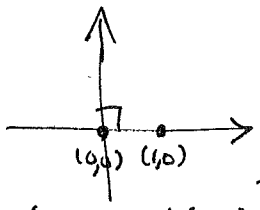
(69)
3/25/2019

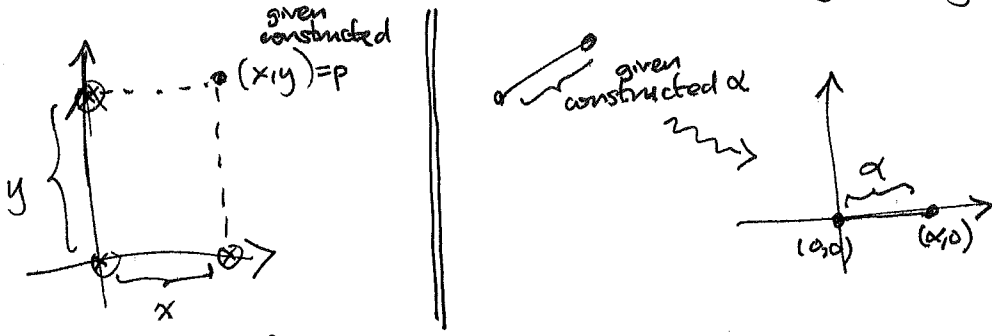
proof of THEOREM: To show every $\alpha \in \mathbb{K}_{con}$ lies in some tower

$$\mathbb{Q} \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots \subset \mathbb{K}_r \ni \alpha$$
$$\mathbb{K}_0 \quad \mathbb{K}_0(\sqrt{\alpha_1}) \quad \mathbb{K}_1(\sqrt{\alpha_2}) \quad \mathbb{K}_{r-1}(\sqrt{\alpha_r})$$

introduce coordinates in $\mathbb{R}^2$ using the original $(0,0), (1,0)$



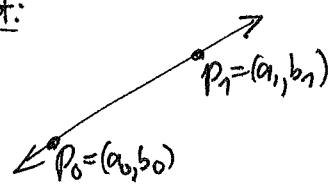
and note that $\mathbb{K}_{con} = \{ x \text{ or } y \text{ appearing in any constructed point } (x,y) \}$:



The theorem follows by induction on the number of construction steps used to reach $p=(x,y)$ if we can show these facts:

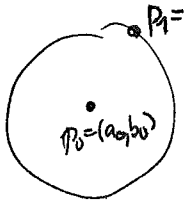
PROPOSITION (15.5.5): (a) If p_0, p_1 have coordinates in a field $\mathbb{K} \subset \mathbb{R}$, the line $\overleftrightarrow{p_0p_1}$ has equation $ax+by=c$ with $a,b,c \in \mathbb{K}$ and circle centered at p_0 through p_1 has a quadratic equation with coefficients in $\mathbb{K}$. (b) Intersecting two such lines gives a point with coefficients in $\mathbb{K}$, and intersecting such a circle and line or two circles gives points whose coefficients lie in $\mathbb{K}$ or some $\mathbb{K}(\sqrt{\alpha})$ where $\alpha \in \mathbb{K}$

proof:

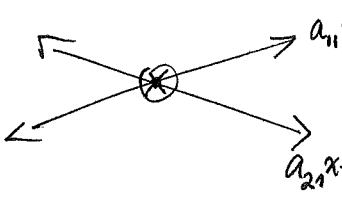


has equation $\frac{y-b_0}{x-a_0} = \frac{b_1-b_0}{a_1-a_0}$ i.e. $(a_1-a_0)(y-b_0) = (b_1-b_0)(x-a_0)$

$ax+by=c$ with coefficients in $\mathbb{K}$

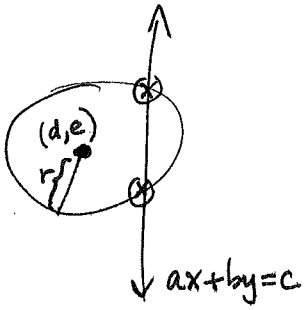


has equation $(x-a_0)^2+(y-b_0)^2 = (a_1-a_0)^2+(b_1-b_0)^2$



line intersection comes from solution to $\underbrace{\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}}_{A}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$

$\Rightarrow \begin{pmatrix} x \\ y \end{pmatrix} = \underbrace{A^{-1}}_{\text{entries in } \mathbb{K} \text{ if } A \in \mathbb{K}^{2\times 2}}\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$



line-circle intersections come from solutions to $(x-d)^2+(y-e)^2=r^2$, $ax+by=c$

Assuming $b\neq 0$ WLOG, write $y=\frac{c-ax}{b}$

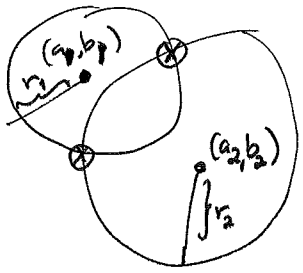
substitute $(x-d)^2+\left(\frac{c-ax}{b}-e\right)^2=r^2$

giving a quadratic equation for x of form

$Ax^2+Bx+C=0$ with $A,B,C\in\mathbb{K}$

$\Rightarrow x=\frac{-B\pm\sqrt{B^2-4AC}}{2A}\in\mathbb{K}\left(\sqrt{B^2-4AC}\right)$

and then $y=\frac{c-ax}{b}\in\mathbb{K}\left(\sqrt{B^2-4AC}\right)$



circle-circle intersections come from solutions to

$$\left\{\begin{aligned}(x-a_1)^2+(y-b_1)^2&=r_1^2\\(x-a_2)^2+(y-b_2)^2&=r_2^2\end{aligned}\right\} \text{ or } \left\{\begin{aligned}x^2-2a_1x+a_1^2+y^2-2b_1y+b_1^2&=r_1^2\\x^2-2a_2x+a_2^2+y^2-2b_2y+b_2^2&=r_2^2\end{aligned}\right\}$$

$\}$ subtract

$$\underbrace{2(a_2-a_1)x+a_1^2-a_2^2+2(b_2-b_1)y+b_1^2-b_2^2=r_1^2-r_2^2}_{\text{linear, of form } Ax+By=C \text{ with } A,B,C\in\mathbb{K}}$$

Hence solutions to $(x-a_1)^2+(y-b_1)^2=r_1^2$, $Ax+By=C$ again come from a quadratic equation on x, giving $x\in\mathbb{K}(\sqrt{\alpha})$, $y\in\mathbb{K}(\sqrt{\alpha})$. ∎

§15.6 Adjoining roots

It's handy to be able to extend a field $\mathbb{F}$ to some larger one $\mathbb{K}$ where a given $f(x) \in \mathbb{F}[x]$ has all its roots, i.e. $f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ with $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$

(e.g. when $\mathbb{F} \subset \mathbb{C}$, like $\mathbb{F} = \mathbb{Q}$ or $\mathbb{R}$ we've used $\mathbb{K} = \mathbb{C}$ like this before)

One can always find such a $\mathbb{K}$ (~~not~~ surprising)

but one can also predict whether the roots $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ will be distinct ahead of time via a calculation inside $\mathbb{F}[x]$!

PROPOSITION: (15.6.3, 15.6.6, 15.6.7, 15.6.8) Given $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$,

(a) $\exists$ a field $\mathbb{K} \supseteq \mathbb{F}$ where $f(x)$ splits completely,

i.e. $f(x) = a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ with $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ in $\mathbb{K}[x]$

(b) the $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct in $\mathbb{K}$

$$\iff \gcd_{\mathbb{K}[x]}(f(x), f'(x)) \left(= \gcd_{\mathbb{F}[x]}(f(x), f'(x)) \right) = 1$$

where $f'(x) := n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1$

$$= \sum_{i=1}^{n} i a_i x^{i-1}$$

(c) and in particular, if $f(x)$ is irreducible in $\mathbb{F}[x]$

then the $\alpha_1, \ldots, \alpha_n$ are distinct $\iff f'(x) \neq 0$,

which always happens if $\mathrm{char}(\mathbb{F}) = 0$

(and can only fail if $\mathrm{char}(\mathbb{F}) = p$ with $f(x) = g(x^p)$ for some $g(x) \in \mathbb{F}[x]$)

Before proving it, let's look at ...

EXAMPLES:

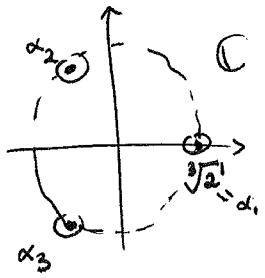
① $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ does not split completely in $\mathbb{Q}(\sqrt[3]{2})[x]$

$= (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$

but it does split completely in $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$

$\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \omega\sqrt[3]{2}$, $\alpha_3 = \omega^2\sqrt[3]{2}$

$\omega = e^{2\pi i/3}$



as $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$.

We could have guessed $\alpha_1, \alpha_2, \alpha_3$ were distinct ahead of time because $\gcd(f(x), f'(x)) = \gcd(x^3 - 2, 3x^2) = 1$

3/27/2019

② On the other hand, $f(x) = x^3 - 3x^2 + 4 \in \mathbb{Q}[x]$

has $f'(x) = 3x^2 - 6x = 3x(x-2)$

which has $x-2$ dividing $\gcd(f(x), f'(x))$ since $f(2) = 8 - 3\cdot 4 + 4 = 0$

(in fact $x - 2 = \gcd(f(x), f'(x))$).

Hence $f(x)$ must have repeated roots, and can check $f(x) = (x-2)^2(x+1)$

③ $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ does not split completely in $\mathbb{F}_2[x]$

but it does in $\mathbb{F}_4[x]$ where $\mathbb{F}_4 = \mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1)$

$= \{0, 1, \alpha, \alpha + 1\}$

as $f(x) = (x + \alpha)(x + \alpha + 1)$ $(= (x - \alpha)(x - (\alpha + 1)))$

It had distinct roots since $f'(x) = 2x + 1 = 1$ has $\gcd(f(x), f'(x)) = 1$

But $g(x) = x^4 + x^2 + 1 = (x^2 + x + 1)^2$ in $\mathbb{F}_2[x]$

does not have distinct roots in $\mathbb{F}_4[x]$: $g(x) = (x - \alpha)^2(x - (\alpha+1))^2$,

which was predictable from $f'(x) = 4x^3 + 2x = 0$

so $\gcd(f(x), f'(x)) = f(x) = x^4 + x^2 + 1 \neq 1$.

(Note $g(x) = f(x^2)$ where $f(x) = x^2 + x + 1$ from above)