Milestone lecture. Here we look back at Greek geometry from approximately the 19th century, in the framework of 17th century algebraic geometry. Some highlights along the way:

- The equivalence of algebraic problems and geometric ones in particular cases was known to the Greeks.
- A clear general statement regarding 3rd degree equations by Persian mathematicians, Al Biruni (973-1048), Omar Khayyam (1048-1131).
- General solution of 3rd and 4th degree equations with radicals, 16th century Italian mathematicians; there, complex numbers appear implicitly, and questions of symmetry can be seen with hindsight. A beautiful short exposition by Alain Connes can be found in ftp://ftp.alainconnes.org/symetries.pdf and in English in Issue 54 of the Newsletter of the European Mathematical Society (should appear in http://www.emis.de/newsletter/). The solution with radicals of 5th degree equations becomes a famous open problem. In the 19th century, Abel demonstrates impossibility of general solution. Galois sees clearly that symmetries are the key notion for studying fields of numbers.

1. Geometry from algebra

Two equivalent structures:
- A plane admitting constructions with straightedge and compass.
- An ordered field, with square root of non-negative elements.

Algebraic geometry takes the field $F$ as a point of departure. We first construct a plane geometry $\Pi(F)$, consisting of points, lines, and circles. A point of the plane $\Pi = F^2$ is an ordered pair $(a,b)$ of elements of $F$.

A line $L$ in $\Pi$ is defined by an equation $ax + by = c$, where $a,b,c \in F$, not both $a = b = 0$;

$$L = L_{a,b,c} = \{(x,y) : ax + by = c\}$$

A circle is defined by an equation: $(x - p)^2 + (y - q)^2 = r^2$ with $p,q,r \in F$.

Excercise 1.1. (1) Any two lines of $\Pi(F)$ meet in at most one point.

(2) Through any two points there passes exactly one line. (Postulate 1 of Book I of the Elements)

(3) A line and a circle intersect in at most two points.

(4) Deduce (2) directly from (1) (or even (1'): through any two points there passes at most one line.)

Excercise 1.2. Assuming $1 + 1 \neq 0$ in $F$, show that any element of $F$ can be written as the difference of two squares. Compare to: Euclid Book II Proposition 8.

Now assume $F$ is an ordered field. (In 20th century algebra, this notion is defined abstractly; if you haven’t seen the definition, you can take $F$ to be a subfield of $\mathbb{R}$, and use the usual ordering $x < y$.) Then we can define the inside and outside of a circle: the inside is $\{(x,y) : (x - p)^2 + (y - q)^2 < r^2\}$. The center is the point $(p,q)$.

Excercise 1.3. If two (equations for) lines have a point of intersection with coordinates in $\mathbb{R}$, this point already has coordinates in $F$. Can you formulate an axioms about the existence of an intersection point, true in $\Pi(F)$, and simpler than Postulate 5 of Euclid’s Book 1?

The following axiom is never mentioned explicitly in Euclid, but can be seen in its use as one of the fundamental principles of construction.

Axiom 1.4. Let $C$ be a circle of radius $r$, and let $L$ be a line passing through some interior point of $C$. Then $C$ intersects $L$. 1
The condition of the excercise can be restated: the distance from the center of \( C \) to some point of \( L \) is \(< r \).

**Theorem 1.5.** The following conditions on an ordered field \( F \) are equivalent:

1. Every positive element of \( F \) has a square root.
2. The plane \( \Pi(F) \) admits constructions by straightedge and compass (in particular Axiom 1.4 holds.)

**Exercise:** prove this theorem. Hint for (2) \( \rightarrow \) (1): by considering the intersection of the line \( y = b \) with the circle \( x^2 + y^2 = a^2 \), conclude that \( b^2 - a^2 \) has a square root in \( F \) whenever \( 0 < a < b \in F \). Then use Example 1.2.

**Exercise 1.6.** Assume Axiom 1.4 holds in \( \Pi(F) \). Let \( C_1, C_2 \) be circles. If the distance between their centers is less than the sum of the radii, but bigger than the absolute value of the difference, show that \( C_1, C_2 \) intersect.

(Hint: Construct the line perpendicular to the line between the radii, from an appropriate point.)

Summary: starting with a plane \( \Pi(F) \) coordinatized with an ordered field \( F \), we saw that \( \Pi(F) \) admits constructions with straightedge and compass if and only if \( F \) has square roots of positive elements.

Let \( F_{\text{Euclid}} \) be the field of all numbers obtained from \( \mathbb{Q} \) by adjoining square roots of positive elements. Then:

**Proposition 1.7.** \( F_{\text{Euclid}} \) is precisely the set of lengths of segments constructed by straightedge and compass, beginning with two fixed points at distance 1.

2. The Impossibility Proof for the Delian Problems

**A Geometry - Algebra Dictionary**

- Squaring of circle: Is \( \pi \in F_{\text{Euclid}} \)?
- Duplication of cube: Is \( 2^{1/3} \in F_{\text{Euclid}} \)?
- Trisection of any angle leads to:
  - regular 9-gon: Is \( 11^{1/9} \in F_{\text{Euclid}} \)?
- Notion: Dimension of \( L \) over \( K \).

**Definition 2.1.** \([L : K] = n \) if there is a basis \( c_1, \ldots, c_n \) of \( L \) over \( K \) = every element of \( L \) can be written uniquely as \( a_1c_1 + \ldots + a_nc_n \), \( a_i \in K \).

**Example 2.2.**

1. \([Q(\pi) : \mathbb{Q}] = \infty \). For any \( n \), there is no \( \mathbb{Q} \)-linear relation between \( 1, \pi, \ldots, \pi^n \); equivalently \( \pi \) is transcendental. Proof by Lindemann, 1883.
2. Assume \( \omega^n = 1, \omega \neq 1 \). Then \([Q[\omega] : \mathbb{Q}] < n \). Indeed we have the relation: \( 1 + \omega + \ldots + \omega^{n-1} = 0 \). If \( n \) is prime, then \([Q(\omega) : \mathbb{Q}] = n - 1 \).
3. \([Q(\sqrt[3]{2}) : \mathbb{Q}] = 3 \). (Exercise!)

**Lemma 2.3.** Let \( F \leq K \leq L \) be fields. If \( c_1, \ldots, c_n \) is a basis for \( L \) over \( K \), and \( b_1, \ldots, b_m \) is a basis for \( K \) over \( F \), then \( b_1c_1, \ldots, b_ic_j, \ldots, c_nb_m \) is a basis for \( L \) over \( F \). Thus

\[
[K : F][L : K] = [L : F]
\]

**Corollary 2.4.** If \( a \in F_{\text{Euclid}} \) (or \( a \in F_{\text{Euclid}}[\sqrt{-1}] \)) then \([Q(a) : \mathbb{Q}] = 2^m \) for some \( m \).
Proof. The number $a$ is the length of a segment that can be reached by some finite sequence of constructions by straightedge and compass. Thus there exist fields $\mathbb{Q} = F_1, \ldots, F_k$ such that $F_{i+1}$ can be obtained from $F_i$ by adjoining a square root of a positive element. So $[F_{i+1} : F_i] = 2$. Using the lemma, $[F_k : \mathbb{Q}] = 2^k$. By the lemma again, since $\mathbb{Q}(a)$ is a subfield of $F_k$, $[\mathbb{Q}(a) : \mathbb{Q}]$ divides $2^k$. So it has the form $2^m$. □

2.5. Division of angle and roots of unity.

Lemma 2.6. A regular $n$-gon can be constructed with straightedge and compass iff there exists a primitive $n$-th root of unity in $F_{\text{Euclid}}[\sqrt{-1}]$: $\omega^n = 1$, $\omega^m \neq 1$ for $1 \leq m < n$.

Using Corollary 2.4, we can say when a regular $n$-gon is constructible:

If $p^2 \mid n$, $p$ an odd prime, never.

If $n = 2^m$, always.

If $n$ is a product $2^m p_1 \cdots p_n$ with $p_i$ distinct primes, if and only if for each $i$, the regular $p_i$-gon is constructible.

For an odd prime $n$; if and only if $n - 1 = 2^k$. and then necessarily $k = 2^m$ for some $m$.

Exercise 2.7. If $2^k + 1$ is prime, then $k = 2^m$ for some $m$.

The Fermat primes are the primes of the form $n = 2^{2^m} + 1$; The first three are 3, 5, 17. The constructions of a regular 3-gon, 5-gon are in Euclid; the 17-gon was constructed by Gauss.