4/8/11

Def: $\mathbb{Q}[x_1, \dots x_n]$ for $x_1, \dots x_n \in \mathbb{R}$ denotes the smallest subfield of $\mathbb{R}$ containing $\mathbb{Q} \cup \{x_1, \dots, x_n\}$.

Recall: F is a field, $\alpha \in F$ is called algebraic over F if $\exists$ a polynomial $p \in F[x]$ with $p(\alpha) = 0$. If α is not algebraic we say α is transcendental over F

Examples:

1) $\sqrt{2}, \sqrt[3]{7} \in \mathbb{R}$ are algebraic over $\mathbb{Q}$

eg. $p(x) = x^2 - 2 \Rightarrow p(\sqrt{2}) = 0$

$q(x) = x^3 - 7 \Rightarrow q(\sqrt[3]{7}) = 0$

NOTE: It is trivial that $\sqrt{2}$ and $\sqrt[3]{7}$ are algebraic over $\mathbb{R}$ since you could take the polynomials $x - \sqrt{2}$ and $x - \sqrt[3]{7}$. Also, π is algebraic over $\mathbb{R}$ ($p(x) = x - \pi$) but transcedental over $\mathbb{Q}$ (Lindenman, 1882 - hard!)

- e is transcedental over $\mathbb{Q}$, but it is not known weather $\pi + e$ is transcedental over $\mathbb{Q}$.

Fun Fact: Gelfand - Schneider Thm:

If a, b are algebraic over $\mathbb{Q}$, $b \notin \mathbb{Q}$ and $a \notin \{0, 1\}$, then a^b is transcedental.

ex: $2^{\sqrt{2}}$ is transcedental

Def: A field F is called <u>algebraicly closed</u> if $\alpha \in E$ and E is an extension of F, then if $\exists\ p \in F[x]$, $p(\alpha) = 0$ then $\alpha \in F$

<u>Examples:</u>

1) $\mathbb{Q}$, $\mathbb{R}$ ($p(x) = x^2 + 1$) <u>not</u> algebraicly closed
2) $\mathbb{C}$ is algebraicly closed

Def: $p \in F[x]$, F is a field. Then p is said to be <u>irreducible</u> if there does not exist non-constant polynomials $q, r \in F[x]$ with $p = q \cdot r$

<u>Examples:</u>

1) $p(x) = x^2 + 1$ is irreducible of $\mathbb{R}$ but not over $\mathbb{C}$, since $p(x) = (x - i)(x + i)$

2) $p(x) = x^3 + x^2 + x + 1$ is not irreducible in $\mathbb{Q}[x]$ since $p(x) = (x + 1)(x^2 + 1)$

<u>NOTE:</u> The definition of irreducible can be extended to $R[x]$ where R is an integral domain.

(FTET) Pf: By decomposing p into irreducible components it suffices to prove that the thm in the case where p is irreducible.
$E = F[x]/\langle p \rangle$. We know by previous thm, that $\langle p \rangle$ is maximal. By HW 8, R/I is a field iff I is maximal for R a ~~unital~~ commutative ring $\alpha = x + \langle p(x) \rangle$ check!

4/11/11

Recall: R an integral domain, $p \in R[x]$. Then p is irreducible if $p = q \cdot r$ for $q, r \in R[x]$ implies q or r is constant (i.e. in R)

Note: $\mathbb{Z}$ is an integral domain. The polynomial $2x^2 + 2 \in \mathbb{Z}[x]$ is irreducible and $\langle 2x^2 + 2 \rangle \subsetneq \langle 2 \rangle \subsetneq \mathbb{Z}[x]$ so the ideal $\langle 2x^2 + 2 \rangle$ is not maximal, which implies the theorem (p irreducible iff $\langle p \rangle$ maximal) is false for integral domains.

Thm: let F be a field and $p \in F[x]$. Then p is irreducible iff $\langle p \rangle$ is maximal.
Pf: Continued on next page →

Pf: $\Rightarrow$ Suppose p is irreducible and let $\langle p \rangle \subseteq J \subseteq F[x]$ for some ideal J. Want to show either $J = \langle p \rangle$ or $J = F[x]$. We proved that $F[x]$ is a principle ideal domain (in fact, we proved $F[x]$ is a Euclidean Domain, which implies $F[x]$ is a principle ideal domain). Then $\exists$ a $q \in F[x]$ with $J = \langle p \rangle$. Since $p \in \langle p \rangle \subseteq J = \langle q \rangle$ $\exists$ an $r \in F[x]$ with $p = q \cdot r$. By irreducibility, either $q \in F^\times$ or $r \in F^\times$. If $q \in F^\times$, then $1 = \frac{1}{q} \cdot q \in \langle q \rangle \Rightarrow \langle q \rangle = F[x]$. If $r \in F^\times$, then $p = q \cdot r \Rightarrow \frac{1}{r} p = q$, hence $q \in \langle p \rangle$. Then $\langle q \rangle \subseteq \langle p \rangle$ and we assumed $\langle p \rangle \subseteq \langle q \rangle$ so $\langle q \rangle = \langle p \rangle$, which implies $\langle p \rangle$ is maximal.

$\Leftarrow$ Suppose $\langle p \rangle$ is maximal. If $p(x) = q(x) r(x)$ for $q, r \in F[x]$, then $p \in \langle r \rangle$ and $p \in \langle q \rangle$, so $\langle p \rangle \subseteq \langle r \rangle$ and $\langle p \rangle \subseteq \langle q \rangle$. By maximality, either $\langle r \rangle = \langle p \rangle$ or $\langle r \rangle = F[x]$. If $\langle r \rangle = \langle p \rangle$, then also, $r(x) = s(x) p(x)$. $r(x) = s(x) q(x) r(x) \Rightarrow s(x) q(x) = 1$ so, s, q are in $F^\times$. This implies that $\deg(q) = 0$, so $\deg(r) = \deg(p)$. If $\langle r \rangle = F[x]$, then $\exists$ a $t \in F[x]$ with $r(x) t(x) = 1$. So r is invertible $\Rightarrow r \in F^\times \Rightarrow \deg(r) = 0$. This shows p is irreducible ∎

Thm: Fundamental Thm of Field Theory

let F be a field, $p \in F[x]$. Then $\exists$ an extension field E of F and $\alpha \in E$ with $p(\alpha) = 0$ (proved p is irreducible).

Pf:

Without irreducibility we decompose p into irreducible components so we are justified in assuming p is irreducible $E = F[x]/\langle p \rangle$. E is a field since p irreducible $\iff$ $\langle p \rangle$ is maximal $\Rightarrow$ (HW 8) $F[x]/\langle p \rangle$ is a field. $\alpha = x + \langle p \rangle$. Show $p(\alpha) = 0$. Here $0 = 0 + \langle p \rangle = \langle p \rangle$. Show $p(\alpha) = \langle p \rangle$. let $p(x) = \sum_{i=0}^{n} \beta_i x^i$ for $\beta_1, \dots, \beta_n \in F$.

$$p(\alpha) = (x + \langle p \rangle)$$
$$= \sum_{i=0}^{n} \beta_i (x + \langle p \rangle)^i$$
$$= \sum_{i=0}^{n} \beta_i (x^i + \langle p \rangle)$$

(by def of multiplication in $F[x]/\langle p \rangle$) ↳

$$p(\alpha) = \sum_{i=0}^{n} (\beta_i x^i + \beta_i \langle p \rangle)$$
$$= \sum_{i=0}^{n} (\beta_i x^i + \langle p \rangle) \quad \text{since } \langle p \rangle \text{ is an ideal}$$
$$= \left(\sum_{i=0}^{n} (\beta_i x^i)\right) + \langle p \rangle$$
$$= p + \langle p \rangle = 0 + \langle p \rangle \quad \text{since } p \in \langle p \rangle$$ ∎

Corollary: If F is a field and $p \in F[x]$, then $\exists$ an extension field E and $\alpha_1, \dots, \alpha_n \in E$ with $p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ where $n = \deg(p)$

PF: Fundamental thm + induction (on $\deg(p)$).

Def: The smallest extension E of F $\ni$ p factors into linear terms is called the splitting field of p.

Example

1) $F = \mathbb{R}$, $p(x) = x^2 + 1$

$\mathbb{R}[x]/\langle x^2+1 \rangle$ is a field since x^2+1 is irreducible in $\mathbb{R}[x]$

$\mathbb{R}[x]/\langle x^2+1 \rangle$ is isomorphic as a field to $\mathbb{C}$, the isomorphism is as follows:

Basis for $\mathbb{R}[x]/\langle x^2+1 \rangle$ is $\{1, x\}$ since $x^2 + 1 = 0$, so $x^2 = 1$.

Construct $\varphi: \mathbb{R}[x]/\langle x^2+1 \rangle \to \mathbb{C}$ by $\varphi(\alpha x + \beta) = \alpha i + \beta$ for $\alpha, \beta \in \mathbb{R}$. $\mathbb{C}$ is the splitting field for $x^2 + 1$.

Next time: A good way to show polynomials are irreducible, then review....