12/10/2018
Mo

38.1

<u>Recall</u> Given a pair of fields $F \subseteq L$, $\alpha \in L$ is <u>algebraic</u> over F
$\Leftrightarrow \exists\ p(x) \in F[x]$ s.t. $p(\alpha) = 0$.

<u>We proved:</u>

1) Given $F \subseteq L$, $\alpha \in L$. α is algebraic $/F \Leftrightarrow \exists$ a field K with (i) $\alpha \in K$, (ii) $F \subseteq K \subseteq L$ (iii) $[K:F] := \dim_F K$ is finite.

2) If $\alpha \in L$ is algebraic over F then
$$F[\alpha] = \{a_0 + a_1\alpha + \dots + a_n\alpha^n \mid n \geq 0,\ a_1 \dots a_n \in F\}$$
is the smallest subfield of L containing F and α;
$$F[\alpha] \cong F[x]/\langle f \rangle \quad \text{where } \langle f \rangle = \{p \in F[x] \mid p(\alpha) = 0\}$$

3) f is an irreducible polynomial called the minimal poly. of α.

<u>Ruler and compass constructions</u>

Suppose we have a line segment I in the plane:

Assume length of I is 1. What are the lengths of line segments can we construct by starting with endpoints of I?

Easy to construct line segments of length n for any $n \in \mathbb{N}$.

In fact we can construct segments of length $r > 0$ for any <u>rational</u> r.

$\rightsquigarrow$ we'll call elements of $\mathbb{Q}$ "constructible".

For any $r, s \in \mathbb{Q}$ $r, s > 0$ we can construct $\sqrt{r^2 + s^2}$.

I.e. we can add to $\mathbb{Q}$ roots of polynomials $x^2 - a \in \mathbb{Q}[x]$.

$\Rightarrow$ The field extensions $\mathbb{Q}[\alpha]$ with $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 2$ are "constructible".

Repeat. We can construct field extensions

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots \subseteq F_n$$

with $[F_i : F_{i-1}] = 2 \quad i = n, \dots 1.$

Question Is there a collection of extensions

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n$$

s.t. $[F_i : F_{i-1}] = 2$ and $\sqrt[3]{2} \in F_n$?

A. No.

To prove the answer we need two lemmas

Lemma 38.1 Let $F \subseteq K \subseteq L$ be three fields with $[L:K]$, $[K:F]$ finite. Then $[L:F]$ is finite and

$$[L:F] = [L:K][K:F]$$

Lemma 38.2 Suppose $F \subseteq K \subseteq L$ are three fields with $[L:F]$ finite. Then $[L:K]$ is finite.

Remark If $F \subseteq K \subseteq L$ and $[L:F]$ is finite, then L is a finite dim v. space over F. $K \subseteq L$ is a vector subspace $\Rightarrow \dim_F K$ is finite and $[K:F] = \dim_F K \leq \dim_F L = [L:F]$

Proof of 38.2 Since $[L:F]$ is finite, L has a basis $\{v_1 \dots v_n\} \subseteq L$ a v. space over F. $\Rightarrow \forall l \in L \ \exists! \, a_i \in F \subseteq K$ st $l = \sum a_i v_i$

Since all $a_i \in K$, $\{v_1 \dots v_n\}$ spans L as a v. space $/K$.

$\Rightarrow \dim_K L \leq n = \dim_F L$. $\square$

Proof of 38.1 Since L is finite dimensional over K $\exists$ a basis $\{v_1 \dots v_m\} \subseteq L$ of L over K.

Since K is finite dimensional over F, $\exists$ a basis $\{w_1 \dots w_n\} \subseteq K$ of K over F.

$\Rightarrow \forall\, \ell \in L \quad \exists!\, a_j \in K$ s.t. $\quad \ell = \sum_{i=1}^{m} a_i v_i$

Given $a_i \in K \quad \exists!\, b_{ij}$ s.t. $\quad a_i = \sum_{j=1}^{n} b_{ij} w_j$

$\Rightarrow \ell = \sum_i \sum_j b_{ij} w_j v_i = \sum_{i,j} b_{ij} (v_i w_j)$

$\Rightarrow \{v_i w_j\}_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ spans L over F.

Not hard to show (do it!) $\{v_i w_j\}$ is linearly independent / F.

$\therefore \{v_i w_j\}_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ is a basis of L over F

$\therefore [L:F] = \dim_F L = n \cdot m = [L:K][K:F]$. $\square$

Back to our question:

$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n \qquad [F_i : F_{i-1}] = 2$

Why can't we have $\sqrt[3]{2} \in F_n$?

If $\sqrt[3]{2} \in F_n$, $\quad \mathbb{Q}[\sqrt[3]{2}] \subseteq F_n$.

$[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$ since $x^3 - 2$ is the min polynomial $\sqrt[3]{2}$.

Since $[F_n : F_{n-1}] = 2 = [F_{n-1} : F_{n-2}]$

$[F_n : F_{n-2}]$ is finite and equals $2 \cdot 2$ by 38.2.

Since $[F_{n-2} : F_{n-3}] = 2$, same argument $\Rightarrow [F_n : F_{n-3}] = 2^3$

.... (ie induction on n)

$[F_n : \mathbb{Q}] = 2^n$.

By 38.2 $\quad [F_n : \mathbb{Q}\sqrt[3]{2}]$ is finite. (since $[F_n : \mathbb{Q}]$ is finite)

$\Rightarrow 2^n = [F_n : \mathbb{Q}] = [F_n : \mathbb{Q}[\sqrt[3]{2}]][\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = [F_n : \mathbb{Q}\sqrt[3]{2}] \cdot 3$

This is impossible since $3 \nmid 2^n$ for any $n \ge 1$

$\Rightarrow \sqrt[3]{2}$ is not constructible by ruler and compass.