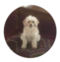
# On points constructible from conics

**Article** *in* The Mathematical Intelligencer · January 1997

DOI: 10.1007/BF03024434





Carlos R. Videla
Mount Royal University

# On points constructible from conics

Carlos R. Videla

**Abstract**

We prove: a complex number $z$ is conic constructible if and only if $z$ is algebraic over $\mathbf{Q}$ and the normal closure $F$ over $\mathbf{Q}$ of $\mathbf{Q}(z)/\mathbf{Q}$ has dimension $2^s3^t$ $s$, $t \geq 0$ over $\mathbf{Q}$.

One important concern of ancient Greek mathematics was the construction of points in the plane using an unmarked ruler and compass. They were unable to decide whether or not certain constructions where possible most notably: 1) the duplication of the cube; 2) trisection of an angle; 3) construction of the regular 7–sided polygon; and 4) the squaring of the circle. One learns in a Galois theory course how to characterize algebraically points that are constructible in this sense and it follows that these four problems are indeed impossible to solve. This is a beautiful achievement of the algebraic formulation of geometric problems i.e. the new mathematics started by Descartes and Fermat in the $17^{th}$ century. A natural question is: what points can be constructed if we are allowed to draw conics?

In antiquity it was known how to solve problems 1 and 2 using parabolas and hyperbolas. The solutions are given in theorems A and B below, which I found mentioned in several places and in one book as exercises (with solutions). There was no mention of a solution using conics of the heptagon problem (nor of the origin of the theorem B). This is what got me started. In this note we characterize algebraically the set of points that can be conswtructed from conics and as a corollary prove that problem 3 can be solved. Problem 4 is not solvable due to the transcendencing of $\pi$. The editor of this journal urged me to find the origin of theorem B. While doing this I found out that Archimedes had solved problem 3. His solutions is remarkable.

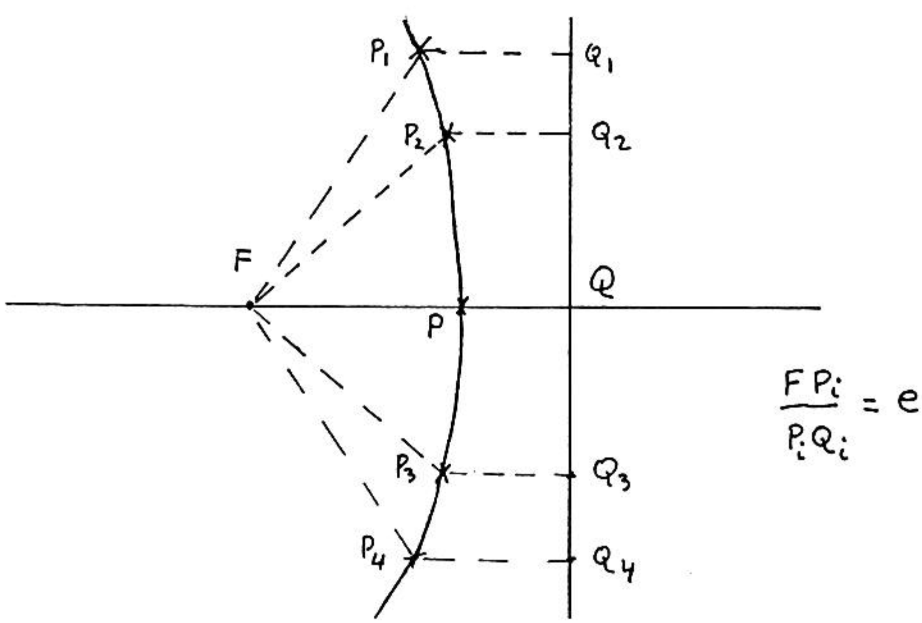
In [3], which I consulted first, theorem B is traced to Pappus. Later, I consulted Heath's second work [4] which is a condensed version of [3] except for one major addition: Archimedes' solution of the heptagon problem (see [4] p. 340). The Greek manuscript is lost but the great Arab geometer Thabit ibn Qurra (836–911) made a translation. It was only in the 1920's that C. Schoy found Qurra's translation in Cairo (Heath's work [3] is form 1921).

We now give the necessary definitions to make the concept of "constructible from conics" precise. The Greek geometers defined a conic section (or simply conic) to be the locus of intersection of a right circular cone with a plane. Excluding circles and lines, the following focus–directrix property of conics was discovered (it is implicit in Euclid's "Surface Loci" and explicitly stated as a proposition in Pappus' "Lemmas to the Surface Loci" see [4] p. 153 and p. 266): the locus of a point which moves so that its distance from a fixed point (called a focus) is in a constant ratio (called the eccentricity) to its distance from a fixed straight line (called a directrix) is a conic section, which is a ellipse, a parabola or an hyperbola according as the given ratio is less than, equal to or greater than unity. See the figure below. We will use this property in our definition.

Let $S = \{P_1, \ldots, P_n\}$ be $n$ points in the plane. Define sets $S_m$ for $m = 1, 2, \ldots$ as follows: $S_1 = S$, and $S_{m+1}$ is the union of $S_m$ and (1) the set of points of intersections of pairs of lines connecting distinct points of $S_m$, (2) the set of points of intersections of lines specified in (1) with all circles having centers in $S_m$ and radii equal to segments having end points in $S_m$, (3) the set of points of intersections of lines specified in (1) with all parabolas, ellipses and hyperbolas having focii in $S_m$, directrix lines which are lines as specified in (1) and eccentriaties equal to the length of a segment having end points in $S_m$, (4) the set of points of intersections of pairs of conics defined in (2) and (3).

Let $C(S) = \bigcup_{m=1}^{\infty} S_m$. We call this set of points the set of conic constructible points from $S$.

Compare with [5] p. 216.



We will only concern ourselves with $S = \{P, Q\}$. We choose a coordinate system in which $P = (0, 0)$ and $Q = (1, 0)$ and identify points in the plane with complex numbers $P = z = x + iy$. From now on we call a complex number $z$ a conic constructible point if $z \in C(P, Q)$. We write $\tilde{C}$ instead of $C(P, Q)$.

# 1 Cardano's formulas and some results of the Greeks.

1.1 We need to know how one can solve by radicals cubic and quartic equations. This is well known, and basically contained in Cardano's formulae in Ars Magna, see [5] p. 205. Let $K$ be a field of characteristic not equal to 2 or 3 and let $f = x^3 + a_2x^2 + a_1x + a_0$ be un irreducible cubic over $K$. Let $y = x + \frac{1}{3}a_2$. Then $f = y^3 + py + q$ where $p = q_1 - \frac{1}{3}a_2^2$, and $q = a_0 + \frac{2}{27}a_2^3 - \frac{1}{3}a_2a_1$. We show, following Cardano, how to solve $y^3 + py + q = 0$ and therefore how to solve $x^3 + a_2x^2 + a_1x + a_0 = 0$. Let $L$ be a splitting field of $x^3 + px + q$ over $K$. There is s $\delta \in L$ such that $\delta^2 = \Delta = 4p^3 - 27q^2$, the discriminant of $x^3 + px + q$. Let $w$ be a cube root of unity different to 1. We know that $w^2 + w + 1 = 0$ so $p(x) = x^2 + x + 1$ is the minimum polynomial of $w$ over $K$, unless $w \in K$. Consider the following diagram of fields

$$\begin{tikzcd}[column sep=small]
 & L(\omega) \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash] & & K(\delta, \omega) \arrow[dl, dash] \\
 & K(\delta) \arrow[d, dash] & \\
 & K &
\end{tikzcd}$$

In the field $L(w)$, set $\beta = \alpha_1 + w\alpha_2 + w^2\alpha_3$ and $\gamma = \alpha_1 + w^2\alpha_2 + w\alpha_3$ where $\alpha_1, \alpha_2, \alpha_3$ are the three roots of $x^3 + px + q = 0$.

It follows that $\beta^3$ and $\gamma^3$ are the elements $\frac{27}{2}q \pm \frac{3}{2}(2w+1)\delta$. Hence $\beta^3$ and $\gamma^3$ belong to the field $K(\delta, w)$ which is an extension of degree at most four over $K$ and if it has degree four it has a subfield $K(\delta)$ of degree 2 over $K$. Notice that $\gamma = -3p/\beta$, and that $\alpha_1 = \frac{1}{3}(\beta + \alpha)$, $\alpha_2 = \frac{1}{3}(w^2\beta + w\gamma)$, $\alpha_3 = \frac{1}{3}(w\beta + w^2\gamma)$.

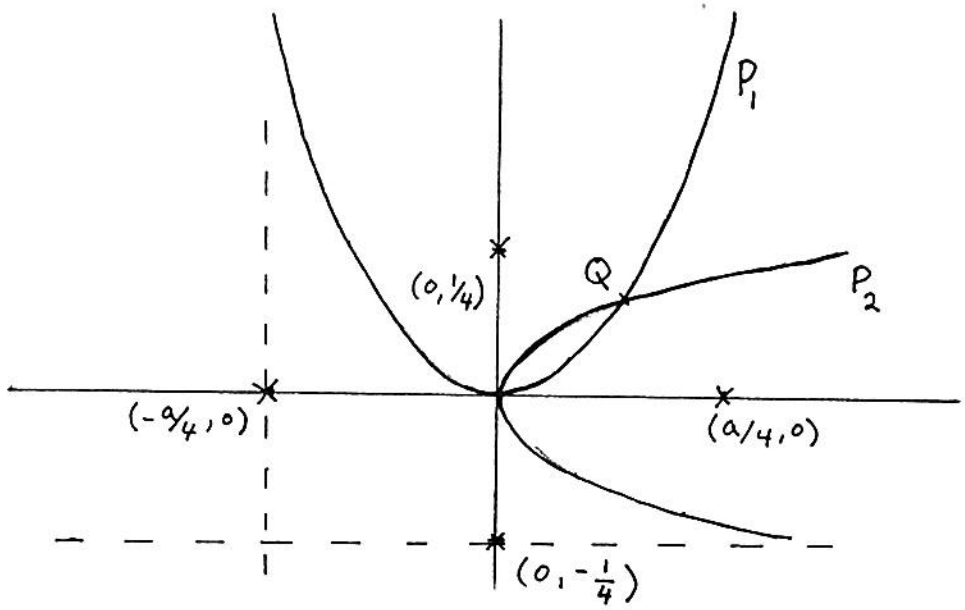
Hence $L(w) = K(\delta, w, \beta)$; so $[L(w) : K(\delta, w)]$ is at most 3 but in any case $L(w) = K(\delta, w)(\beta)$ with $\beta^3 \in K(\delta, w)$. We have shown that if $\alpha$ is a root of $x^3 + px + q = 0$ then there exist fields $K \subset K(\delta) \subset K(\delta, w) \subset K(\delta, w, \beta)$ such that $\delta^2 \in K, w^3 \in K(\delta), \beta^3 \in K(\delta, w)$ and $\alpha \in K(\delta, w, \beta)$. In the terminology of Theorem 2 below the roots of a cubic equation belong to a (2,3)–tower over $K$. The case of quartic polynomials is treated in a similar way (see [2] p. 115) and in particular one defines a sequence of fields $K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset K(\alpha_1, \alpha_2, \alpha_3) \subset K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ where $\alpha_1^n \in K$ and $\alpha_i^n \in K(\alpha_1, ..., \alpha_{i-1})$ for $i = 2, 3, 4$, and $n \in \{2, 3\}$; the roots of the quartic equation will belong to $K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$. So we also have a (2,3)–tower over $K$.

1.2 The Greeks were unable to duplicate the cube and trisect any given angle, only using a ruler and compass. However, they were able to do so in other ingenious ways: using conics and "movable" mechanisms. Plato constructed one such mechanism for duplicating the cube. We will need the following.

This is probably not true

**Teorem A.** (Menaechmus ≈ 350 B.C. tutor of Alexander the Great). Given the length a, one can determine using parabolas a segment of length $c$ such that $c^3 = a$.

Proof: The construction is contained in the following diagram:




The parabola $P_1$ has the constructible point $(0, 1/4)$ as focus and the constructible line $y = -1/4$ as directrix. Its cartesian equation is $y = x^2$. The parabola $P_2$ has the constructible point $(a/4, 0)$ as focus and the constructible line $x = -a/4$ as directrix. Its cartesian equation is $x = \frac{y^2}{a}$. The points of intersection are given by solving

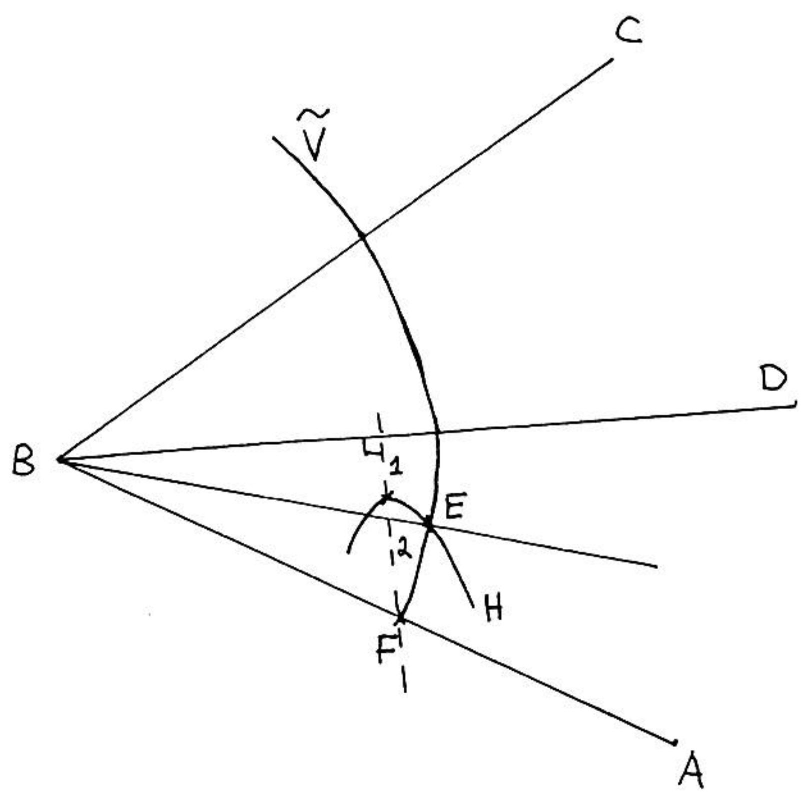
$$y = x^2 = \frac{y^4}{a^2}$$

$$\text{so} \quad y(a^2 - y^3) = 0 \quad \text{so} \quad y = 0, \sqrt[3]{a^2}$$

Hence the point labelled $Q$ is $(a^{1/3}, a^{2/3})$.

**Theorem B** (Pappus $\approx$ third century $A.D$). Given an angle $\sphericalangle ABC$ one can construct an angle whose measure is a third of the measure of $\sphericalangle ABC$.

Proof: The construction is contained in the following diagram:




Given the angle $\angle ABC$, bisect it by choosing any point $F$ on $\overline{AB}$. Let $\angle FBD$ be half $\angle ABC$.

Construct the hyperbola $H$ of eccentricity 2 having $F$ as focus and $\overline{BD}$ as directrix. Draw the circle $\tilde{V}$ of centre $B$ and radius $\overline{BF}$. Let $E$ be the point of intersection of $H$ and $\tilde{V}$. Draw the line through $B$ and $E$. Then the angle $\angle EBF$ trisects $\angle ABC$. We leave the proof of this last statement to the reader.

As the referee pointed out, by the $17^{\text{th}}$ century it was known how to solve any equation of degree 4 or less using conics, see [1] p.155 (the reference was supplied by the referee). This follows from theorems A and B together with the observations in 1.1. Since a point $z = x + iy$ is constructible if and only if $x$ and $y$ are, in order to construct the heptagon it is necessary and sufficient to construct the numbers $\cos\frac{2\pi}{7}$ and $\sin\frac{2\pi}{7}$, and hence it is enough to construct one of them, say $\cos\frac{2\pi}{7}$. If we could write down an equation of degree at most four with coefficients which were known to be constructible we would be done. It is possible to write down an equation of degree 6 with integer (hence constructible) coefficients which has $\cos\frac{2\pi}{7}$ as solution. One could try to factorize this polynomial over $\mathbb{Q}$ or over a quadratic extension of $\mathbb{Q}$ and hence solve the problem. We do not pursue this any further and proceed to the algebraic characterization.

## 2 The algebraic characterization.

In this section we characterize in terms of field extensions the points constructible by conics.

**Theorem 1.** The set $\tilde{C}$ of conic constructible points is the smallest subfield of $\mathbb{C}$ closed under conjugation, square and cube roots.

Proof: It is well known how to construct (in fact, using only ruler and compass) $z + z', zz', z/z'$ if $z' \neq 0, \overline{z}$ and $\sqrt{z}$ from $z$ and $z'$. Now suppose $z = re^{i\theta}$ is given. To construct any one of the three cube roots of $z$ one has to determine a length $d$ equal to $r^{1/3}$ and an angle $\alpha$ equal to $\theta/3$. This was done by the Greeks as explained above.

Now let $C'$ be a subfield of $\mathbb{C}$ closed under conjugation and square and cube roots. We will show that points obtained by intersecting conics whose definitions involve points and lengths of segments joining points of $C'$ all belong to $C'$. This shows that $C' \supset \tilde{C}$. As in the classical case if $z = x + yi \in C'$, $x$ and $y$ real then $x, y \in C'$ and conversely. It follows that if the conic is constructed from data belonging to $C'$ then its equation $ax^2 + bxy + cy^2 + dx + ey + f = 0$ (where $a, b, c, d, e, f$ are real) has its coefficients in $C'$. Let $E'$ be another conic with equation

$$a'x^2 + b'xy + c'y^2 + d'x + e'y + f' = 0$$

with real coefficients belonging to $C'$ (we assume $E \neq E'$ and that neither $E$ nor $E'$ is a line since this case is trivial). Then $E \cap E'$ has at most four points. The $x$-coordinates (or $y$-coordinates depending on the coefficients of the equations) of these points are obtained by solving these two equations simultaneously. This leads to either $P(x) = 0$ or $Q(y) = 0$ where

$P$ and $Q$ are polynomials with real coefficients belonging to $C'$ of degree at most 4. By what we remarked before it follows that the roots of these polynomials are obtained by taking square and cube roots of elements in $C'$. Supposing we have determined in this way the $x$-coordinates of the points of intersection say, we may by substitution and solving a quadratic equation determine the $y$-coordinates. Hence, if $P = x + iy$ with $P$ an intersection point we get $P \in C'$. It remains to show how one can construct the polynomials $P(x)$ or $Q(y)$ mentioned above. The troublesome term is the $xy$ term.

We have three combinations to consider:

a) $b = b' = 0$ b) $bb' \neq 0$ and c) $b = 0, b' \neq 0$ or viceversa

Case a) is simple. Multiplying apropriately and adding both equations one finds that the points of intersection of $E$ and $E'$ are given by the points of intersection of $E$ say and $E''$ where $E''$ is a conic with equation

$$a''x^2 + d''x + e''y + f'' = 0 \qquad \text{or} \qquad c''y^2 + d''x + e''y + f'' = 0.$$

Depending on these two possibilities one has by substitution either $P(x) = 0$ or $Q(y) = 0$ with $P, Q$ of degree at most four and real coeficients in $C'$.

Case b) can be reduced to case c) by multiplying appropriately (so that $b' = b = 1$ say) and subtracting. So the points of $E \cap E'$ are the same as those in $E \cap E''$ where $E''$ is a conic with no $xy$ term.

Suppose the conic $E$ has an $xy$ term but that $E'$ does not. It follows that the axis of the conic $E'$ is at right angles with our $(x, y)$-coordinate system.

We can translate using ruler and compass both conics $E \to \tilde{E}$ and $E' \to \tilde{E}'$ so that the centre of $\tilde{E}'$ is at $(0, 0)$. Note that the coefficients of the cartesian equations of $\tilde{E}$ and $\tilde{E}'$ still belong to $C'$.

We distinguish three situations:

I) $\tilde{E}'$ is a parabola. In this case $\tilde{E}'$ has equation of the form $y = \alpha x^2 + \beta$ or $x = \alpha y^2 + \beta$ with $\alpha, \beta \in C' \cap \mathbb{R}$. By substitution in the equation of $\tilde{E}$ one readily obtains an equation

$$P(x) = 0 \qquad \text{or} \qquad Q(y) = 0$$

of degree at most 4 as desired. In this way we get $\tilde{E} \cap \tilde{E}' \subset C'$ and by translation $E \cap E' \subset C'$.

II) $\tilde{E}'$ is a circle or an ellipse. In this case $\tilde{E}'$ has an equation of the form $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 1$ $\alpha, \beta \in C' \cap \mathbb{R}$.

Suppose the equation of $\tilde{E}$ is $ax^2 + bxy + cy^2 + dx + ey + f = 0$ writing $x^2 = \alpha^2(1 - \frac{y^2}{\beta^2})$ and substituting into $\tilde{E}'s$ equation we get:

$$a\alpha^2(1 - \frac{y^2}{\beta^2}) + cy^2 + ey + f = x(-by - d) = -x(by + d)$$

Squaring and arranging we get

$$(a\alpha^2(1 - \frac{y^2}{\beta^2}) + cy^2 + ey + f)^2 - (by + d)^2\alpha^2(1 - \frac{y^2}{\beta^2}) = 0$$

Calling the left hand side $P(y)$ we have obtained what we wanted.

III) $\tilde{E}'$, is a hyperbola, with equation $\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} = 1$. This is treated as above.

The following is a useful criterion to find out when a point $z$ is conic constructible.

**Theorem 2.** Let $z \in \mathbb{C}$ be given. Then $z$ is conic constructible if and only if $z$ is contained in a subfield of $\mathbb{C}$ of the form $\mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_l)$ where $\alpha_1^n \in \mathbb{Q}$ and $\alpha_i^n \in \mathbb{Q}(\alpha_1, ..., \alpha_{i-1})$ for $2 \leq i \leq l$ and $n \in \{2, 3\}$. We will call such a field a (2,3)–tower over $\mathbb{Q}$.

Proof: Let $C'$ be the set of complex numbers contained in an (2,3)–tower over $\mathbb{Q}$.

Since $\tilde{C}$, is closed under square and cube roots we get $\tilde{C} \supset C'$. For the other inclusion note that $C'$ is a subfield of $\mathbb{C}$ closed under square and cube roots. Since $\overline{\mathbb{Q}(\alpha_1, ..., \alpha_l)} = \mathbb{Q}(\overline{\alpha}_1, ..., \overline{\alpha}_l)$ it follows that $C'$ is closed under conjugation.

The next result is the main point.

**Theorem 3.** A complex number $z$ is conic constructible if and only if $z$ is algebraic over $\mathbb{Q}$ and the normal closure $K/\mathbb{Q}$ of $\mathbb{Q}(z)/\mathbb{Q}$ has dimension $2^n 3^m$ $(m, n \in \mathbb{N})$ over $\mathbb{Q}$.

**Proof:** Suppose $z$ is conic constructible. By theorem 2 it is contained in an (2,3)–tower $\mathbb{Q}(\alpha_1, ..., \alpha_l)$. We may assume this (2,3)–tower is a Galois extension over $\mathbb{Q}$ (see Lemma 5 p. 255 of [5]). Hence the normal closure $K/\mathbb{Q}$ of $\mathbb{Q}(z)/\mathbb{Q}$ which is a subfield of $\mathbb{Q}(\alpha_1, ..., \alpha_l)$ has dimension $2^n 3^m$ over $\mathbb{Q}$. Conversely, suppose the normal closure $K/\mathbb{Q}$ of $\mathbb{Q}(z)/\mathbb{Q}$ has dimension $2^s 3^t$ over $\mathbb{Q}$. The Galois group $G = Gal(K/\mathbb{Q})$ has order $2^s 3^t$.

By Burnside's $p-q$ theorem (see [6] p. 240) $G$ is solvable. Therefore $G$ has a decomposition series $G = G_1 \rhd G_2 \rhd G_3 \cdots \rhd G_k = 1$ such that $G_i/G_{i+1}$ is of order 2 or 3. By the main theorem of Galois theory we have a sequence of subfields $F_i$ of $K$ such that

$$\mathbb{Q} = F_1 \subset F_2 \subset F_3 \subset \cdots \subset F_l = K$$

where $[F_{i+1} : F_i] = 2$ or 3. Write $F_{i+1} = F_i(\alpha_i)$. Any degree 2 extension is obtained by adjoining a square root. If the extension $F_{i+1}/F_i$ is of degree 3 and not obtained by adjoining a cube root then the tower at the $i^{th}$ extension $F_i \subset F_{i+1}$ can be replaced by a sequence $F_i \subset L_i' \subset L_i'' \subset L_i''', \alpha_i \in L_i'''$ which is a (2,3)–tower as explained in 1.1. Hence $z$ belongs to a (2,3)–tower over $\mathbb{Q}$ and so is contructible by theorem 2.

# 3 Constructible regular polygons.

Next we find out which regular polygons are constructible.

**Theorem 4.** The regular $n$ sided polygon is conic constructible if and only if $n = 2^s 3^t p_3 ... p_i ... p_k$ with $s, t \geq 0$, $p_i \neq 2, 3$; $p_i \neq p_j$ $3 \leq i, j \leq k$ and the prime factors of $p_i - 1$ are 2 or 3.

Proof: Following Gauss, one has to construct the number $z = e^{2\pi i/n}$. Let

$F_n$ be the cyclotomic field of $n^{th}$ roots of unity. $F_n/\mathbb{Q}$ is Galois and has degree $\varphi(n)$. If $n = 2^s 3^t p_3^{e_3} ... p_k^{e_k}$ $s \geq 1$ $t \geq 1$ then $\varphi(n) = 2^s 3^{t-1} p_3^{e_3 - 1}(p_3 - 1) ... p_k^{e_k - 1}(p_k - 1)$. If $t = 0$ or $s = 0$ one obtains a similar formula; so $e_i = 1$ $i = 3, ..., k$ and $p_i - 1$ must only have 2 or 3 as its prime divisors.

**Corollary.** The 7–gon is conic constructible.

**Proof:** $\varphi(7) = 6 = 2.3$.

**Remarks:** It turns out that ellipses are superfluous in the construction of new points. Can one get by using only lines, circles and hyperbolas?

Conics are curves of genus cero. What points do we get if we are also allowed to draw curves of genus 1 i.e. cubics?

**References.**


1. L. Bieberbach, Theorie der Geometrichen Konstruktionen, Birkhäuser 1952.

2. D.J.H. Garling, A course in Galois Theory, Cambridge University Press, Cambridge 1986.

3. T.L. Heath, A history of Greek Mathematics, 2 volumes, Oxford University Press, Oxford 1960.

4. T.L Heath, A manual of Greek Mathematics, Dover Publications, New York 1963.

5. N. Jacobson, Basic Algebra I, W.H. Freeman & Co., New York 1985.

6. D. Robinson, A course in the theory of Groups, G.T.M. # 80, Springer–Verlag, New York 1982.