* Final 8:00 AM Wed April 27 4/13/11

Fix From Last Time:

$\langle 2x^2+2\rangle \subsetneq \langle 2\rangle \subsetneq \mathbb{Z}[x]$ is not a counterexample to (p irreducible $\Leftrightarrow$ p maximal) since $2x^2+2$ is not irreducible! $2(x^2+1)$, $2 \notin \mathbb{Z}^\times$

Real counterexample:

$p(x) = x^2+2$ is irreducible in $\mathbb{Z}[x]$

$\langle p\rangle \subsetneq J \subsetneq \mathbb{Z}[x]$ where

$J = \{ p \in \mathbb{Z}[x] : p$ has even constant coefficients$\}$

so, $\langle p\rangle$ is not maximal in $\mathbb{Z}[x]$

Let R be an integral domain. How do you tell if $p \in R[x]$ is irreducible?

Def: An ideal $I \subseteq R$ is called prime if for $x, y \in R$, if $xy \in I$ then either $x \in I$ or $y \in I$.

Examples:

1) $R = \mathbb{Z}$, $I = p\mathbb{Z}$ where p is prime
if $m, n \in \mathbb{Z}$ and $m \cdot n \in p\mathbb{Z}$. since p is prime, either p divides n or p divides m
$\Rightarrow$ either $n \in p\mathbb{Z}$ or $m \in p\mathbb{Z}$
(motivating example)

2) $R = C_0(\mathbb{R})$, $I_x = \{f \in C_0(\mathbb{R}) : f(x) = 0\}$ $(x \in \mathbb{R})$
If $g, h \in C_0(\mathbb{R})$ and $gh \in I_x$ then $g(x)h(x) = 0$
$\Rightarrow$ either $g(x) = 0$ or $h(x) = 0$ $\Rightarrow$ either $g \in I_x$ or $h \in I_x$.

Eisenstein's Criterion (awesome):

Suppose R is an integral domain and $I \subseteq R$ is a prime ideal. If $p(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$ (monic) $\in R[x]$ and $a_0, \dots, a_{n-1} \in I$ but there are no elements $\beta, \gamma \in I$ with $a_0 = \beta\gamma$, then p is irreducible in $R[x]$.

Applications usually to $\mathbb{Z}[x]$ or $\mathbb{Q}[x]$.
let $p(x) = x^6 + 9x^2 + 12x + 6$
$I = 3\mathbb{Z}$. $9, 12, 6 \in 3\mathbb{Z}$ but $6 \neq nm$ for $n, m \in 3\mathbb{Z}$ since $6 = 1 \cdot 6$ or $6 = 2 \cdot 3$ and neither 2 or 1 are in $3\mathbb{Z}$
Then p is irreducible in $\mathbb{Z}[x]$.

HW: #8, #3

Show: If F is a field and E an extension of F, then the subset of E consisting of all algebraic elements of E over F is a field.

Notation: $[E:F]$ means the degree of E over F, which is the dimension of E as a vector space over F.

Thm: Let $\alpha \in E$ be algebraic over F and let $p \in F[x]$ be irreducible, $p(\alpha) = 0$. Then $F[x]/\langle p \rangle$ is field isomorphic to $F(\alpha)$, the smallest subfield of E containing both F and α.

Pf: (sketch)

Define $\Phi: F[x] \to F(\alpha)$ by $\Phi(q(x)) = q(\alpha)$ $\forall\, q \in F[x]$. Extend to $\bar{\Phi}: F[x]/\langle p \rangle \to F(\alpha)$ $\bar{\Phi}(q(x) + \langle p \rangle) = q(\alpha)$. $\bar{\Phi}$ is surjective since the image contains both F (constant polynomials) and α (take $q(x) = x$) Injective since $\bar{\Phi} \neq 0$ and fields have no nontrivial proper ideal. observe $\bar{\Phi}$ is a homomorphism ∎

Thm: Let E be an extension field of F and K an extension field of E then $[K:F] = [K:E][E:F]$

Pf: tedious linear algebra...

Thm: $\alpha \in E$ is algebraic over F iff $[F(\alpha):F]$ is finite.

Pf: $\Rightarrow$ Suppose α algebraic. Take a polynomial p in $F[x]$ of minimal degree with $p(\alpha) = 0$. p is automatically irreducible, hence $f(\alpha)$ is field isomorphic to $F[x]/\langle p \rangle$. If the degree of p is n, →

Pf $\Rightarrow$ cont: then $1, x, x^2, \dots, x^{n-1}$ constitutes a basis for $F[x]/\langle p\rangle$ under the image of the quotient map. ie., $1+\langle p\rangle, x+\langle p\rangle, \dots x^{n-1}+\langle p\rangle$.
Since $p(x) = \sum_{i=0}^{n} a_i x^i$ then
$x^n + \langle p\rangle = -\frac{1}{a_n} \sum_{i=0}^{n-1} a_i x^i + \langle p\rangle$. This implies
$[F[x]/p : F] = n$ so, $[F(\alpha) : F] = n$.

$\Leftarrow$ Suppose $[F(\alpha) : F] = n$ then $\underbrace{1, \alpha, \alpha^2, \dots \alpha^n}_{n+1} \in F($

and $\{1, \alpha, \dots \alpha^n\}$ is linearly dependent over F, Hence $\exists\ \beta_0, \beta_1, \dots \beta_n \in F$ (not all zero) w/ $\sum_{i=0}^{n} \beta_i \alpha^i = 0$. Then α is a root of $\sum_{i=0}^{n} \beta_i x^i$, hence α is algebraic ☒

Corrolary: $[E : F]$ finite $\Rightarrow$ E algebraic

Pf:

let $\alpha \in E$ then $[F(\alpha) : F] = \dfrac{[E : F]}{[E : F(\alpha)]} \leq [E : F] < \infty$

by previous thm, α is algebraic ☒

Notation: $\alpha_1, \dots \alpha_n \in E$.
$F(\alpha_1, \dots, \alpha_n)$ = smallest subfield of E containing F and $\{\alpha_1, \dots, \alpha_n\}$

Prop: $F(\alpha, \beta) = (F(\alpha))(\beta)$
Pf: easy, use definition

HW: let $\alpha, \beta \in E$, α, β algebraic. $F(\alpha,\beta) = (F(\alpha))(\beta)$

Pf: $[(F(\alpha))(\beta) : F]$

$= \underbrace{[(F(\alpha))(\beta) : F(\alpha)]}_{\text{Finite}} \cdot \underbrace{[F(\alpha) : F]}_{\text{Finite}}$

since α, β algebraic over F. So $[F(\alpha,\beta) : F] < \infty$, hence $F(\alpha,\beta)$ is algebraic $\Rightarrow$ α/β, $\alpha+\beta$, $\alpha\cdot\beta$, $\alpha-\beta$ all algebraic! ▨