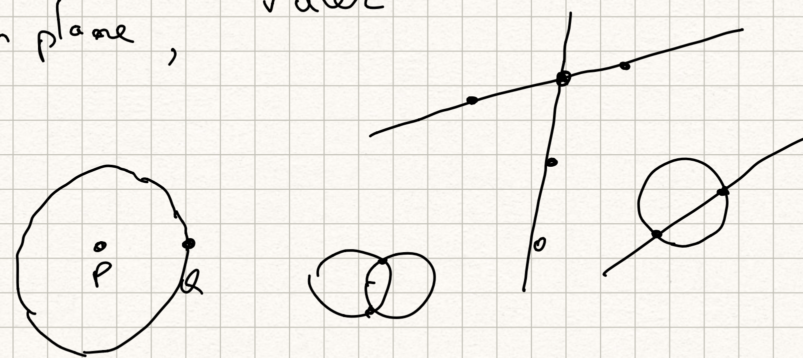
lect 18 Ruler-Compass constructions.

Refs: Rotman Appendix C.

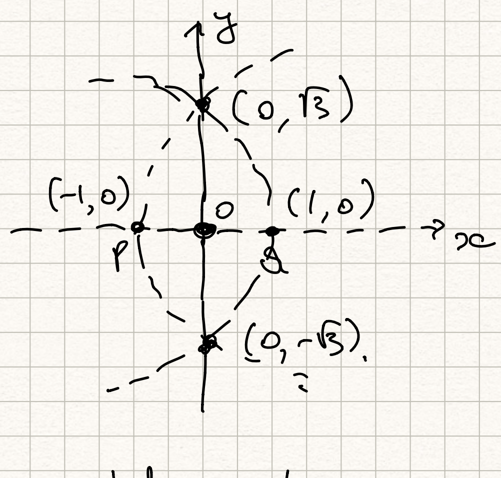
[Morandi, Fields & Galois theory, Sect III.15
pdf available via Columbia online library

point on plane, ruler

Compass



which points can we build iterating this construction?



what other points can we build

$p=(a,b)$ $\quad a,b\in\mathbb{R}$

$z=a+bi\in\mathbb{C}$.

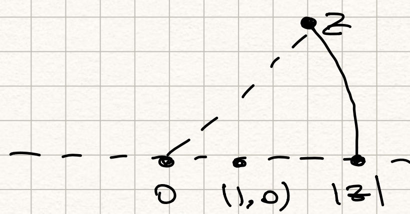
what point on x-axis can we get this way?

Call $z\in\mathbb{C}$ constructible if can build it from $(1,0),(-1,0)$.

Call $a \in \mathbb{R}$ constructible

$\mathbb{R}$-constructible

if $(a,0)$ is constructible



if z

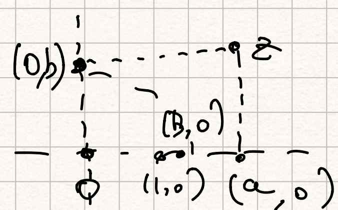
$\mathbb{R}$, $\mathbb{C}$.

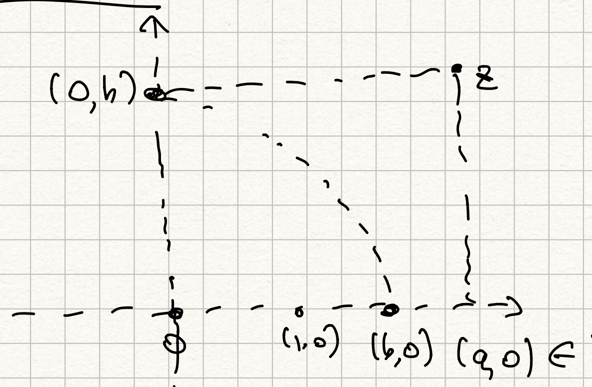
K - set of constructible complex numbers

$K_{\mathbb{R}}$ - set of constructible real numbers

1) If $z \in K \Rightarrow |z| \in K_{\mathbb{R}}$, $|z|$ is $\mathbb{R}$-constructible

2) $z = a + bi \in K \Longleftrightarrow a, b \in K_{\mathbb{R}}$





$a \in K_{\mathbb{R}}$

3) $z \in K \Longleftrightarrow -z \in K$

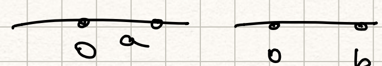
$a \in K_{\mathbb{R}} \Longleftrightarrow -a \in K$

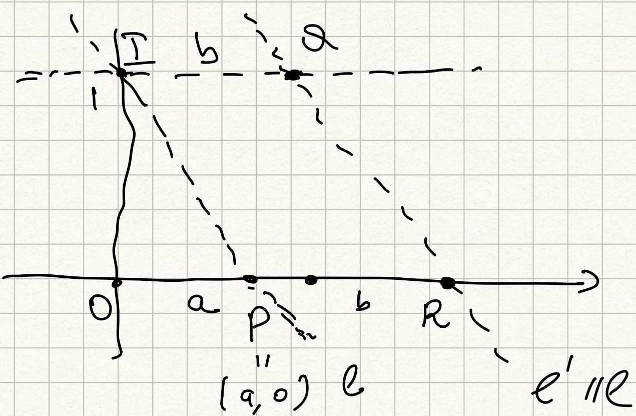
Claim $K \subset \mathbb{C}$ is a subfield

$K_{\mathbb{R}} \subset \mathbb{R}$ is a subfield

Thm $K_{\mathbb{R}}$ is a subfield of $\mathbb{R}$.

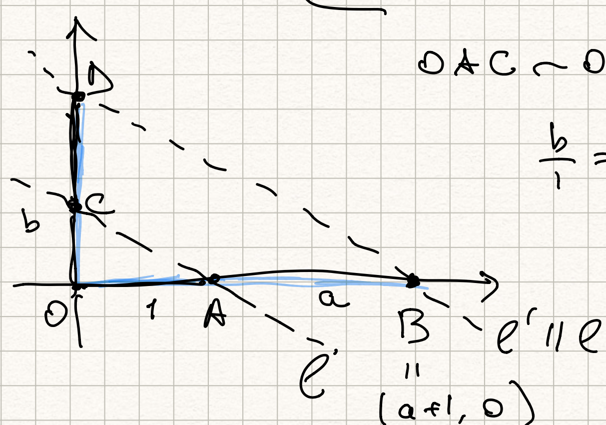
Proof 1) $a, b \in K_{\mathbb{R}} \overset{?}{\Rightarrow} a+b \in K_{\mathbb{R}}$.





$|OR| = a+b$.

2) $\Rightarrow ab \in K_{\mathbb{R}}$



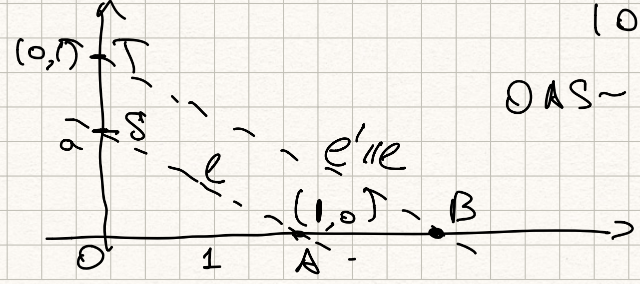
$OAC \sim OBD$

$\frac{b}{1} = \frac{|OD|}{1+a}$

$|OD| = b(1+a) =$
$b + ba$.

$|CD| = ba$

3) $a \neq 0 \Rightarrow a^{-1}$ is constructible



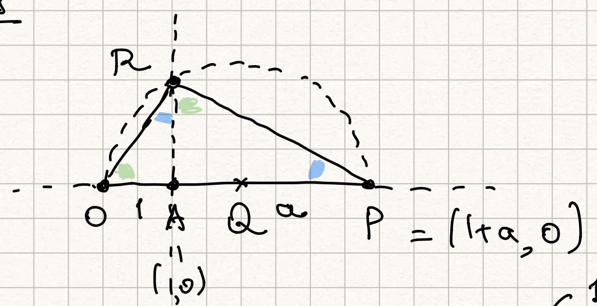
$|OB|$

$OAS \sim OBT$ $\quad \frac{|OB|}{|OA|} = \frac{|OT|}{|OS|}$

$$\frac{|OB|}{1} = \frac{1}{a} \qquad |OB| = \underline{\underline{a^{-1}}} \qquad \square$$

<u>Thm</u> for any $a \in K_{\mathbb{R}}$, $a > 0$ $\sqrt{a} \in K_{\mathbb{R}}$.

<u>Proof</u>



$Q = \left(\frac{1+a}{2}, 0\right)$

$\triangle OR \sim \triangle RP \qquad \frac{|OA|}{|AR|} = \frac{|AR|}{|AP|}$ with $|OA| = 1$, $|AP| = a$

$|AR|^2 = a \qquad |AR| = \sqrt{a}$. $\Rightarrow \sqrt{a}$ is constructible.

<u>Thm</u> $K_{\mathbb{R}}$ is a subfield of $\mathbb{R}$; for each $a \in K_{\mathbb{R}}$, <u>$a > 0$ $\sqrt{a} \in K_{\mathbb{R}}$.</u>

$\mathbb{Q} \subset K_{\mathbb{R}}, \quad \mathbb{Q}(\sqrt{\tfrac{3}{2}}) \subset K_{\mathbb{R}} \quad \sqrt{3 + \frac{\sqrt{2}}{5}} \in K_{\mathbb{R}}$

Can iterate square roots in $K_{\mathbb{R}}$

$\sqrt{\underbrace{3 - \sqrt{2}}_{>0}} \in K_{\mathbb{R}} \qquad \sqrt{\underbrace{3 - \sqrt{10}}_{<0}}$.

<u>Want to show</u> $K_{\mathbb{R}}$ is the smallest subfield of $\mathbb{R}$ with this property.

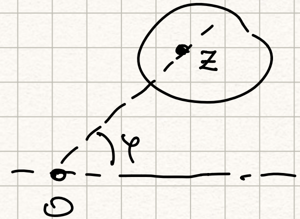
$[K_{\mathbb{R}} : \mathbb{Q}] = \infty$ $\qquad \underbrace{K \subset \mathbb{C}}_{\text{field}}$ $\qquad K_{\mathbb{R}} \subset \mathbb{R}$

Thm K is a subfield of $\mathbb{C}$.

$$K_{\mathbb{C}} = K \subset \mathbb{C}$$
$$\cup \qquad \cup$$
$$K_{\mathbb{R}} \subset \mathbb{R}$$

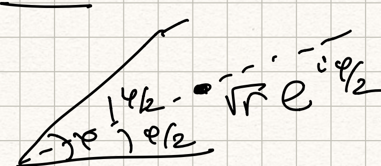
$z_1, z_2 \qquad a_1, b_1, a_2, b_2 \in K_{\mathbb{R}}$

$$z_1 z_2 = (a_1 + b_1 i)(a_2 + b_2 i) =$$
$$= \underbrace{(a_1 a_2 - b_1 b_2)}_{\in K_{\mathbb{R}}} + \underbrace{(a_1 b_2 + a_2 b_1)}_{\in K_{\mathbb{R}}} i \in K = K_{\mathbb{C}}$$



$\overset{\in K_{\mathbb{C}}}{z} = r e^{i\varphi} \Rightarrow r \in K_{\mathbb{R}}, \ \sqrt{r} \in K_{\mathbb{R}}$

$e^{i\varphi}$ – complex constructible



$z \in K_{\mathbb{C}} \Rightarrow \sqrt{z} \in K_{\mathbb{C}}$

$\pm\sqrt{z}$

Thm 1) if $a, b, c \in K_{\mathbb{C}}$, then roots of $f(x) = ax^2 + bx + c$ are in $K_{\mathbb{C}}$.

2) if $a, b, c \in K_{\mathbb{R}}$, $f(x)$ has real roots, they are in $K_{\mathbb{R}}$

Proof Use the discriminant f-la

$$x_{1,2} = \frac{-b \pm \sqrt{\mathcal{D}}}{2a} \in K_{\mathbb{R}} \qquad \underline{\mathcal{D}} = b^2 - 4ac \geq 0 \qquad K_{\mathbb{R}}$$

over $\mathbb{C}$, don't need $\mathcal{D} \geq 0$.

$\forall \mathcal{D}$ works $\quad \sqrt{\mathcal{D}} \in K_{\mathbb{C}}$.
$\cap$
$\mathbb{C}$

This shows that $K_{\mathbb{R}}, K_{\mathbb{C}}$ are "large"

if $F \subset K_{\mathbb{R}}$, α^2 $\alpha \in \mathbb{R}, \alpha^2 \in F \Rightarrow \alpha \in K_{\mathbb{R}}$.

$F \subset F(\alpha)$ then $F(\alpha)$ is also in $K_{\mathbb{C}}$

$\uparrow 2$ (or in $K_{\mathbb{R}}$ if $\alpha > 0$).

in $K_{\mathbb{R}}$ or $K_{\mathbb{C}}$

In char 0, any quadratic extension E/F.
has the form $E = F(\alpha)$, $\alpha^2 \in F$.
$x^2 - \beta$ $\qquad \alpha^2 = \beta$

<u>Claim</u> Cannot get anything else.

<u>Thm</u> 1) $\underline{\alpha \in K_{\mathbb{R}}}$ iff $\exists$ a chain of degree 2 extensions

$[F_{i+1} : F_i] = 2$

$$\mathbb{Q} \underset{2}{\subset} F_1 \underset{2}{\subset} F_2 \dots \underset{2}{\subset} F_n \subset \mathbb{R}$$

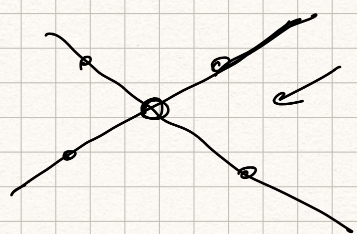
$[F_n : \mathbb{Q}] = 2^n \quad \mathcal{D}_i > 0$

$\alpha \in F_n$. $\qquad F_{i+1} = F_i(\sqrt{\mathcal{D}_i})$.

2) Same for $\mathbb{C}$: $\alpha \in K_{\mathbb{C}}$ iff $\exists$ a chain of deg 2 extensions

$$\mathbb{Q} \subset F_1 \subset F_2 \ldots \subset F_n \qquad [F_{i+1} : F_i] = 2$$
$$\quad\ \cap \quad \cap \qquad\quad \cap \qquad [F_n : \mathbb{Q}] = 2^n$$
$$\quad\ \mathbb{C} \quad \mathbb{C} \qquad\quad \mathbb{C}$$

$\alpha \in F_n$.



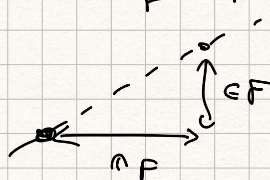
solve system of 2 equations with 2 unknowns.

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \qquad A\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

lin, lin

$a_{ij} \in F \qquad b_i \in F \qquad x_i \in F$

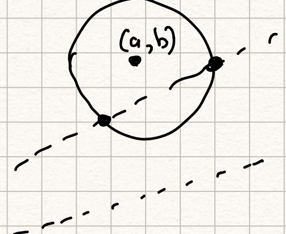
$$y = \underset{F}{a}x + \underset{F}{b}$$



$$\begin{cases} y = cx + d & \text{linear} \\ (x-a)^2 + (y-b)^2 = r^2 & \text{quadratic} \end{cases}$$

$a, b \in \mathbb{R}$- constructible $\Leftrightarrow \in K_{\mathbb{R}}$

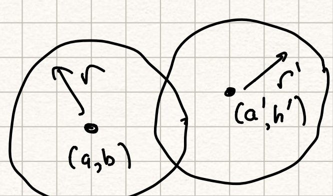
$r \in K_{\mathbb{R}}$



$$\begin{cases} (x-a)^2 + (cx+d-b)^2 = r^2 \\ (1+c^2)x^2 + ux + v = 0 \end{cases}$$

$x \in$ some quadratic extension of

$\sqrt{D} \qquad D > 0$



$$\begin{cases} (x-a)^2 + (y-b)^2 = r^2 \\ (x-a')^2 + (y-b')^2 = (r')^2 \end{cases}$$

(1) $x^2 + y^2 +$ lin terms $\ldots x + \ldots y + \ldots = 0$.

(2) $x^2 + y^2 + \ldots x + \ldots y + \ldots = 0$

$$\underline{tx + t'y + t'' = 0}$$ t, t', t'' — build from a, b, r, a', b', r'!

y as f'n of x

$$\underline{y = (t')^{-1}(-t'' - tx)}$$ lin f'n

$y = ux + v$

$$x^2 + (ux+v)^2 + \text{lin}(x) + \text{constant} = 0.$$

$$(1+u^2)x^2 + wx + w' = 0$$

add x by adding $\sqrt{D}$

D

$\mathbb{R}$-Constructible #'s are elements of

$$\mathbb{Q} \underset{2}{\subset} F_1 \underset{2}{\subset} F_2 \ldots \underset{2}{\subset} F_n$$

$F_{i+1} = F_i(\sqrt{D_i})$

$D_i \in F_i$

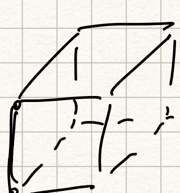
$D_i > 0$

$\sqrt[3]{2}$ is not constructible

$\underline{E = \mathbb{Q}(\sqrt[3]{2})}$ $[E : \mathbb{Q}] = 3$ $E \not\subset F_n$ not a subfield

$$\underbrace{\mathbb{Q} \underset{3}{\subset} E \underset{a}{\subset} F_n}_{2^n}$$

$2^n = 3a$ contradiction

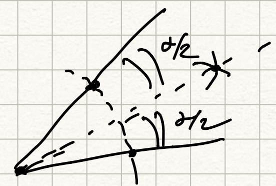
$\sqrt[3]{2}$  c vol$(c) = 2$

Can we construct $\sqrt[3]{2}$ via ruler+compass

start $\overset{0}{\bullet}\!-\!\overset{2}{-}\!-\!\bullet$

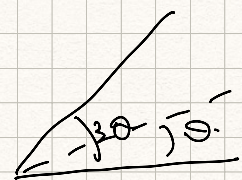
$\underline{19}$

One impossibility solved.



trisect? not possible for 60°

$$e^{i\theta} = \cos\theta + i\sin\theta$$



$\cos 3\theta$

$$e^{3i\theta} = \cos 3\theta + i\sin 3\theta$$

$$e^{-3i\theta} = \cos 3\theta - i\sin 3\theta$$

$$\cos 3\theta = \frac{e^{3i\theta} + e^{-3i\theta}}{2}$$

$$2\cos 3\theta = \underbrace{e^{3i\theta}}_{z^3} + \underbrace{e^{-3i\theta}}_{z^{-3}} \qquad z = e^{i\theta}$$

$$u = z + z^{-1} = 2\cos\theta$$

$$2\cos 3\theta = z^3 + z^{-3} =$$

$$= (z+z^{-1})^3 - 3(z+z^{-1}) = u^3 - 3u$$

$\cos\theta$

$$(z+z^{-1})^3 = z^3 + \underbrace{\binom{3}{1}}_{=3} z + \underbrace{\binom{3}{2}}_{=3} z^{-1} + z^{-3}$$

$$u^3 - 3u = 2\cos 3\theta.$$

given 3θ

$3\theta = 60^\circ \quad \theta = 20^\circ$

$$u^3 - 3u = 1$$

$\cos 3\theta = \frac{1}{2}$.

$$u^3 - 3u - 1 = 0$$

$2\cos 20^\circ$ is a root of

$u^3 - 3u - 1$ irred $/\mathbb{Q}$

hw
rational root criterion if $a_0 + \dots + a_n x^n \in \mathbb{Z}[x]$

$\frac{r}{s}$ is a root, $(r,s) = 1 \Rightarrow r \mid a_0,\ s \mid a_n$

$u^3 - 3u - 1$ $\quad \pm 1$ is not a root $\Rightarrow$ no rational roots

$\Rightarrow$ irr $/\mathbb{Q}$

$[\mathbb{Q}(2\cos 20°) : \mathbb{Q}] = 3.$ $\quad$ $\cos 20°$ is not $K_{\mathbb{R}}$-constructible.

$\quad \| $

$\underline{\mathbb{Q}(\cos 20°)}$

not possible to trisect angle $60°$. $\square$.

$\sqrt[n]{a}$ . . . . . $\qquad$ $x^2 - a \quad a \in F$.

char F.

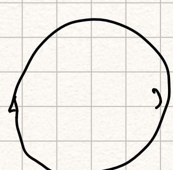
$x^n + \underline{a_{n-1}} x^{n-1} + \dots$ $\qquad$ $\underline{x^2 + \boxed{ax} + b}$

$\left(x + \frac{a_{n-1}}{n}\right)^n + . \quad = x^n + \frac{a_{n-1}}{n} \cdot n x^{n-1}$ $\qquad$ $\underline{\left(x + \frac{a}{2}\right)}^2 + \dots$

$\quad \|$

$\quad y$

$x^n + a_{n-2} x^{n-2} + \dots + a_0 = 0$



π is $\underline{\text{transcendental}}$. $\quad$ $\underline{\text{not algebraic}}$

$\leftarrow$ some complex analysis

$\sqrt{\pi}$ $\qquad$ π $\qquad$ ruler & compass

$\pi \notin F \qquad [F : \mathbb{Q}] < \infty.$

$\mathbb{Q}(\pi)$ - no relations

$\cong$ $\swarrow$ formal variable t

$\mathbb{Q}(t)$

$\underbrace{\pi^n + a_{n-1}\pi^{n-1} + \dots + a_0 = 0}$. $\qquad a_i \in \mathbb{Q}.$

uncountable $\mathbb{C}$ complex field + distance (topology)

$\cup$

countable $\overline{\mathbb{Q}}$ algebraic

$\cup$ E

$\mathbb{Q}$ rational

$e, \pi \in \mathbb{C} \setminus \overline{\mathbb{Q}}$

not algebraic.

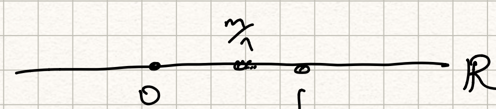
$$\begin{array}{l} \mathbb{C} \\ \cup \\ \overline{\mathbb{Q}} \\ \cup \\ E \ni \alpha \qquad [\mathbb{Q}(\alpha):\mathbb{Q}] = 2^n \qquad \sqrt[3]{2} \\ \cup \\ \mathbb{Q} \end{array}$$

$\overline{\mathbb{Q}}$ formally add roots of equations

$\cup$

$\mathbb{Q} \longrightarrow \mathbb{R}, \mathbb{C}$

"completion"



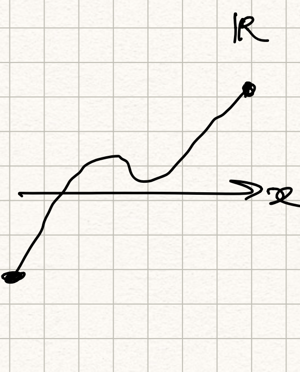
$\mathbb{C}$ ← alg. closed

almost alg. closed

$\mathbb{Q} \to \mathbb{R} \to \mathbb{C}$

i

x^2+1



π, e

$\overline{\mathbb{F}_p}$

$\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \mathbb{F}_{p^6} \ldots$

$\mathbb{F}_{p^3}$

$\underline{x^4 - 2}$