Groups & Rings: Lecture #23

Splitting fields & geometric constructions (§21.2–3)

- Existence of splitting fields
- Uniqueness of splitting fields
- Straightedge and compass constructions

Existence of splitting fields

Def: Let $p(x) \in F[x]$ not constant. A splitting field of $p(x)$ is a field extension K/F such that

"big enough" (i) $p(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ in $K[x]$ $(c, \alpha_i \in K)$

"not too big" (ii) $K = F(\alpha_1, \ldots, \alpha_n)$

Rmk: If $F \subset E$ with E algebraically closed (e.g. $\mathbb{Q} \subset \overline{\mathbb{Q}}$ or $\mathbb{Q} \subset \mathbb{C}$)
then $p(x)$ splits in E: $p(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ $(c, \alpha_i \in E)$
so $K = F(\alpha_1, \ldots, \alpha_n)$ is a splitting field of $p(x)$.

Ex (21.30) $p(x) = x^3 - 3$ over $\mathbb{Q}$. Then one root is $\alpha = \sqrt[3]{3}$.
(irreducible by Eisenstein: $p=3$)

Two more roots: $\zeta\alpha, \zeta^2\alpha$ where $\zeta^3 = 1, \zeta \neq 1$, $\zeta = e^{\frac{2\pi}{3}i} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

Splitting field: $K = \mathbb{Q}(\alpha, \zeta\alpha, \zeta^2\alpha) = \mathbb{Q}(\alpha, \zeta)$

Minimal polynomials:

α: $x^3 - 3$ (deg 3)

exercise

ζ: $\frac{x^3-1}{x-1} = x^2 + x + 1$ (cyclotomic polynomial, also irr over $\mathbb{Q}(\alpha)$)

$$\underbrace{\mathbb{Q} \subset \mathbb{Q}(\alpha)}_{\substack{\text{deg } 3 \\ \text{basis } 1, \alpha, \alpha^2}} \underbrace{\subset \mathbb{Q}(\alpha, \zeta)}_{\substack{\text{deg } 2 \\ \text{basis } 1, \zeta}} \Rightarrow \text{deg } 6, \text{ basis: } 1, \alpha, \alpha^2, \zeta, \zeta\alpha, \zeta\alpha^2$$

Exc 21.3c) Find splitting field of $p(x) = x^3 + 2x + 2$ over $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$

Irreducible? $\deg p = 3$, irr $\Leftrightarrow$ no roots.

$p(0) = 2, \quad p(1) = 1+2+2 = 2, \quad p(2) = 8+4+2 = 2$

No roots $\Rightarrow$ irreducible.

To get one root: $E = \mathbb{F}_3[x]/(p(x))$, $\quad \alpha = \bar{x} = x + (p(x))$

$\underbrace{\mathbb{F}_3 \subset \mathbb{F}_3(\alpha)}_{\deg 3,\ \text{basis } 1, \alpha, \alpha^2} = E$

Over E: $\quad p(x) = (x-\alpha)\underbrace{(x^2 + ax + b)}_{\text{splits?}}$

First determine a & b.

$$x^3 + 2x + 2 = (x-\alpha)(x^2 + ax + b)$$
$$= x^3 + \underbrace{(-\alpha + a)}_{=0} x^2 + \underbrace{(b - a\alpha)}_{=2} x \underbrace{- \alpha b}_{=-2=1}$$

$$\Rightarrow \boxed{\begin{aligned} a &= \alpha \\ b &= 2 + a\alpha = 2 + \alpha^2 \end{aligned}}$$

$$p(x) = (x-\alpha)\underbrace{(x^2 + \alpha x + 2 + \alpha^2)}$$

$$x^2 + \alpha x + 2 + \alpha^2 = \left(x + \frac{\alpha}{2}\right)^2 + 2 + \cancel{\alpha^2} - \cancel{\left(\frac{\alpha}{2}\right)^2} \qquad \left(\frac{1}{2} = \frac{1}{-1} = -1\right) \text{ in } \mathbb{F}_3$$
$$= (x-\alpha)^2 - 1$$

$\boxed{\text{roots: } x = \alpha \pm 1}$ $\qquad p(x) = (x-\alpha)(x-\alpha-1)(x-\alpha+1)$

so E is a splitting field $[E : \mathbb{F}_3] = 3$.

<u>Thm 21.31</u>: $p(x) \in F[x]$ non-constant. There $\exists$ a splitting field of $p(x)$.

<u>pf</u>: Idea: induction on $\deg p(x)$ for all fields simultaneously.

<u>Base case</u>: $\deg p = 1$: F is a splitting field.

<u>Induction step</u>: Assume theorem holds for all fields and all polynomials of degree $\leq \deg p - 1$.

<u>case 1</u>: If p reducible: $p(x) = p_1(x) p_2(x)$, apply (induction) theorem to $p_1(x)$ and get $F \subset E$ s.th.

- $p_1(x) = (x - \alpha_1) \cdots (x - \alpha_m)$ in $E[x]$.
- $E = F(\alpha_1, \dots, \alpha_m)$

Apply theorem to $p_2(x) \in E[x]$ and get $\underbrace{F \subset E}_{\deg \leq m!} \underbrace{\subset K}_{\deg \leq (n-m)!}$ where also $p_2(x)$ splits. Done.

<u>case 2</u>: If p irreducible: take $E = F[x]/(p(x))$, $\alpha = \bar{x} \in E$

$$p(x) = (x - \alpha)\, q(x), \quad q(x) \in E[x]$$

Apply theorem to $q(x) \in E[x]$ and $\dots$ as before. $\square$

$$\underbrace{F \subset E}_{\deg n} \underbrace{\subset K}_{\leq (n-1)!}$$

<u>Exc 21.11</u>: There exists a splitting field of degree $\leq n!$ where $n = \deg p$. Follows from proof and observation: $(m!)(n-m)! \leq n!$

Uniqueness of splitting fields

Let $p(x) \in F[x]$ be non-constant and let $F \subset E_1$ and $F \subset E_2$ be two splitting fields of $p(x)$. We will see that $\exists\, \phi: E_1 \xrightarrow{\cong} E_2$ isomorphism such that $\phi|_F = id_F$, that is, $\phi(a) = a \ \forall a \in F$.
(ϕ is not unique)

Lem 21.32: Given F_1 and F_2 and isomorphism $\phi: F_1 \xrightarrow{\cong} F_2$, and given two extensions $F_1 \subset F_1(\alpha_1) = E_1$ and $F_2 \subset F_2(\alpha_2) = E_2$ with minimal polynomials $p_1 \in F_1[x]$ and $p_2 \in F_2[x]$ of α_1 and α_2.
If α_2 is a root of $\phi(p_1)$, then there exists a unique isomorphism $\bar{\phi}: E_1 \longrightarrow E_2$ such that:

(i) $\bar{\phi}|_{F_1} = \phi$

(ii) $\bar{\phi}(\alpha_1) = \alpha_2$

Rmk: $\phi: F_1 \xrightarrow{\cong} F_2 \quad \rightsquigarrow \quad \phi: F_1[x] \xrightarrow{\cong} F_2[x]$

$\phi(p_1) \in F_2[x]$ irreducible & monic. $\qquad \sum a_i x^i \longmapsto \sum \phi(a_i) x^i$

If α_2 root of $\phi(p_1)$, then $p_2 = \phi(p_1)$. $\qquad \sum \phi^{-1}(b_i) x^i \longleftarrow \sum b_i x^i$

proof: (of Lemma) $\quad E_1$ has basis $1, \alpha_1, \alpha_1^2, \dots, \alpha_1^{n-1} \qquad n = \deg p_1$

E_2 has basis $1, \alpha_2, \alpha_2^2, \dots, \alpha_2^{n-1} \qquad n = \deg p_2$

$\bar{\phi}$ has to take α_1 to $\alpha_2 \rightsquigarrow \bar{\phi}(\alpha_1^k) = \bar{\phi}(\alpha_1)^k = \alpha_2^k$.

$\rightsquigarrow \bar{\phi}\left(\sum_{k=0}^{n-1} a_i \alpha_1^k\right) = \sum_{k=0}^{n-1} \phi(a_i) \alpha_2^k$

$\bar{\phi}$ isomorphism of vector spaces. Ring homomorphism?

Note that: $E_1 \cong F_1[x]/(p_1(x)) \qquad E_2 \cong F_2[x]/(p_2(x))$

$$\begin{tikzcd} p_1(x) \in F_1[x] \arrow[r, "q_1"] \arrow[d, "\phi"', "\cong"] & E_1 \arrow[d, dashed, "\overline{\phi}"] \\ p_2(x) \in F_2[x] \arrow[r, "q_2"] & E_2 \end{tikzcd}$$

because $E_1 = F_1(x)/(p_1(x))$

$\exists$ unique ring homom. $\overline{\phi}$ as above $\iff q_2(\phi(p_1(x))) = 0$

But $\ker(q_2) = (p_2(x)) = \phi(p_1(x))$. $\square$

<u>Thm 21.33</u>: Let $F_1 \xrightarrow{\phi} F_2$ be an isomorphism of fields. Let $p_1 \in F_1[x]$ non-constant pol, $p_2 = \phi(p_1)$. If E_1/F_1 and E_2/F_2 are splitting fields, then there $\exists$ isomorphism $\overline{\phi}: E_1 \to E_2$ such that $\overline{\phi}|_{F_1} = \phi$. (WARNING: $\overline{\phi}$ not unique)

<u>sketch of pf</u>: Induction on deg p_1. Pick one root $\alpha_1 \in E_1$ of p_1.
<u>Let α_2 be a root</u> of corr. irr. factor of p_2. (involves a choice)

$$\begin{tikzcd} F_1 \arrow[d, "\phi"'] & \subset & F_1(\alpha_1) \arrow[d, dashed, "\exists \text{ by Lemma}"] & \subset & E_1 \\ F_2 & \subset & F_2(\alpha_2) & \subset & E_2 \end{tikzcd}$$

by induction get $E_1 \xrightarrow{\overline{\phi}} E_2$. $\square$

<u>Ex</u>: $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2})$ $\qquad F_1 = F_2 = F$, $\phi = id_F$, $E_1 = E_2 = E$.

(a) $\overline{\phi}: \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$ $\rightsquigarrow \overline{\phi} = id_E$
$\sqrt{2} \longmapsto \sqrt{2}$

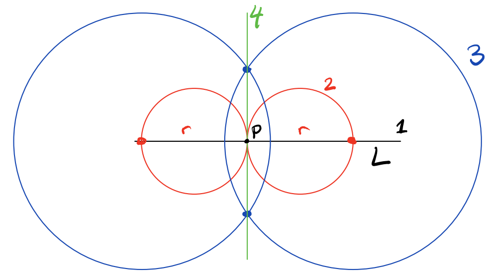
(b) $\overline{\phi}: \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$ $\qquad \overline{\phi} =$ "conjugation"
$\sqrt{2} \longmapsto -\sqrt{2}$ $\qquad$ (we saw this for quad. numbers)

Geometric Constructions

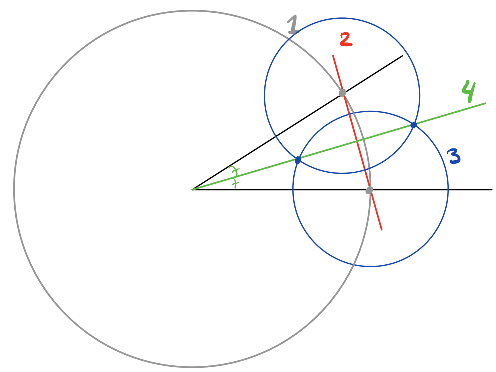
Possible constructions with straightedge (ruler w/o markings) and compass?

Basic constructions:

(1) perpendicular line to L through P
(steps 1–4)



(2) bisect an angle
(steps 1–4)



Classical problems from ancient Greeks

(1) Can you **trisect an angle**? (for an arbitrary angle)

(2) Can you **double a cube**? (can you construct $\sqrt[3]{2}$?)

(3) Can you **square a circle**? (can you construct $\sqrt{\pi}$?)

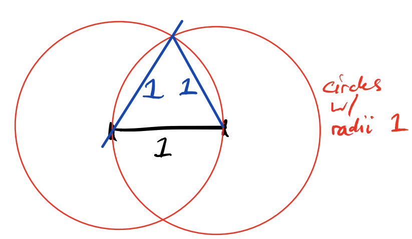
Answers are **NO**. (Wantzel 1837, Lindemann 1882)

A similar problem from ancient Greeks

For which d can you construct a regular polygon with d vertices?

Easy: $d = 3, 4, 6, 8$

$d=3$



Greeks also knew: $d = 5$

Bisecting angle gives: d possible $\Rightarrow$ $2d$ possible

First open cases: 7, 9, 11, ...

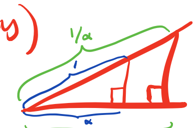
Thm (Gauss 1796, Wantzel 1837): A regular d-gon is constructible exactly when $d = 2^h p_1 p_2 \cdots p_m$, where $h \in \mathbb{N}$ and p_i are Fermat primes, that is, primes of the form $p = 2^{2^n}+1$ (the only known Fermat primes are $p = 3, 5, 17, 257, 65537$)
$n = 0, 1, 2, 3, 4$

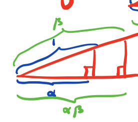
For example: heptagon impossible but 17-gon possible.

Def: $\alpha \in \mathbb{R}$ is **constructible** if starting from a unit interval it is possible to construct an interval of length α.

Thm 21.35: The constructible numbers form a subfield of $\mathbb{R}$.

sketch of pf: α, β cons $\Rightarrow$ $\alpha+\beta$, $\alpha-\beta$ cons. (easy)

$\alpha \neq 0$ cons $\Rightarrow$ $1/\alpha$ cons (sim. triangles )

α, β cons $\Rightarrow$ $\alpha\beta$ cons (sim tri. ) $\square$

Thm 21.41: Constructible numbers are given by repeatedly extracting square roots. That is, given a constructible number $\alpha \in \mathbb{R}$, there exists:

$$\underbrace{\mathbb{Q} \subset \mathbb{Q}(\sqrt{a_1})}_{\deg 2} \subset \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}) \subset \cdots \subset \underset{\substack{\cup\!\!\!\!\mid \\ \alpha}}{\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_m})}$$

(second $\deg 2$ under $\mathbb{Q}(\sqrt{a_1}) \subset \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2})$)

In particular, if α is constructible, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] \mid 2^m$ so the minimal polynomial of α has degree 2^h for some $h \in \mathbb{N}$.
Also, constructible numbers are algebraic ($\mathbb{Q} \subset \{\text{constr. numbers}\} \subset \overline{\mathbb{Q}}$).

Impossible constructions:

- **Doubling cube**: $\alpha = \sqrt[3]{2}$ not constructible b/c min. pol. $x^3 - 2$ (deg 3)
- **Trisecting angle**: α root of $x^3 - \frac{3}{4}x - \frac{1}{8} = 0$, not constructible b/c deg 3.
- **Squaring circle**: $\alpha = \pi$ (or $\sqrt{\pi}$) not constructible b/c not algebraic (Lindemann)