Abstract Algebra III

This lecture will be recorded. If you do not want your face in the recording, please turn off your camera. If you do not want your voice in the recording, please participate using the chat.

Let K/F a finite, separable extension

$[K:F] < \infty$ $\quad$ $\forall \alpha \in K$, $m_{\alpha,F}$ separable

distinct roots

By the Primitive Element Theorem

$\exists\, \alpha \in K$ with $K = F(\alpha)$

$$[K:F] = n = \deg m_{\alpha,F}$$

$= \#$ of distinct roots of $m_{\alpha,F}$

$x^2+1 \in \mathbb{Q}[x]$

no roots

$\rightarrow$ go to the splitting field

$(x-i)(x+i)$

no repeated factors

Aside: irred polynomial with repeated roots

$F = \mathbb{F}_3(t)$ field with elements of the form

$$\frac{p(t)}{q(t)}, \; p, q \in \mathbb{F}_3[t]$$

— inseparable

$f(x) = x^3 - t \in \mathbb{F}_3(t)[x]$ this does not have a root in $\mathbb{F}_3(t)$

$= (x - t^{1/3})^3 \in \mathbb{F}_3(t^{1/3})[x]$ $r = t^{1/3} \notin \mathbb{F}_3(t)$

repeated linear factor

irreducible

$K = F(\alpha)$ roots of $m_{\alpha,F}$ be $\{\alpha_1=\alpha, \alpha_2, \alpha_3 \dots \alpha_n\}$

$$
\begin{tikzcd}
 & L \ni \alpha_1, \alpha_2, \dots, \alpha_n \arrow[dd, dash] \\
F(\alpha)=K \ni \alpha=\alpha_1 \arrow[ur, dash] & \\
 & F \arrow[ul, dash]
\end{tikzcd}
$$

L splitting field of $m_{\alpha,F}$

maybe more roots but we don't know

Let $\sigma \in \mathrm{Aut}(K/F)$

Know that

$\sigma(\alpha) \in \{\alpha_1, \dots, \alpha_n\}$

because

$0 = m_{\alpha,F}(\alpha)$

$= \sigma(m_{\alpha,F}(\alpha)) = m_{\alpha,F}(\sigma(\alpha))$

Claim: If $\alpha_i \in K$ then $\exists\, \sigma \in \mathrm{Aut}(K/F)$ such that $\sigma(\alpha) = \alpha_i$

In this setting, σ is unique because $K = F(\alpha)$ so σ is determined by the value of $\sigma(\alpha)$,

$k \in K$ $\quad k = \dfrac{p(\alpha)}{q(\alpha)}$, $\quad \sigma(k) = \dfrac{p(\sigma(\alpha))}{q(\sigma(\alpha))}$

Recap
if $\sigma \in \mathrm{Aut}(K/F)$
$\sigma(\alpha) = \alpha_i$
some i

Note that if $\alpha_i \notin K$ then no $\sigma \in Aut(K/F)$ with $\sigma(\alpha) = \alpha_i$ because $\sigma : K \to K$.

So $\# Aut(K/F) \leq n = \deg m_{\alpha,F} = [K:F]$

this number is equal to the number of roots of $m_{\alpha,F}$ that are in K

3rd equivalent definition

K/F is Galois if $\# \mathrm{Aut}(K/F) = [K:F]$

K/F is Galois if it has the maximum possible number of automorphisms $/F$

if $K = F(\alpha)$, all the roots of $m_{\alpha,F}$ are in K.

Other defs:

K/F: finite, normal, separable ; K is a splitting field of a sep poly $/F$

splitting field of something

Theorem

If K/F is Galois, $f \in F[x]$ irreducible then either f has no root in K or f splits completely in K.

HW8 #1 $K = \mathbb{Q}(\sqrt{3+\sqrt{5}})$

$K = \mathbb{Q}(\alpha)$
$\alpha = \sqrt{3+\sqrt{5}}$

a) $K/\mathbb{Q}$ is Galois

Strategy: Find $m_{\alpha,\mathbb{Q}}$
Show all its roots are in K

Find $m_{\alpha,\mathbb{Q}}$

$$x = \sqrt{3+\sqrt{5}}$$ square both sides

$$x^2 = 3+\sqrt{5}$$ subtract 3

$$x^2 - 3 = \sqrt{5}$$ square both sides

$$(x^2-3)^2 = 5$$

$$x^4 - 6x^2 + 9 = 5$$ subtract 5

$$f(x) = x^4 - 6x^2 + 4 = 0$$

Let $f(x) = x^4 - 6x^2 + 4$, then $\underbrace{f\left(\sqrt{3+\sqrt{5}}\right) = 0}$

if this is not clear, check by plugging in

1 1 1 1
1 1 2
1 3
2 2

Note that
$f(x) \in \mathbb{Q}[x]$
f is monic

<u>If</u> f is irreducible, then $f = m_{\alpha, \mathbb{Q}}$

If f is <u>not</u> irreducible, then it either has a linear factor (i.e. a root in $\mathbb{Q}$) or it factors as 2 quadratic polynomials.

Aside: Checking if a poly is irreducible

0. Check if Eisenstein
1. Don't, leave it for the end, but do say "I assume it's irreducible, I'll come back to it if I can"

2. If you do, hard, basically only do degs 2, 3, 4 higher than that, more tricks

in degs 2, 3 enough check for linear factor
4 linear factor + 2 quadratics

0 $f(x) \in \mathbb{Z}[x]$ $\quad f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$

f is Eisenstein if $\quad p \mid a_i$ for $i = 0, \dots, n-1$

$\exists\, p$ prime $\quad p^2 \nmid a_0$

$p \nmid a_n = 1$

if f is Eisenstein, f is irreducible

Example $\quad f(x) = x^5 + 2x^4 + 6x^3 + 4x^2 + 2x + 10$

is irreducible

② $f(x) = x^4 - 6x^2 + 4$ not Eisenstein

$p=2$ $\quad 2 \mid 6$ but $4 \mid 4$

$p=3$ $\quad 3 \mid 6$ but $3 \nmid 4$

$(\pm 1)^4 - 6(\pm 1)^2 + 4 \neq 0$

$(\pm 2)^4 - 6(\pm 2)^2 + 4 \neq 0$

$(\pm 4)^4 - 6(\pm 4)^2 + 4 \neq 0$

linear factor/root in $\mathbb{Q}$: rational root theorem

if $\frac{r}{s} \in \mathbb{Q}$ is a root $r, s \in \mathbb{Z}$ $\quad s \mid a_n \quad r \mid a_0$

here $a_n = 1$ $\quad s \mid 1 \Rightarrow s = \pm 1$

$a_0 = 4$ $\quad r \mid 4 \Rightarrow r = \pm 1, \pm 2, \pm 4$

$\Bigg\} \frac{r}{s} = \pm 1, \pm 2, \pm 4$

try them

check for quadratic factors

can assume WLOG that $a, b, c, d \in \mathbb{Z}$

$$x^4 - 6x^2 + 4 = (x^2 + ax + b)(x^2 + cx + d)$$

$$= x^4 + cx^3 + dx^2 + ax^3 + acx^2 + adx + bx^2 + bcx + bd$$

$a(d-b) = 0$

$a = c = 0$ ✗

$d = b$

$\Rightarrow a + c = 0$

$d + \cancel{a}c^{0} + b = -6$

$ad + bc = 0$

$bd = 4$

$c = -a$

$b = \pm 1, \pm 2, \pm 4$

$d = \pm 4, \pm 2, \pm 1$

That's all for today!

Monday: lecture on HW9

Wednesday: #4 HW9

Friday: Quiz 8

If you want me to finish #1 HW8

Campuswire