Announcements

Midterm 1: Wednesday 2/19 7:00-8:30pm Sidney Lu 1043

- Material: everything through §13.2
- One reference sheet allowed (regular size, two sided)
- see policy email for more

Practice problems (from D&F): see policy email

HW4 posted (due Wed. 2/26 @ 9am)

Recall: F: Field, $p(x) \in F[x]$ irred, nonconstant

If $\alpha \in K \supseteq F$ is a root of p, then

- $$F(\alpha) \cong F[x]/(p(x))$$
  $$\alpha \mapsto \overline{x}$$

- $[F(\alpha):F] = \deg p(x) =: n$, and
  $\{1, \alpha, \dots, \alpha^{n-1}\}$ is an F-basis of $F(\alpha)$.

- In particular,
  $$F(\alpha) = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_i \in F\}$$
  is a field, even though it doesnt look like one

- If β is another root of $p(x)$, then
  $$F(\alpha) \cong F(\beta)$$
  $$\alpha \mapsto \beta$$

Extension Theorem: Let $\varphi: F \xrightarrow{\sim} F'$ be an isom. of fields. Let $p(x) \in F[x]$ be irred., and let $p'(x) \in F'[x]$ be the irred. poly obtained by applying φ to the coeffs. of p.

Let α be a root of p (in some extn of F)

Let β be a root of p' (in some extn of F')

Then $\exists$ isom.

$$\sigma: F(\alpha) \xrightarrow{\sim} F'(\beta)$$

$$f \longmapsto \varphi(f) \qquad (\sigma|_F = \varphi)$$

$$\alpha \longmapsto \beta$$

(Seems unintuitive now, but useful later)

$$\begin{tikzcd} \sigma: F(\alpha) \arrow[r, "\sim"] \arrow[d, dash] & F'(\beta) \arrow[d, dash] \\ \varphi: F \arrow[r, "\sim"] & F' \end{tikzcd}$$

Pf (skip in class): Let $\tilde{\varphi}$ be the isom.

$$\tilde{\varphi} : F[x] \xrightarrow{\sim} F'[x]$$
$$f \mapsto \varphi(f)$$
$$x \mapsto x$$

Then $\tilde{\varphi}$ maps $(p(x))$ to $(p'(x))$, so it induces an isom

$$F[x]/(p(x)) \xrightarrow{\sim} F'[x]/(p'(x))$$
$$f \overset{\sim}{\longmapsto} \varphi(f) + (p')$$
$$x + (p) \overset{\sim}{\longmapsto} x + (p')$$

Combining this w/ our previous isoms., σ is the map

$$F(\alpha) \xrightarrow{\sim} F[x]/(p(x)) \xrightarrow{\sim} F'[x]/(p'(x)) \xrightarrow{\sim} F'(\beta)$$
$$f \longmapsto f + (p) \longmapsto \varphi(f) + (p') \longmapsto \varphi(f)$$
$$\alpha \longmapsto x + (p) \longmapsto x + (p') \longmapsto \beta$$

$\square$

Algebraic Extensions

Rephrasing the facts from the start of class:

Thm: $K := F(\alpha)$.

a) If $[K:F] < \infty$, $\exists\, p(x) \in F[x]$ irred.
s.t. $p(\alpha) = 0$ and $K \cong F[x]/(p(x))$

b) If $[K:F] = \infty$, then $K \cong F(x)$
and $\forall p(x) \in F[x]$, $p(\alpha) \neq 0$.

Def:

In case a), we call α and K/F <u>algebraic</u>
In case b), we call α and K/F <u>transcendental</u>

Prop/def: If α is alg. / F, there exists a unique monic poly. $m_{\alpha,F}(x) \in F[x]$ of min'l degree s.t. $m_{\alpha,F}(\alpha) = 0$. Furthermore, $\deg m_{\alpha,F} = [F(\alpha):F]$

and $\underset{p \in F[x]}{p(\alpha) = 0} \iff p \in (m_{\alpha,F}(x))$

Example: $F = \mathbb{Q}$ $\alpha = \sqrt{2}$

$m_{\alpha,F}(x) = x^2 - 2$

$p(\sqrt{2}) = 0 \iff x - \sqrt{2} \mid p(x)$ in $\mathbb{Q}(\sqrt{2})[x]$
$p \in \mathbb{Q}[x]$

$\iff x^2 - 2 \mid p(x)$ in $\mathbb{Q}[x]$

Pf: Let $I = \{p(x) \in F[x] \mid p(\alpha) = 0\}$. Since $F[x]$ is a PID, let $m_{\alpha,F}(x)$ be a (monic) generator for I. Since I is a prime ideal, p is irred. Now we have

$$F(\alpha) \cong F[x]/(m_{\alpha,F}(x)), \text{ so}$$

$$[F(\alpha):F] = \deg m_{\alpha,F}.$$

$\square$

Prop: If α alg./F and $F \subseteq L$, then α is alg./L and $m_{\alpha,L}(x) \mid m_{\alpha,F}(x)$ in $L[x]$.

Pf: $m_{\alpha,F}(x) \in F[x] \subseteq L[x]$, so α is alg./L.

Since $m_{\alpha,F}(\alpha) = 0$, $m_{\alpha,F}$ must therefore be a multiple of $m_{\alpha,L}(x)$. $\square$

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, $\alpha + \beta$, α/β, ... are alg. / F.)

Pf: Since β is alg. / F, it is alg. / $F(\alpha)$. Let $b_1, \ldots, b_m$ be a basis for $F(\alpha, \beta)$ over $F(\alpha)$, and let $a_1, \ldots, a_n$ 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. $\square$

*details next time