a proper subset of P^1. Then W is the set of zeros of polynomial in $\mathcal{P}^1$ given by composition $g_i \circ X$. Thus it is finite. Hence $V(g_i)$ is finite. As $V(\pi_{ab})$ is infinite, for some i we have that $V(g_i)$ is infinite. Thus for such i we get $V(\pi_{ab}) = V(g_i)$.

Hence from 1.4 we have that $\pi_{ab} = cg_i^u$ for some $u \in \mathbb{N}, c \in \mathbb{C}$. Thus the image is a curve of degree d, such that $d \mid d_X$. ■

7.2 Degree preserving mappings

Observation 7.6. Composing a moving point A (a mapping $\mathbb{P}^1 \to \mathbb{P}^2$) with any linear mapping $\mathbb{P}^2 \to \mathbb{P}^2$ gives a moving point of the same degree.

Proposition 7.7. Connecting a moving point with a fixed point to get a line is a linear mapping.

Proof. Let $[a, b, c]$ be the fixed point, then the mapping is defined as

$$[x, y, z] \mapsto [bz - cy, cx - az, ay - bx],$$

hence it's linear. □

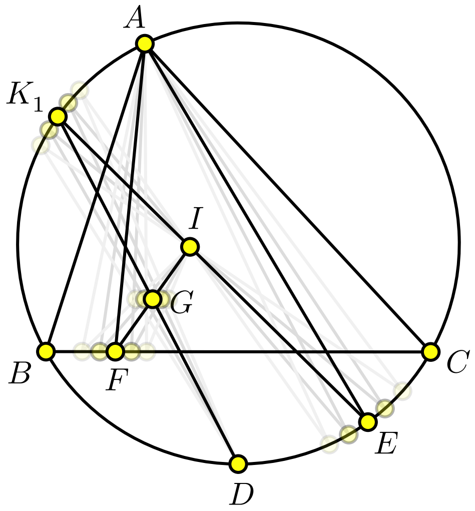
Proposition 7.8. Intersection of a moving line with a fixed line is a linear mapping.
Proof. It's dual to the proposition 7.8. □

Proposition 7.9. Let γ be a nondegenerate conic and P a point not lying on γ. Then there exists a linear mapping that maps each point $X \in \gamma$ to the second intersection of PX with γ.
Proof. Let p be the polar of P with respect to γ. As $P \notin \gamma$ we have that p intersects γ at two distinct points I, J. Now consider a linear mapping θ mapping $I \mapsto [1, i, 0]$ and $J \mapsto [1, -i, 0]$. Then this mapping maps γ to a conic passing through circle points, thus a circle. And line p gets mapped onto the infinity line. Hence the point P becomes the center of that circle. Reflection by this point τ is a linear mapping; hence we construct the final mapping as $\theta^{-1} \circ \tau \circ \theta$. Thus it's linear. □

Problem 7.1 (IMO 2010/P2). Let I be the incentre of a triangle ABC and let Γ be its circumcircle. Let the line AI intersect Γ again at D. Let E be a point on the arc BDC and F a point on the side BC such that

$$\measuredangle BAF = \measuredangle CAE < \frac{1}{2}\measuredangle BAC.$$

Finally, let G be the midpoint of the segment IF. Prove that the lines DG and EI intersect on Γ.



Solution. Define $K_1 = EI \cap \Gamma$. Let E be a moving point with degree 2 and locus Γ. Then from 7.9 we have that the degree of K_1 is 2. From 7.1, we have that degree of the line AE is at most 1. As the reflection by angle bisector BAC is a linear mapping, we have that degree of AF is one, hence from 7.2, we have that degree of F is at most 1. Homothethy with coefficient $\frac{1}{2}$ and center I is linear. Thus G has a degree at most 1. Again from 7.1, we have that degree of the line DG is at most 1 and the degree of the line DK_1 is at most one. Thus to confirm that $DK_1 = DG$, using dual of 7.4, we have to check three different positions of E.

- If $E = D$ then $DK_1 = DG = DA$.

- If $E = B$. Then K_1 is the center of the arc AC. And it sufficies to prove that K_1D is the bisector of CI. From symmetry it sufficies to prove that the triangle IDC is isosceles. Denote M the center of the arc BA. The conclusion follows from

$$\begin{aligned} \angle(ID, IC) = \angle(AD, AC) + \angle(AC, CM) = \\ = \angle(AB, AD) + \angle(CM, CB) = \angle(CI, CD). \end{aligned}$$

- If $E = C$, then from symmetry we use the same proof as for $E = B$ just rename B and C.

8 Cubic curves

Theorem 8.1 (Caley-Bacharach). Let ω_1 and ω_2 be two cubic curves intersecting at 9 different points. Then any any cubic curve passing through eight of those points passes through the ninth.
Proof. For proof see [2] Theorem CB3 named *Chasles*.

Definition. Any non-singular curve of degree three is called an *elliptic curve*.

Definition. Take any ireducible singular cubic curve γ with singular point Q. Then will call an *singular elliptic curve* the set $\gamma \setminus \{Q\}$.

Theorem 8.2. We can define a group operation on any elliptic curve ϵ as follows. Take any point $O \in \epsilon$ to be the zero. Then addition for points $A, B \in \epsilon$ is defined as follows. First, we construct C as the third intersection of the line AB and ϵ. Then construct D as the third intersection of OC with ϵ. Then $D = A + B$.
Proof. For singular elliptic curve see chapter *Singular cubic curves* in [6]. **TODO singular**

Observation 8.3. Independently of the choice of O we have for points $A, B, C \in \epsilon$ that $A + B + C = 0$ if and only if A, B, C are collinear.

Proposition 8.4. For points $A, B, C, D, E, F \in \epsilon$ we have that there is a conic passing through A, B, C, D, E, F if and only if $A + B + C + D + E + F = 0$.
Proof. Denote

- X the third intersection of AB with ϵ.
- Y the third intersection of CD with ϵ.
- Z the third intersection of EF with ϵ.

Then $X = -(A + B)$, $Y = -(C + D)$ and $Z = -(E + F)$. Hence from 8.3 we have that $A + B + C + D + E + F = 0$ if and only if X, Y, Z are collinear. Now let $\alpha = AB \cup CD \cup EF$. Then points A, B, C, D, E, F, X, Y, Z are the nine intersections of cubics α and ϵ. Hence from Caley-Bacharach theorem we have that X, Y, Z are collinear if and only if A, B, C, D, E, F lie on a conic. □

Problem 8.1 (IMO 2019/6). Let I be the incentre of an acute triangle ABC with $AB \neq AC$. The incircle ω of ABC is tangent to sides BC, CA, and AB at D, E, and F, respectively. The line through D perpendicular to EF meets ω at R. Line AR meets ω again at P. The circumcircles of triangles PCE and PBF meet again at Q. Prove that lines DI and PQ meet on the line through A perpendicular to AI.
Solution.
Lemma. Let B, F, E, C and T be five points. Then the set of all points X, such that radical axes of circumcircles of BFX and ECX pass through T, is cubic passing through the circle points. Additionally we have that B, F, E, C, T and $BF \cap EC$ lie on this cubic.
Proof. All circles passing through B, F form a pencil, so choose ω_1, ω_2 any two such circles as generators. Analogously choose γ_1 and γ_2 some generators of circles passing through E, C. Then to get a circle passing through BFX, we take a combination of ω_1 and ω_2, that is zero at X, that is

$$\omega = \omega_1(X)\omega_2 - \omega_2(X)\omega_1$$

Analogously we have that a circle passing through ECX is

$$\gamma = \gamma_1(X)\gamma_2 - \gamma_2(X)\gamma_1.$$

To get the radical axes we have to normalize these circles, hence the radical axes polynomial multiplied by z is

$$(\omega_1(X)-\omega_2(X))(\gamma_1(X)\gamma_2-\gamma_2(X)\gamma_1)-(\gamma_1(X)-\gamma_2(X))(\omega_1(X)\omega_2-\omega_2(X)\omega_1)$$

As T does not lie on the infinity line, T lies on the radical axis if and only if

$$\begin{gathered}(\omega_1(X)-\omega_2(X))(\gamma_1(X)\gamma_2(T)-\gamma_2(X)\gamma_1(T))- \\ -(\gamma_1(X)-\gamma_2(X))(\omega_1(X)\omega_2(T)-\omega_2(X)\omega_1(T))=0,\end{gathered}$$

which is a quartic polynomial in X. We want to show, that it is divisible by z to get a cubic polynomial. So we look at all terms that do not contain any z. In every circle those are exactly terms x^2 and y^2, but those cancel out in $\omega_1(X)-\omega_2(X)$ and in $\gamma_1(X)-\gamma_2(X)$. Thus every final term contains z, so we can write this as a $z\cdot\epsilon$ for some cubic ϵ.

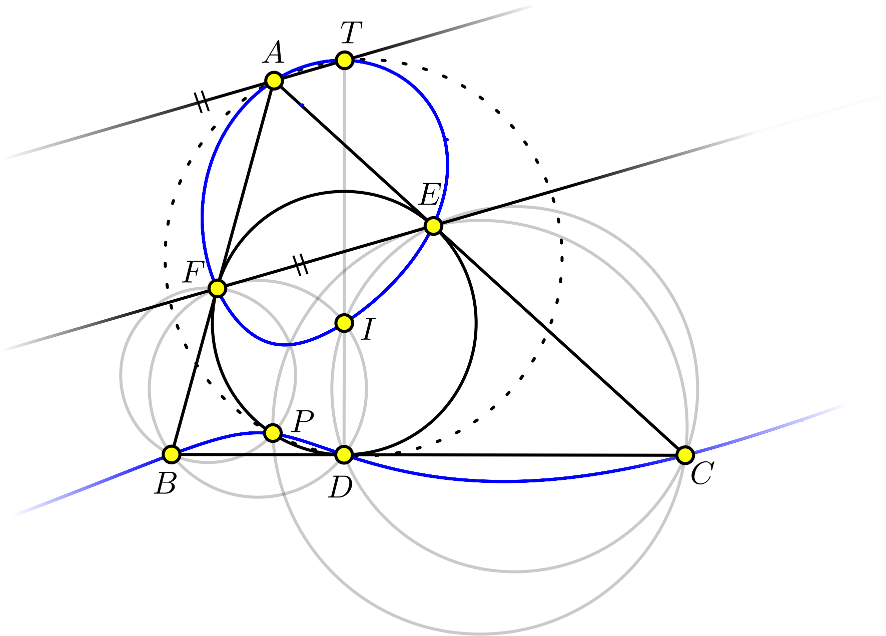
Now let us take one circle point $[1,i,0]$. We want to substitute it for X in ϵ. So every term containing z^2 will be zero in ϵ, as we set $z=0$. Every term that comes from a multiple of (x^2+y^2) will also be zero, as $1^2+i^2=0$. The remaining important terms are $\lambda_1 xz$ and $\lambda_2 yz$ from every circle. So we can take a look at expression containing only these terms:

$$\begin{gathered}(\omega_1'(X)-\omega_2'(X))(\gamma_1'(X)\gamma_2'(T)-\gamma_2'(X)\gamma_1'(T))- \\ -(\gamma_1'(X)-\gamma_2'(X))(\omega_1'(X)\omega_2'(T)-\omega_2'(X)\omega_1'(T)).\end{gathered}$$

Here every ω_k' is just a line passing through the origin, multiplied by z, and so is every γ_k'. But the construction remains the same, so we have some lines ω_1' and ω_2', which we weigh to get a line ω' passing through origin and T. Analogously we get γ' as a line passing through the origin and T. And then, we normalize them and subtract them. As they both are lines passing through the origin and T, after normalization, they are the same polynomial, so we get that the result is the zero polynomial. Hence when plugging $[1,i,0]$ into ϵ we get 0. Analogously for $[1,-i,0]$. Thus the circle points lie on ϵ.

Substituting $X=B$ we have $\omega_1(B)=\omega_2(B)=0$ which cancels all terms. Similarly with $X=F,E,C$. When $X=T$ we have $\gamma_1(T)\gamma_2(T)-\gamma_2(T)\gamma_1(T)=0=\omega_1(T)\omega_2(T)-\omega_2(T)\omega_1(T)$, which is zero. Denote $A=BF\cap EC$, as A lies on the radical axes of ω_1 and ω_2 we have $(\omega_1(A)-\omega_2(A))=0$ and similarly $(\gamma_1(A)-\gamma_2(A))=0$. Thus B, F, E, C, T and A lie on ϵ. □

Denote T the intersection of DI with the line passing through A perpendicular to AI. We want to prove, that P, Q, T are collinear. Look at triangle EDF with its circumcircle ω. We have $\angle(FD,DR)=\angle(FD,FE)+90°$. Denote M the midpoint of DE. From central angle we have that $\angle(FD,FE)=\angle(DI,IM)$, hence $\angle(DI,DE)=\angle(FD,FE)+90°=\angle(FD,DR)$. Denote D' the second intersection of DI with ω. From the inscribed angles we have that arcs FR and $D'E$ have the same length, thus $RD'\parallel FE\parallel AT$. As $RD'DP$ is cyclic we have $\angle(RP,RD')=\angle(DP,DD')$ and because of the parallel lines we have that $\angle(AP,AT)=\angle(DP,DT)$, hence $ATPD$ is cyclic. So we can forget the original definition of P and redefine it as the second intersection of circles ω and the circumcircle of ATD.



Denote J_1, J_2 the circle points. Observe that $DIEC$ and $DIFB$ are cyclic. From lemma we have A, B, F, E, C, T, P, Q, D, I, J_1, J_2 on one cubic ϵ. Using 8.3 and 8.4 we have that

$$T = -(D + I) = E + C + J_1 + J_2$$

Adding A to both sides and using 8.3 we have

$$T + A = (A + E + C) + J_1 + J_2 = J_1 + J_2.$$

Thus $TA \cap J_1J_2 \in \epsilon$. As J_1J_2 is the infinity line and $TA \parallel FE$, we get that

$$T + A = F + E$$

Hence finaly

$$D + F + E + J_1 + J_2 = D + T + A + J_1 + J_2$$

From that conics $DFEJ_1J_2$ and $DTAJ_1J_2$ intersect on ϵ, as they pass through J_1, J_2 they are just circles circumscribed to DFE and DTA respectively. Hence $P \in \epsilon$. Thus from the definition of ϵ, we have that the radical axis of circumcircles of PBF and PEF, in other words the line PQ, passes through T.

Problem 8.2. Let H be the orthocenter of $\triangle ABC$ with circumcircle ω and $D = AH \cap BC$. Let U, V be the points on BC such that $\measuredangle BHU = \measuredangle VHC$. Let PQ $(P, Q \in \omega)$ be the chord of ω passing through U. Let RS $(R, S \in \omega)$ be the chord of ω passing through V. Let H_P, H_Q, H_R, H_S be the orthocenters of $\triangle ADP, \triangle ADQ, \triangle ADR, \triangle ADS$, respectively. Prove that H_P, H_Q, H_R, H_S are concyclic.

Solution. Let H' be H reflected across BC. As $\angle(AB, AC) = \angle(CH, BH) = \angle(BH', CH')$, we have that $H' \in \omega$. Lines $H'U$ and $H'V$ meet ω for the second times at X and Y. Denote H_X and H_Y orthocenters of $\triangle ADX$ and $\triangle ADY$ respectively.

Lemma. Points H_P, H_Q, H_Y are collinear. And by symmetry H_R, H_S and H_X are collinear.

Proof. Denote $T = H_PH_Q \cap BC$. As $H_PP \parallel H_QQ \parallel H_YY \parallel BC$, we have $H_PT\colon H_QT = PU\colon QU$. Moreover

$$\angle(H_QD, DT) = \angle(AQ, AH') = \angle(XQ, XH') = \angle(XQ, XU).$$

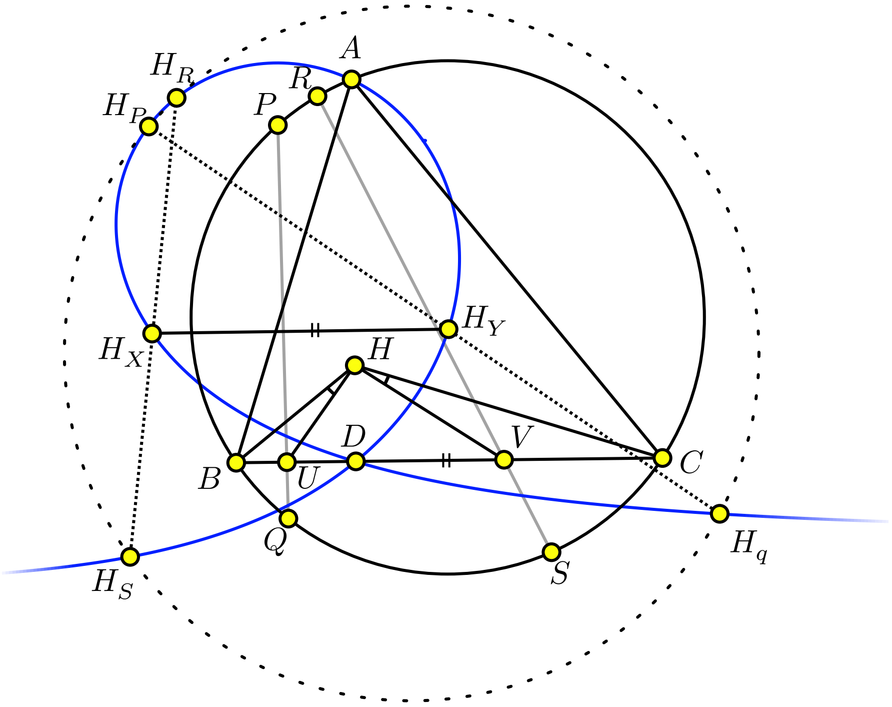
Analogously $\angle(H_PD, DT) = \angle(XP, XU)$. Angle observations gives us that $\triangle XPQ \sim \triangle DH_PH_Q$. And the ratio observation adds, that $\triangle XPQ \cup U \sim \triangle DH_PH_Q \cup T$. Let XY intersect H_PH_Q at H'_Y and PQ at W. Again from parallel lines we have $PW\colon QW = H_PH'_Y\colon H_QH'_Y$. Thus $\triangle XPQ \cup W \cup U \sim \triangle DH_PH_Q \cup H'_Y \cup T$. Hence

$$\angle(H'_YD, DT) = \angle(WX, XU) = \angle(XY, XH') = \angle(AY, AH').$$

As $AH' \perp DT$ we get that $AY \perp DH'_Y$. Thus $H'_Y = H_Y$. □

Lemma. Let K be a point on ω. Then locus of orthocenters of triangles ADK is elliptic curve ϵ.

Proof. Let ℓ be the infinity line. Denote $\infty_{\perp AK}$ the intersection of the perpendicular line to AK with line ℓ. Analogously denote $\infty_{\perp DK}$ the intersection of the line perpendicular to DK with ℓ. We animate K on ω with degree 2. Then from 7.1, we have that degree of AK is 1 and as rotation by 90° around A is linear, we have that degree of the line perpendicular to AK is 1. Thus from 7.2 we get that degree of $\infty_{\perp AK}$ is one, hence from 7.1 degree of $D\infty_{\perp AK}$ is one. Similarly, we get that degree of DK is 2. Hence the degree of $A\infty_{\perp DK}$ is 2. As the orthocenter of ADK is the intersection $A\infty_{\perp DK} \cap D\infty_{\perp AK}$, we have that its degree is at most 3. Hence from 7.5, it moves along a curve of degree 3. □



Lemma. Denote ∞_{BC} the intersection of ℓ with BC. Then $\infty_{BC} \in \epsilon$.

Proof. Take $K = H' \in \epsilon$. Then $A\infty_{\perp DH'} \parallel BC \parallel D\infty_{\perp AH'}$. Thus their intersection is $\infty_{BC} \in \epsilon$ and it lies on ϵ.

Lemma. Denote J_1, J_2 the circle points. Then $J_1, J_2 \in \epsilon$.

Proof. Point J_1 lies on ω. Let us find the orthocenter of J_1AD. Rotation matrix for rotation by 90° around A is a matrix of a form

$$\begin{pmatrix} 0 & -1 & a \\ 1 & 0 & b \\ 0 & 0 & 1 \end{pmatrix}.$$

From definition it maps $A \mapsto A$ and it maps $[1, i, 0] \mapsto [-i, 1, 0] = -i[1, i, 0] = [1, i, 0]$. Thus it fixes line AJ_1. Analogously rotation around D fixes line DJ_1. And translation also fixes the infinity line, thus J_1 lies on both $A\infty_{\perp DJ_1}$ and $D\infty_{\perp AJ_1}$, thus it lies on ϵ. Analogously for J_2. □

Thus we have points H_X, H_Y, H_P, H_Q, H_R, H_S, J_1, J_2, ∞_{BC} on one elliptic curve ϵ. As $H_XH_Y \parallel BC$ and J_1J_2 is the infinity line, we have that $H_XH_Y \cap J_1J_2 = \infty_{BC} \in \epsilon$. Thus $H_X + H_Y = J_1 + J_2$. From this and given lines we have

$$(J_1 + J_2) + H_P + H_Q + H_R + H_S = (H_X + H_Y) + H_P + H_Q + H_R + H_S = 0$$

Thus from 8.4 points J_1, J_2, H_P, H_Q, H_S, H_R lie on one conic and as this conic passes through J_1, J_2 we have that points H_P, H_Q, H_S, H_R are concyclic.

Conclusion

We've presented different algebraic techniques for olympiad geometry problems. Usually these geometry problems are solved just using similar triangles and angle chasing. As shown here, there can be alot of different approaches to solving a gemetry problem.

The Method of Animation is from my own experience the strongest and most widely usable method presented here. As it allows to solve the problem just in some degenerate cases and from that deduce that it holds everywhere.

I believe that the method utilizing elliptic curves could become more frequent when people find some more examples of cubic curves in olympiad problems..

Bibliography

[1] Chroman Z., G. K. Goel, and A. Mudgal (2019). The Method of Animation. https://cdn.bc-pf.org/resources/math/geometry/bash/Chroman_Goel_Mudgal-The_Method_of_Animation.pdf

[2] Eisenbud, D., M. Green, and J. Harris (1996). Cayley-Bacharach Theorems and Conjectures. *Bulletin of the American Mathematical Society*. Vol. 33, #3, July 1996. Pages 295 to 324.

[3] Fulton, W. (2008). Algebraic Curves (An Introduction to Algebraic Geometry). https://dept.math.lsa.umich.edu/~wfulton/CurveBook.pdf

[4] Kala, V. (2021). Komutativní okruhy. https://karlin.mff.cuni.cz/~kala/files/KO-2021.pdf

[5] Nguyen, N. P. (2019). A Generalization of Desargues' Involution Theorem. https://arxiv.org/abs/1912.12200

[6] Silverman, J. H., and J. late (2015). Rational Points on Elliptic Curves. *Springer.*

[7] Washington, L. C. (2008). Elliptic Curves, Number Theory and Cryptography. *Chapman & Hall/CRC.*

[8] The Art of Problem Solving forum. https://artofproblemsolving.com/