4/22/14

Exam 3 on Thursday

Today: Review

Topic: Polynomials in 1 variable.

Let $S \supseteq R$ be a ring extension. Then for all $\alpha \in S$ we have an evaluation homomorphism

$$ev_\alpha : R[x] \longrightarrow S$$
$$f(x) \longmapsto f(\alpha).$$

We define "R adjoin α":

$$R[\alpha] := im(ev_\alpha)$$
$$= \{ f(\alpha) : f(x) \in R[x] \}.$$

This is the smallest subring of S containing $R \cup \{\alpha\}$. By the First Isomorphism Theorem we have

$$\frac{R[x]}{\ker(ev_\alpha)} \approx R[\alpha] \subseteq S$$

Q: What can we say about $\ker(ev_\alpha)$?

A: In general not much. However, if $R = K$ is a field then $K[x]$ is a PID and hence

$$\ker(ev_\alpha) = (m_\alpha(x)) < K[x]$$

for some unique polynomial (with leading coefficient 1) called the minimal polynomial of $\alpha \in S$ over K.

If $m_\alpha(x) = 0$ we say α is transcendental over K. If $m_\alpha(x) \neq 0$ then we say α is algebraic over K.

If furthermore S is a domain then we have the

☆ Minimal Polynomial Theorem:

Let $S \supseteq K$ be a ring extension where K is a field, S is a domain, and $\alpha \in S$ is algebraic over K.

Then

(1) The minimal polynomial $m_\alpha(x) \in K[x]$ is irreducible.

(2) $K[\alpha]$ is a field, and we can write $K[\alpha] = K(\alpha)$.

(3) $K(\alpha)$ is finite dimensional as a vector space over K. In fact if $\deg(m_\alpha(x))$ then $K(\alpha)$ has basis

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}.$$

We say $[K(\alpha) : K] = \deg(m_\alpha(x))$.

Proof:

(1) Suppose for contradiction that

$$m_\alpha(x) = f(x)g(x)$$

where $f, g \in K[x]$ are proper factors. Evaluate at α to get

$$0 = m_\alpha(\alpha) = f(\alpha)g(\alpha).$$

Since S is a domain this implies $f(\alpha) = 0$ or $g(\alpha) = 0$. WLOG say $f(\alpha) = 0$.

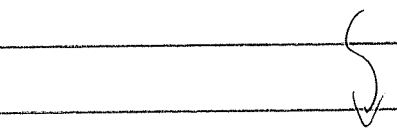
Then $f(x) \in \ker(ev_\alpha) = (m_\alpha(x))$ so that $m_\alpha(x) \mid f(x)$ and $\deg(m_\alpha) \leq \deg(f)$. This contradicts the fact that f is a proper factor. //

(2) Since $m_\alpha(x)$ is irreducible we know that $(m_\alpha) < K[x]$ is maximal among principal ideals. Then since $K[x]$ is a PID we know that (m_α) is maximal among <u>all</u> ideals. It follows that

$$K[\alpha] \approx K[x]/(m_\alpha)$$

is a field. //

(3) Let $n = \deg(m_\alpha)$. We will show that $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a basis for $K(\alpha)$ over K in two steps.



i) Span? Consider any element $f(\alpha) \in K(\alpha)$ and divide by $m_\alpha(x)$ in $K[x]$ to get

- $f(x) = q(x) m_\alpha(x) + r(x)$
- $r(x) = 0$ or $\deg(r) < \deg(m_\alpha) = n$

Evaluating at α gives

$$f(\alpha) = q(\alpha) \cancel{m_\alpha(\alpha)}^{0} + r(\alpha)$$
$$= r(\alpha) \in \text{span}_K\{1, \alpha, \dots, \alpha^{n-1}\}. \quad //$$

ii) Independent? Suppose that there exist $a_0, a_1, \dots, a_{n-1} \in K$ such that

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} = 0.$$

We want to show that $a_0 = a_1 = \cdots = a_{n-1} = 0$. So define the polynomial

$$f(x) := a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in K[x].$$

Since $f(\alpha) = 0$ we have $f \in \ker(ev_\alpha) = (m_\alpha)$ and hence $m_\alpha(x) \mid f(x)$.

↓

If $f \neq 0$ this implies that

$$n = \deg(m_\alpha) \leq \deg(f) \leq n-1.$$

Contradiction. Hence $f = 0$ as desired.

∎

Algebraic closure:

Let $S \supseteq K$ be a ring extension where K is a field and S is a domain.
Define the algebraic closure of K in S:

$$\overline{K} := \{ \alpha \in S : f(\alpha) = 0 \text{ for some } f(x) \in K[x] \}.$$

Certainly this is a subset of S.
I claim that $\overline{K}$ is actually a field.

To show this consider any $\alpha, \beta \in \overline{K}$.
We want to show that $\alpha - \beta \in \overline{K}$
and $\alpha \beta^{-1} \in \overline{K}$ (assume $\beta \neq 0$).

↓

Proof: Since $\alpha \in \overline{K}$ is algebraic over K we have

$$[K(\alpha) : K] = \dim_K(K(\alpha)) < \infty.$$

Then since $\beta \in \overline{K}$ is algebraic over K (hence also over $K(\alpha)$) we have

$$[K(\alpha)(\beta) : K(\alpha)] = \dim_{K(\alpha)}(K(\alpha)(\beta)) < \infty.$$

Using the Tower Law (T.O.U.) we have

$$[K(\alpha)(\beta) : K] = [K(\alpha)(\beta) : K(\alpha)]\,[K(\alpha) : K] < \infty.$$

Finally for any $\gamma \in K(\alpha)(\beta)$ we know that the set $1, \gamma, \gamma^2, \cdots$ is linearly dependent over K, hence there exist $a_0, a_1, \cdots, a_n \in K$ not all zero such that

$$a_0 + a_1\gamma + \cdots + a_n\gamma^n = 0.$$

We conclude that γ is algebraic over K. Since $\alpha - \beta, \alpha\beta^{-1} \in K(\alpha)(\beta)$ we conclude that they are algebraic over K ///

Now we will prove

The Tower Law: Given fields $M \supseteq L \supseteq K$ we have

$$[M:K] = [M:L][L:K].$$

Proof: Let $M \supseteq L$ have basis

$$\alpha_1, \alpha_2, \ldots, \alpha_m$$

and let $L \supseteq K$ have basis

$$\beta_1, \beta_2, \ldots, \beta_n.$$

I claim that $\{\alpha_i \beta_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for $M \supseteq K$.

i) Span? Given any $a \in M$ we have

$$a = a_1 \alpha_1 + \cdots + a_m \alpha_m$$

for some $a_1, \ldots, a_m \in L$. Then for all $1 \leq i \leq m$ we have

$$a_i = b_{i1}\beta_1 + \cdots + b_{in}\beta_n$$

for some $b_{ij} \in K$. We conclude that

$$a = \sum_i \left(\sum_j b_{ij}\beta_j \right) \alpha_i$$

$$= \sum_{i,j} b_{ij}\alpha_i\beta_j \quad \text{as desired.}$$

ii) Independent? Consider any $c_{ij} \in K$ such that

$$\sum_{i,j} c_{ij}\alpha_i\beta_j = 0.$$

Then $0 = \sum_i \left(\sum_j c_{ij}\beta_j \right) \alpha_i$ and since the α_i are independent over L we have

$$\sum_j c_{ij}\beta_j = 0$$

for all i. Then since the β_j are independent over K we have

$$c_{ij} = 0$$

for all i,j.

Kronecker's Theorem:

Let $K[x]$ be a field and consider any irreducible polynomial $f(x) \in K[x]$. Then $(f(x)) < K[x]$ is a maximal ideal and the quotient ring

$$L := K[x]/(f(x)) \text{ is a field.}$$

Note that the ring homomorphism

$$\varphi : K \longrightarrow K[x] \longrightarrow K[x]/(f(x))$$
$$a \longmapsto a \longmapsto a + (f(x))$$

is injective. Indeed, consider $a, b \in K$ such that $a + (f(x)) = b + (f(x))$. Then

$$a - b \in (f(x)).$$

If $a - b \neq 0$ this implies $a - b = f(x)g(x)$ for some $0 \neq g(x) \in K[x]$ and hence

$$0 = \deg(a-b) = \deg(f) + \deg(g) \geq \deg(f).$$

But since f is irreducible we have $\deg(f) \geq 1$. Contradiction. Hence $a = b$. ///

Now the First Isomorphism gives

$$K \approx K/(0) \approx \operatorname{im}\varphi \subseteq L$$

and we can think of L as a field extension of K.

Note that $f(x) \in K[x]$ has no root in K (it's irreducible — use Descartes) but it does have a root in L.

Indeed, let $\alpha := x + (f(x))$. Then we evaluate $f(x)$ at α to get

$$\begin{aligned} f(\alpha) &= f(x + (f(x))) \\ &= f(x) + (f(x)) \\ &= 0 + (f(x)) \\ &= 0 \in L. \end{aligned}$$

///

By Descartes we can factor

$$f(x) = (x - a)\, g(x) \quad \text{in } L[x].$$

Then by induction on degree there exists a field extension $M \supseteq L \supseteq K$ in which g, and hence f, splits.

This is called Kronecker's Theorem.

Final Topics:

Recall Descartes' Theorem and long division of polynomials