Lecture 20

How to determine whether $p(x)$ is irreducible

eg 1 Over $\mathbb{R}$, a quadratic $p(x) = x^2 + bx + c$ is irred iff the discriminant $b^2 - 4c < 0$.

eg 2 Over $\mathbb{Q}$, use Eisenstein's criterion:

prop. Let R be an integral domain. Let P be a prime ideal.
Let $f(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1 x + c_0 \in R[x]$ $(n \geq 1)$
Suppose the coefficients $c_{n-1}, \dots, c_1, c_0$ are all elements of P and suppose $c_0 \notin P^2$.
Then $f(x)$ is irred in $R[x]$.

Pf. Suppose $f(x)$ were reducible, ie there are non constant polynomials $a(x), b(x)$ s.t. $f(x) = a(x)b(x)$ (then $n \geq 2$).
Reduce this mod P: $f(x) \equiv a(x)b(x) \bmod P \equiv x^n \bmod P$
ie. $\overline{a(x)b(x)} = x^n$ in $(R/P)[x]$.
$\Rightarrow$ $\overline{a(x)}, \overline{b(x)}$ must be of the form $\bar{a}_k x^k$, $\bar{b}_\ell x^\ell$
where $k, \ell \geq 1$ (and $\bar{a}_k, \bar{b}_\ell \in R/P$.), because R/P is ID..
$\Rightarrow \bar{a}_0, \bar{b}_0 = 0 \in R/P \Rightarrow a_0, b_0 \in P \Rightarrow a_0 b_0 \in P^2$. $\lightning$

∎

Over $\mathbb{Z}$ and $\mathbb{Q}$:

Cor Let p be a prime in $\mathbb{Z}$ and let

$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, with $n \geq 1$.

Suppose $p \mid a_i$ $\forall$ $0 \leq i \leq n-1$, and $p^2 \nmid a_0$.

Then $f(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

Note $\mathbb{Z}$ is a UFD. $f(x)$ irred in $\mathbb{Z}[x] \Rightarrow f(x)$ irred in $\mathrm{Frac}(\mathbb{Z})[x]$.

Examples

① $f(x) = x^4 + 10x + 5$. For $p = 5$, $f(x)$ satisfies Eisenstein's Criterion.

$\Rightarrow f$ is irred in $\mathbb{Q}[x]$.

② $f(x) = x^4 + 1$ Change of variables: $f(x+1) = (x+1)^4 + 1$

$g(x) = x^4 + 6x^3 + 4x^2 + 6x^2 + 2$ is irred iff $f(x)$ is irred.

And $g(x)$ is Eisenstein at $p = 2$.

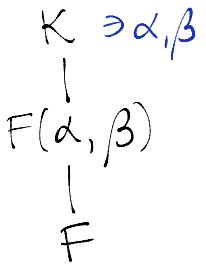
Recall Rational Root Theorem? eg. $x^3 - 3x - 1$.

defn. Let K be an extension of F.

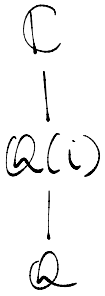
Let $\{\alpha_i\}_{i\in I} \subset K$ be a collection of elements in K.

The smallest subfield of K containing F and all $\{\alpha_i\}$, denoted $F(\{\alpha_i\}_{i\in I})$, is called the field generated by by $\{\alpha_i\}$ over F

eg.



eg.



defn. If K is generated by a single element α over F, ie. $K = F(\alpha)$, then K is a simple extension of F

and α is called a primitive element for the extension

analogous property:

"primitive" ~ primitive root of unity

eg. $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Let $\alpha = \sqrt{2}+\sqrt{3}$, and consider $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{2},\sqrt{3})$.

$\alpha^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6}$ $\rightsquigarrow$ have $\sqrt{6} \in \mathbb{Q}(\alpha)$

α^3 gives $\sqrt{6}(\sqrt{2}+\sqrt{3}) = \sqrt{2}\sqrt{3}\sqrt{2} + \sqrt{2}\sqrt{3}\sqrt{3}$

$= 2\sqrt{3} + 3\sqrt{2}$

actually $\left(\frac{\alpha^2-5}{2}\right)\cdot\alpha$

Subtract 2α or 3α to get $\sqrt{2}, \sqrt{3}$ individually in $\mathbb{Q}(\alpha)$.

$\cdots \Rightarrow \mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\alpha)$.

Relationship b/w roots of ireds + simple extensions:

thm. Let $p(x) \in F[x]$ be ired.

Suppose K is an extension of F containing a root α of $p(x)$

ie $p(\alpha)=0$.

* ie any field containing a root of $p(x)$ has a subfield $\cong F[x]/(p(x))$

Then $F(\alpha) \cong F[x]/(p(x))$.

Pf. The natural hom. $\varphi: F[x] \longrightarrow F(\alpha) \subseteq K$
$a(x) \longmapsto a(\alpha)$

Note that $p(x) \mapsto 0$ so $(p(x)) \subseteq \ker \varphi$.

$\Rightarrow \varphi$ factors through $F[x]/(p(x))$:

Now also restrict the codomain. We get a map

$$\psi: \underbrace{F[x]/(p(x))}_{\text{field.}} \longrightarrow F(\alpha).$$

$\psi(1) \neq 0 \Rightarrow \psi$ is injective. Also φ was surjective onto $F(\alpha)$,

so ψ is an isom. ∎

Rmk. So now we know

$$F[x]/(p(x)) \cong F(\alpha) = \{ a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid \alpha_i \in F \ \forall i \} \subseteq K.$$

$F[x]/(p(x))$: an abstract field, previously.

$F(\alpha)$: lives inside K

eg. $\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(-\sqrt{2})$

* There is a C_2-symmetry of this field extension...

Algebraic Extensions

defn. Let K, F be fields, where $F \subset K$.

① $\alpha \in K$ is *algebraic over F* if α is the root of some (nonzero) polynomial $f(x) \in F[x]$.

↳ If α is *not* algebraic, then we call it *transcendental*

eg. $\sqrt{2}$ is algebraic over $\mathbb{Q}$; π is not.

② The extension K/F is *algebraic* if every element $\alpha \in K$ is algebraic.

There is a "best choice" for $f(x) \in F[x]$ (as above) for $\alpha \in K$ algebraic over F:

prop. Let α be algebraic over F.

(a) Then there is a *unique* monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root.

(b) $f(x) \in F[x]$ has α as a root iff $m_{\alpha,F}(x) \mid f(x)$ in $F[x]$.

Pf.

(a) Let $g(x) \in F[x]$ be a polynomial of *minimal* degree having α as a root.

- multiply by a constant in F; WLOG, may assume $g(x)$ is monic.

Claim: $g(x)$ is irreducible

Suppose $g(x) = a(x)b(x)$, where $\deg a(x), \deg b(x) < \deg g(x)$.

Then $g(\alpha) = a(\alpha)\,b(\alpha)$; since F is an ID, it must be that $a(\alpha) = 0$ or $\beta(\alpha) = 0$, contradicting minimality of the deg of $g(x)$. //

(b) Now suppose $f(x) \in F[x]$ has α as a root.

Use the Euclidean Algorithm to write

$$f(x) = q(x)\cdot g(x) + r(x) \qquad \deg r(x) < \deg g(x).$$

($g(x)$: minimal degree as in (a))

$$f(\alpha) = q(\alpha)\cdot \cancel{g(\alpha)}^{\,0} + r(\alpha) = 0 \implies r(\alpha) = 0.$$

Contradicts minimality of $\deg g(x) = 0 \Rightarrow r(x) = 0$.

$$\Rightarrow f(x) = q(x)\cdot g(x).$$ ∎

Cor. If we have

$$\begin{array}{c} K \ni \alpha \\ | \\ L \\ | \\ F \end{array}$$

and α is algebraic over both L and F,

then $m_{\alpha,L}(x) \mid m_{\alpha,F}(x)$ in $L[x]$.

dfn. • $m_{\alpha,F}(x)$ is the minimal polynomial of α over F

↪ sometimes write $m_\alpha(x)$ if F elided

• $\deg m_{\alpha,F}(x)$ = the degree of α.

* Gröbner bases.

Eg. $f(x) = x^n - 2$ is irred by Eisenstein. Let α be a root.

$$\Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = n$$

Observations

① also the degree of the extension $F(\alpha)$ over F:

$F(\alpha) \cong F[x]/(m_\alpha(x))$.

② α is algebraic over F iff $[F(\alpha):F]$ is finite.

$\Rightarrow$ $F(\alpha) \cong F[x]/(m_\alpha(x))$ has basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

$\Leftarrow$ If $[F(\alpha):F] < \infty$, then

$\{1, \alpha, \ldots, \alpha^{n-1}, \alpha^n\}$ is linearly dependent,

so there exists a nonzero polynomial $(b_i \in F)$

$$p(x) = \sum_{i=0}^{n} b_i x^i$$

where $p(\alpha) = 0 \Rightarrow \alpha$ is alg over F.

③ So if K/F is finite, it must be algebraic.

↳ can prove that K must be $F(\underbrace{\alpha_1, \alpha_2, \ldots, \alpha_k}_{\text{finite \# of generators}})$

where $\deg \alpha_i < \infty \ \forall\ i$.

Eg. $p(x) = x^3 - 3x - 1$ Recall Rational root theorem?

Roots: