# Announcements

First part of HW4 posted (due Wed. 2/19)

Midterm 1: Thurs. 2/15 7:00-8:30 pm Loomis Lab. 144

- Covers roughly everything through Friday (will be more precise)
- Will post practice questions (from D&F) by the weekend; we'll discuss them next week)

---

Recall: If $\alpha$ is alg. / $F$, there exists a unique monic poly. $m_{\alpha,F}(x) \in F[x]$ of min'l degree s.t. $m_{\alpha,F}(\alpha) = 0$. This is called the <u>minimal poly.</u> of $\alpha$ over $F$.

Furthermore,

- $m_{\alpha,F}$ is irred.
- $\deg m_{\alpha,F} = [F(\alpha):F]$
- $\underset{p \in F[x]}{p(\alpha) = 0} \iff p \in (m_{\alpha,F}(x))$
- If $F \subseteq L$, $m_{\alpha,L} \mid m_{\alpha,F}$

Def: $K/F$ is algebraic if every $\alpha \in K$ is alg. $/F$.

Prop: If $[K:F] < \infty$, then $K/F$ is alg.
"finite ext'n"

Pf: If $\alpha \in K$ is not alg., then $1, \alpha, \alpha^2, \ldots$ are linearly indep.

$\square$

Converse doesn't hold

e.g. $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$

$K$ is alg. $/\mathbb{Q}$, but $[K:\mathbb{Q}] = \infty$

since $x^n - 2$ is the min'l poly. for $\sqrt[n]{2}$ (by Eisenstein), so

$$[K:\mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}] = n \quad \forall n$$

Def: The set of algebraic numbers is

$$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ is alg.}/\mathbb{Q}\}$$

Thm: $\overline{\mathbb{Q}}$ is a field.

This follows from:

Prop: Let $F \subseteq K$ and let $\alpha, \beta \in K$ be alg. / $F$.
Then $F(\alpha,\beta)/F$ is alg.

(so in particular, $\alpha+\beta$, $\alpha/\beta$, ...) are alg. / $F$.)

Pf: Since $\beta$ is alg. / $F$, it is alg. / $F(\alpha)$.

Let $b_1, \dots, b_m$ be a basis for $F(\alpha,\beta)$ over $F(\alpha)$, and let $a_1, \dots, a_n$ be a basis for $F(\alpha)$ over $F$.

Then every elt. of $F(\alpha,\beta)$ is an $F$-linear comb. of $a_i b_j$*, so $[F(\alpha,\beta):F]$ is finite and thus alg.

*details in a moment □

Let's take a more general view here:

Tower Law: Let $F \subseteq K \subseteq L$. Then,

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

Pf: First assume RHS is finite.

$$n := [K:F] \quad \text{basis: } \alpha_1, \dots, \alpha_n \in K$$

$$m := [L:K] \quad \text{basis: } \beta_1, \dots, \beta_m \in L$$

We claim that $\{\gamma_{ij} := \alpha_i \beta_j \in L\}$ forms an $F$-basis for $L$.

Example: $\overset{F}{\mathbb{Q}} \subseteq \overset{K}{\mathbb{Q}(\underset{\alpha^3}{\underset{\parallel}{\sqrt{2}}})} \subseteq \overset{L}{\mathbb{Q}(\underbrace{\sqrt[6]{2}}_{\alpha})}$

$$\beta \in \mathbb{Q}(\sqrt[6]{2}) \quad \beta = a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 + f\alpha^5$$

$$= (a + d\sqrt{2}) + (b + e\sqrt{2})\alpha + (c + f\sqrt{2})\alpha^2$$

Basis for $K/F$: $1, \sqrt{2}$

Basis for $L/K$ : $1, \alpha, \alpha^2$

Basis for $L/F$ : $1, \alpha, \alpha^2, \underset{\sqrt{2}}{\alpha^3} , \underset{\alpha\sqrt{2}}{\alpha^4}, \underset{\alpha^2\sqrt{2}}{\alpha^5}$

Return to proof:

Let $l \in L$. Since $\{\alpha_1, \dots, \alpha_n\}$ basis for $L/K$,

$$l = k_1\alpha_1 + \cdots + k_n\alpha_n, \quad k_i \in K \quad \text{(unique!)}$$

Since $\{\beta_1, \dots, \beta_m\}$ basis for $K/F$,

$$k_i = f_{i1}\beta_1 + \cdots + f_{im}\beta_m, \quad f_{ij} \in F \text{ (unique!)}$$

So

$$l = f_{11}\alpha_1\beta_1 + f_{12}\alpha_1\beta_2 + \cdots + f_{nm}\alpha_n\beta_m \quad \text{(unique!)}$$

Now, if RHS is infinite, LHS is also infinite since

$$[L:F] \geq [L:K] \quad \text{and} \quad [L:F] \geq [K:F]$$

$\square$

Cor: $F \subseteq K \subseteq L$.

a) If $L/K$ and $K/F$ are both finite, so is $L/F$

b) If $L/K$ and $K/F$ are both algebraic, so is $L/F$

Pf: a) follows from the Tower Law.

b) Let $\beta \in L$, and consider

$$m_{\beta,K}(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 \in K[x].$$

Since simple alg. ext'n's are finite (w/ degree equal to deg. min'l poly.), $K(\beta)/K$ is finite since

$$F \subseteq F(\alpha_0) \subseteq F(\alpha_0, \alpha_1) \subseteq \cdots \subseteq F(\alpha_0, \ldots, \alpha_n) \subseteq F(\alpha_0, \ldots, \alpha_n, \beta)$$

are simple, alg. ext'n's. Thus $\beta$ is alg. / $F$ $\forall \beta \in L$, so $L$ is alg / $F$. $\square$

Surprising consequences such as:

Ex: $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$

Pf: $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ since $x^n - 2$ is irred.

If $\sqrt{2} \in \mathbb{Q}(\sqrt[3]{2})$, then $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[3]{2})$ and

$$3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})]\underbrace{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]}_{2},$$ a contradiction $\square$

Next time: use Tower Law to explore constructability w/ straightedge and compass