Lecture 13: Constructable numbers; Splitting Fields

Last time: Straightedge and compass

Start with two pts • •

(A) Given two points, can draw the line between them or the circle centered at one and passing through the other.

(B) Can find pts of intersection between lines + circles.

$C = \{a \in \mathbb{R} \mid$ Can construct $(a, 0)$ via the above$\}$

Thm: $a \in C$. Then $[\mathbb{Q}(a) : \mathbb{Q}] = 2^n$.

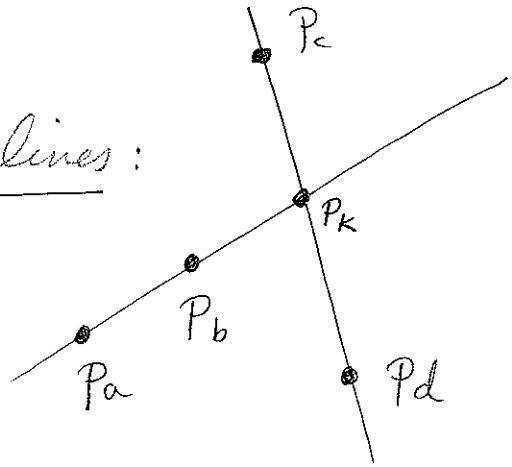
Cor: Can't trisect an angle (Pierre Wantzel 1837)

Cor: Can't square the circle (1882)

Proof of Thm: Let $P_0 = (0,0)$, $P_1 = (1,0)$, $P_2, P_3, \ldots, P_n = (a,0)$ be the points constructed to show $a \in C$. Let

$F_k = \mathbb{Q}(\text{coor of } P_0, \ldots, P_k)$.

Claim: $[F_K : F_{K-1}] = 1$ or 2 $(\Rightarrow$ Thm.)



Case P_K comes from intersecting two lines:

Then $F_K = F_{K-1}$ since

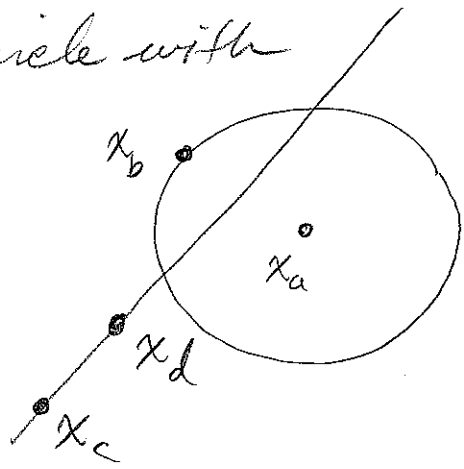
$P_K = (x_K, y_K)$ satisfies

$$(y_b - y_a)x_K - (x_b - x_a)y_K = x_a y_b - x_b y_a$$
$$(y_d - y_b)x_K - (x_d - x_b)y_K = x_c y_d - x_d y_c$$

Solving this linear sys shows that $x_K, y_K \in F_{K-1}$.

Case P_K comes from intersecting a circle with a line. Then

$$(x_K - a_1)^2 + (y_K - a_2)^2 = a_3^2$$



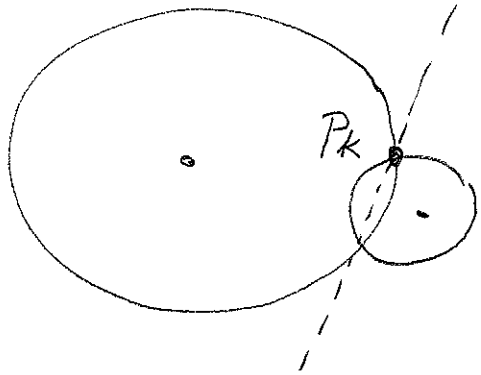
and

$$a_4 x_K + a_5 y_K = a_6$$

with $a_i \in F_{K-1}$. Solve for one of x_K, y_K in terms of the other. $y_K = \frac{a_6}{a_5} - \frac{a_4}{a_5} x_K$.

Get quadratic eqn for x_k. So

$$[F_k = F_{k-1}(x_k) : F_{k-1}] = 1 \text{ or } 2.$$



Case intersecting two circles:

Note x_k, y_k sat

$$g_1(x_k, y_k) = 0 \text{ and } g_2(x_k, y_k) = 0$$

$$\Leftrightarrow g_1(x_k, y_k) = 0 \text{ and } (g_2 - g_1)(x_k, y_k) = 0$$

If $g_i = (x_k - a_i)^2 + (y_k - b_i)^2 - c_i$

then $g_2 - g_1$ is <u>linear</u> $= d x_k + e y_k + f$.

So back to last case.

Q: What line is this?

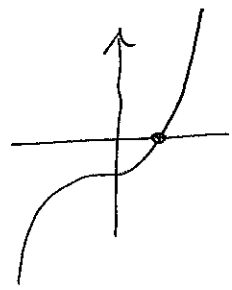
Splitting Fields: K/F is a splitting field for $f(x) \in F[x]$ if

(a) $f(x)$ factors into linear terms in $K[x]$ ("splits completely.")

(b) $f(x)$ does not split completely in any $F \subseteq L \subsetneq K$.

Ex: $\mathbb{Q}(\sqrt{2})$ is a splitting field for $x^2 - 2$ in $\mathbb{Q}(x)$, as $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$

Q: What is the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$ (inside $\mathbb{C}$)?



Note: $\mathbb{Q}(\sqrt[3]{2})$ isn't big enough:

$$f(x) = x^3 - 2 = (x - \sqrt[3]{2})\underbrace{(x^2 + \sqrt[3]{2}\,x + (\sqrt[3]{2})^2)}_{\text{irreducible}}$$

Let $\rho = e^{2\pi i/3}$, so $\rho^3 = 1$. Then $f(\rho\sqrt[3]{2}) =$

$f(\rho^2\sqrt[3]{2}) = 0.$

Ex: Over $K = \mathbb{Q}(\sqrt[3]{2}, \rho)$, have

$$X^3 - 2 = (X - \sqrt[3]{2})(X - \rho\sqrt[3]{2})(X - \rho^2\sqrt[3]{2})$$

Then K is a *splitting field* for f.

(Since $\mathbb{Q}[x]$ is a U.F.D., any subfield where f splits must contain $\sqrt[3]{2}$ and ρ.)

Thm: Let $f(x) \in F[x]$. Then $\exists$ an extension K/F which is a *splitting field* of F.

Proof: Successively add in roots till f splits completely.

Formal proof: induct on $\deg(f)$

Note: $[K_{\text{splitting}} : F] \leq n!$

In fact: Pick $f(x) \in \mathbb{Z}[x]$ "at random".

With prob $\to 1$, $[\text{Splitting field of } F : F] = n!$ or $\frac{n!}{2}$.