Lecture 18: Euclidean Geometry & Splitting Fields...

The primary focus of this lecture is splitting fields and algebraic closures (§13.4 of D&F). However we take about 5 minutes to survey the achievements of §13.3 which show what field theory has to say about classical problems of Euclidean Geometry.

- I: DOUBLING THE CUBE
- II: TRISECTING AN ANGLE
- III: SQUARING THE CIRCLE

  using compass & straightedge, can we construct a square whose area is precisely the area of a given circle?

Proposition (23) If $\alpha \in \mathbb{R}$ is obtained from $F \subseteq \mathbb{R}$ by series of compass & straightedge constructions then $[F(\alpha) : F] = 2^k$ for some non-neg. int. k.

Thm (24) I., II., III. are all impossible.

Proof: each construction in I., II. and III. implies an extension field of odd order $\neq 2^k$ hence contradicting Prop. 23.

I.) doubling cube $\approx$ construct $\sqrt[3]{2}$ in $\mathbb{R}$ starting with 1 $\Rightarrow [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 2^k$

II. & III. are longer stories, see p. 534-535. //

Def^n/ The extension field K of F is called a <u>splitting field</u> for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors (a.k.a. splits completely) in $K[x]$ <u>and</u> $f(x)$ does not split completely in any proper subfield of K containing F

E1 the splitting field for $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ is $\mathbb{Q}(\sqrt{2})$ since $f(x) = (x+\sqrt{2})(x-\sqrt{2})$ in $\mathbb{Q}(\sqrt{2})[x]$.

E2 the splitting field for $f(x) = (x^2-2)(x^2-3)$ is given by $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ since in $\mathbb{Q}(\sqrt{2}, \sqrt{3})[x]$ we see

$$f(x) = (x+\sqrt{2})(x-\sqrt{2})(x+\sqrt{3})(x-\sqrt{3})$$

E3 the splitting field of $x^3 - 2$ over $\mathbb{Q}$ is not $\mathbb{Q}(\sqrt[3]{2})$ since this is a <u>real</u> subfield of $\mathbb{C}$ whereas the roots of $f(x) = x^3 - 2$ are:

$$\sqrt[3]{2}, \quad \underbrace{\sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right), \sqrt[3]{2}\left(\frac{-1-i\sqrt{3}}{2}\right)}$$

Conjugate pair, not surprising

Let's call these $\alpha, \alpha\omega, \alpha\omega^2$ since $\omega = \exp\left(\frac{2\pi i}{3}\right)$ makes that true. Of course $\mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2)$ completely splits $x^3 - 2$. There is an easier description,

$$\frac{\omega\alpha}{\omega\alpha} = \omega = \frac{-1}{2} + \frac{i\sqrt{3}}{2} \Rightarrow i\sqrt{3} = 2\omega + 1$$

$$\text{or } \sqrt{-3} = 2\omega + 1$$

Key Point: adjoining $\sqrt{-3}$ to $\mathbb{Q}$ gets us an ω.

E3 continued

The field $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ contains all three roots for $f(x) = x^3 - 2$ since $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$ can be generated by $\mathbb{Q}$, $\sqrt[3]{2}$ and $\sqrt{-3} = i\sqrt{3}$.

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \qquad (m_{\sqrt[3]{2}}(x) = x^3 - 2 \text{ irred. over } \mathbb{Q})$$

$$[\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] = 2 \qquad (m_{\sqrt{-3}}(x) = x^2 + 3 \text{ irred. over } \mathbb{Q})$$

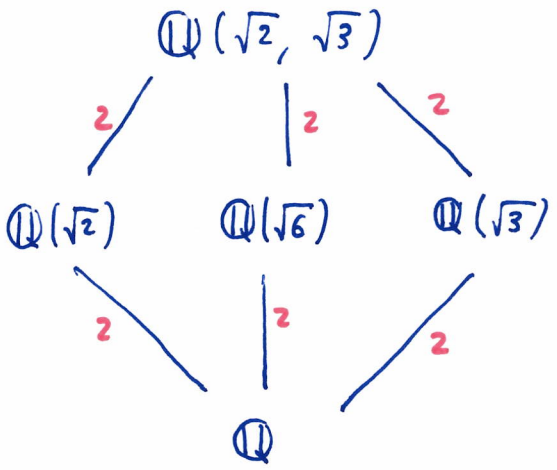
Therefore, as $\gcd(2, 3) = 1$,

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}] = 2(3) = 6.$$

- Can argue this by noting that as $\sqrt{-3}$ solves $x^2 + 3 = 0$ the $[\mathbb{Q}(\sqrt[3]{2})(\sqrt{-3}) ; \mathbb{Q}(\sqrt[3]{2})] \leq 2$ and it must be 2 since we can see $\mathbb{Q}(\sqrt[3]{2})$ is not splitting field for $x^3 - 2$ over $\mathbb{Q}$.
- or, letting K be splitting field, $\mathbb{Q}(\sqrt{-3}) \subseteq K$ thus $[\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] = 2$ divides $[K : \mathbb{Q}]$. But $\mathbb{Q}(\sqrt[3]{2}) \subseteq K$ and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ divides $[K : \mathbb{Q}]$. Hence 6 divides $[K : \mathbb{Q}]$, but we know $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ is degree 6 over $\mathbb{Q}$ $\therefore$ $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$

Remark: the problem to grasp is whether $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ is minimal.

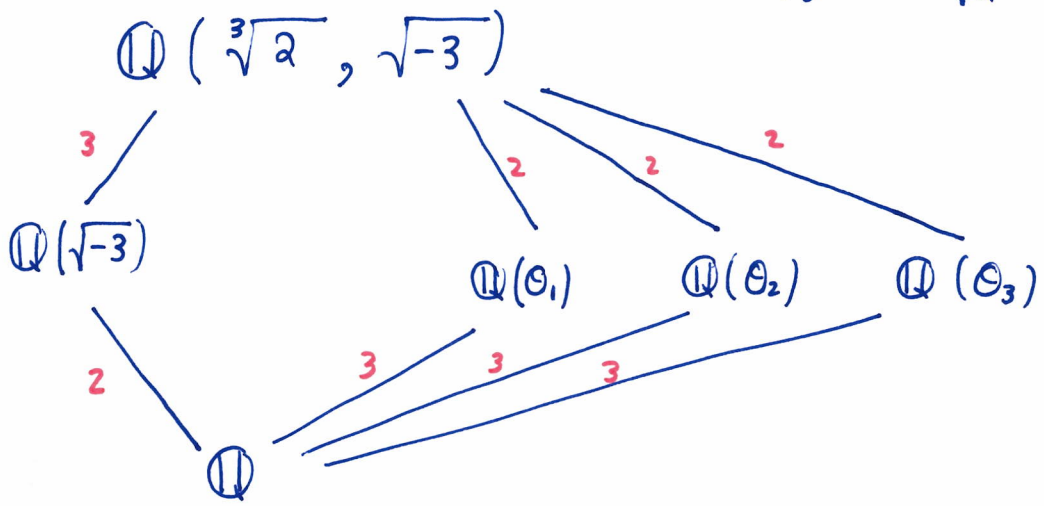
E2 and E3 visualized



$\theta_1 = \sqrt[3]{2}$

$\theta_2 = \omega\sqrt[3]{2} = \sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right)$

$\theta_3 = \omega^2\sqrt[3]{2} = \sqrt[3]{2}\left(\frac{-1-i\sqrt{3}}{2}\right)$



E4 Consider x^4+4 over $\mathbb{Q}$ we have

$$x^4+4 = (x^2+2)^2 - 4x^2$$
$$= (x^2+2x+2)(x^2-2x+2)$$
$$= (x+1+i)(x+1-i)(x-1+i)(x-1-i)$$

We find roots $1+i$, $1-i$, $-1+i$, $-1-i$ then the splitting field is just $\mathbb{Q}(i)$.

I omit proof for Th^{m}s to follow, we may add them later if needed, but I want to be sure to get the big ideas in front of us here (§13.4 has proofs)

Th^m (25) For any field F, if $f(x) \in F[x]$ then $\exists$ an extension K of F which is a splitting field for $f(x)$

Def^n If K is an algebraic extension of F which is the splitting field of F for a collection of polynomials $f(x) \in F[x]$ then K is called a normal extension of F

Proposition (26)
A splitting field of a polynomial of degree n over F is of degree at most $n!$ over F

We show later that a "generic polynomial" of degree n has a splitting field of degree $n!$

E5 The splitting field of $X^n - 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\zeta_n)$ where ζ_n is an n^{th} root of unity given by $\exp\left(\frac{2\pi i}{n}\right) = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$

E6 The splitting field of $X^p - 2$ where p is prime contains ζ_p and $\sqrt[p]{2}$ and it turns out is just $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ of degree $p(p-1)$ over $\mathbb{Q}$.

Thm (27)

Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields.
Let $f(x) \in F[x]$ and $f'(x) \in F'[x]$ be obtained by applying φ to the coefficients of $f(x)$.

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \Rightarrow f'(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n.$$

Let E be a splitting field for $f(x)$ over F and E' a splitting field for $f'(x)$ over F'. Then the isomorphism φ extends to $\sigma : E \xrightarrow{\sim} E'$

$$\begin{array}{ccc} \sigma : & E & \xrightarrow{\sim} & E' \\ & | & & | \\ \varphi : & F & \xrightarrow{\sim} & F' \end{array}$$

Corollary (28)

Any two splitting fields for a polynomial $f(x) \in F[x]$ over a field F are ISOMORPHIC

Def^n The field $\bar{F}$ is called an <u>algebraic closure</u> of F if $\bar{F}$ is algebraic over F and if every polynomial $f(x) \in F[x]$ splits completely over $\bar{F}$ (hence $\bar{F}$ contains all elements algebraic over F)

Def^n A field K is said to be <u>algebraically closed</u> if every polynomial with coefficients in K has a root in K

PROPOSITION 29

Let $\bar{F}$ be an algebraic closure of F. Then $\bar{F}$ is algebraically closed.

PROPOSITION 30

For any field F there exists an algebraically closed field K containing F.

(proof of this is quite neat)

PROPOSITION 31

Let K be an algebraically closed field and let F be a subfield of K. Then the collection of elements $\bar{F}$ of K that are algebraic over F is an algebraic closure of F. An algebraic closure of F is unique up to isomorphism.

Th^{m} (Fundamental Theorem of Algebra)

The field $\mathbb{C}$ is algebraically closed

Corollary (32)

The field $\mathbb{C}$ contains an algebraic closure for any of its subfields. In particular, $\bar{\mathbb{Q}} \subseteq \mathbb{C}$ is an algebraic closure of $\mathbb{Q}$.

Remark: ok, but, what about $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(?)$.
How does that work out ???