Chris Wang
collab { nawaz riaz

Modern Algebra 2

HW 9

34/35

1) Assume that $5^{1/3} \in \mathbb{Q}(2^{1/3})$ and it satisfies
$$5^{1/3} = a + b2^{1/3} + c2^{2/3} \text{ for some } a,b,c \in \mathbb{Q}$$
Because $5^{1/3} \in \mathbb{Q}(2^{1/3})$, $5^{1/3} \in \mathbb{Q}(w, 2^{1/3})$. The Galois group is S_3 (as seen in class)

Consider $\mathbb{Q}(w) \subset \mathbb{Q}(w, 2^{1/3})$ where $[\mathbb{Q}(w, 2^{1/3}) : \mathbb{Q}(w)] = 3$. $w = e^{2\pi i/3}$

Thus the corresponding subgroup has order 3. The only subgroup of S_3 with order 3 is A_3.

$A_3 \cong \mathbb{Z}_3$ so it is cyclic.

The automorphisms send $2^{1/3}$ to $2^{1/3}$, $w2^{1/3}$, or $w^2 2^{1/3}$. ✓

Let $\sigma : 2^{1/3} \to w2^{1/3}$ correspond to the generator of A_3.

$$\sigma(5^{1/3}) = \sigma(a + b2^{1/3} + c2^{2/3})$$
$$= a + b\sigma(2^{1/3}) + c\sigma(2^{2/3})$$
$$= a + bw2^{1/3} + cw^2 2^{2/3}$$

σ must send $5^{1/3}$ to $5^{1/3}$, $w5^{1/3}$, or $w^2 5^{1/3}$ (which all satisfy $x^3 - 5$).

Case 1: $\sigma(5^{1/3}) = 5^{1/3}$

5

$$5^{1/3} = a + bw2^{1/3} + cw^2 2^{2/3}$$
$\Rightarrow$ $b = 0$ and $c = 0$ ✓

$\Rightarrow$ $a = 5^{1/3}$ $\Rightarrow$ $5^{1/3} \in \mathbb{Q}$

However $x^3 - 5$ (min polynomial of $5^{1/3}$) is irreducible in $\mathbb{Q}$ by the Eisenstein Criterion.

$\Rightarrow$ Contradiction.

Case 2: $\sigma(5^{1/3}) = w5^{1/3}$

$$w5^{1/3} = a + bw2^{1/3} + cw^2 2^{2/3}$$ ✓

$\Rightarrow$ $a = c = 0$

$\Rightarrow$ $w5^{1/3} = bw2^{1/3}$ $\Rightarrow$ $b = (5/2)^{1/3}$

$\Rightarrow$ $(5/2)^{1/3} \in \mathbb{Q}$

However $2x^3 - 5$ (min poly of $(5/2)^{1/3}$) is irreducible in $\mathbb{Q}$ by the Eisenstein Criterion

$\Rightarrow$ Contradiction ✓

Case 3: $\sigma(5^{1/3}) = w^2 5^{1/3}$

$$w^2 5^{1/3} = a + bw2^{1/3} + cw^2 2^{2/3}$$

$\Rightarrow$ $a = b = 0$

$\Rightarrow$ $w^2 5^{1/3} = cw^2 (4)^{1/3}$ $\Rightarrow$ $c = (5/4)^{1/3}$

$\Rightarrow$ $(5/4)^{1/3} \in \mathbb{Q}$

However $4x^3 - 5$ (min poly of $(5/4)^{1/3}$) is irreducible in $\mathbb{Q}$ by Eisenstein Criterion

$\Rightarrow$ Contradiction.

Therefore in all cases, a contradiction arises. Thus $5^{1/3} \notin \mathbb{Q}$ ∎

2) Let $\Omega = e^{2\pi i/p}$

The roots of $x^{p}-2$ are: $\{2^{1/p}, \Omega 2^{1/p}, \dots, \Omega^{p-1}2^{1/p}\}$

Ω solves $x^{p-1}+x^{p-2}+\dots+x+1 \rightarrow$ degree $p-1$

$2^{1/p}$ solves $x^{p}-2 \rightarrow$ degree p (splitting field of x^p-2)

Thus the size of the Galois Group of $\mathbb{Q}(\Omega, 2^{1/p})$ is $(p)(p-1)$ ✓

The group of matrices also has size $(p)(p-1)$ (by inspection)

Each element of the Galois group maps Ω to $\Omega, \Omega^2, \dots,$ or Ω^{p-1} and $2^{1/p}$ to $2^{1/p}, \Omega 2^{1/p}, \dots,$ or $\Omega^{p-1}2^{1/p}$

Let $\sigma_{a,b}: \Omega \mapsto \Omega^{a}$, $2^{1/3} \mapsto \Omega^{b}2^{1/3}$. and Let $\psi: (\sigma_{a,b}) \mapsto \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$

$$\psi(\sigma_{a_1b_1})\psi(\sigma_{a_2b_2}) = \begin{bmatrix} a_1 & b_1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1a_2 & a_1b_2+b_1 \\ 0 & 1 \end{bmatrix}$$ ✓

$\sigma_{a_1b_1}\sigma_{a_2b_2}: \Omega \mapsto \Omega^{a_2} \mapsto (\Omega^{a_2})^{a_1}$, $2^{1/3} \mapsto \Omega^{b_2}2^{1/3} \mapsto (\Omega^{b_2})^{a_1}\Omega^{b_1}2^{1/3}$ $\Rightarrow$ $\sigma_{a_1b_1}\sigma_{a_2b_2}: \Omega \mapsto \Omega^{a_1a_2}$, $2^{1/3} \mapsto \Omega^{a_1b_2+b_1}2^{1/3}$

$$\psi(\sigma_{a_1b_1}\sigma_{a_2b_2}) = \begin{bmatrix} a_1a_2 & a_1b_2+b_1 \\ 0 & 1 \end{bmatrix} \Rightarrow \psi \text{ is a homomorphism.}$$ ✓

Consider $\ker(\psi)$. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ = identity of group of matrices ✓

$\psi(\sigma_{ab}) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow a=1,\ b=0. \Rightarrow \sigma_{1,0}: \Omega \mapsto \Omega$, $2^{1/3} \mapsto 2^{1/3}$.

$\sigma_{1,0}$ is the identity element. Thus the kernal of ψ is trivial $\Rightarrow \psi$ is injective.

Because the size of the groups are the same and ψ is injective $\Rightarrow \psi$ is surjective.

$\Rightarrow \psi$ is an isomorphism ∎ ✓

5

3) The min polynomial of α is $f(x)$ because $f(x)$ is irreducible ✓

Thus $[K:\mathbb{Q}] = 4$ ✓ [Its corresponding subgroup has order 6. Only subgroup of S_4 w/ 6 elements is S_3] ✓

Any subfield $E \subset K$ would need to have $[K:E] = 2$

Beause of inclusion reversing, the corresponding subgroup would have order $2 \cdot 6 = 12$

The subgroup of S_4 with order 12 is A_4. ✓

Thus S_3 would need to be a subgroup of A_4.

This is not true

$\Rightarrow K$ has no proper subfield ∎ ✓

5

6

4) Because imaginary roots always come in pairs for real-valued polynomials, $f(x)$ either has 0 or 2 imaginary roots.

Assume that $f(x)$ has 2 imaginary roots. Let α be the real root.

$\alpha \notin \mathbb{Q}$ because otherwise, the Galois group would not be S_3 (one of the elements to be permuted would be left out)

Consider $\mathbb{Q}(\alpha)$ and let K be the splitting field of $f(x)$. $\mathbb{Z}_3$

$K \supset \mathbb{Q}(\alpha) \supset \mathbb{Q}$. Because α is real, $K \neq \mathbb{Q}(\alpha)$ because $\mathbb{Q}(\alpha)$ is missing the imaginary roots.

By Galois main theory, there exists a proper subgroup of $\mathbb{Z}_3$.

However there are no proper subgroups of $\mathbb{Z}_3$

$\therefore f(x)$ has no imaginary roots ∎

5) Min poly of $\sqrt{a}$ is $x^2 - a$. $[\mathbb{Q}(\sqrt{a}):\mathbb{Q}] = 2$

Min poly of $\sqrt{b}$ is $x^2 + b$. $[\mathbb{Q}(\sqrt{b}):\mathbb{Q}] = 2$

Case 1: WLOG $a | b$.

$\Rightarrow \sqrt{a} \mid \sqrt{b}$, Thus $\sqrt{b} \in \mathbb{Q}(\sqrt{a})$

Thus $K = \mathbb{Q}(\sqrt{a}) \Rightarrow [K:\mathbb{Q}] = 2$

$\mathrm{Aut}(K/\mathbb{Q})$ sends $\sqrt{a}$ to $\sqrt{a}$ or $-\sqrt{a} \Rightarrow |\mathrm{Aut}(K/\mathbb{Q})| = 2$

$|\mathrm{Aut}(K/\mathbb{Q})| = [K:\mathbb{Q}] \Rightarrow K/\mathbb{Q}$ is Galois. ✓

As stated before $\phi: K \to K$, $\sqrt{a} \mapsto \sqrt{a}$ and $\psi: K \to K$, $\sqrt{a} \mapsto -\sqrt{a}$ are the elements of $\mathrm{Gal}(K/\mathbb{Q})$.

$\psi^2 = \phi$ and ϕ is the identity $\Rightarrow \mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ ✓

Case 2: WLOG $a \nmid b$

Thus $[K:\mathbb{Q}] = [K:\mathbb{Q}(\sqrt{a})][\mathbb{Q}(\sqrt{a}):\mathbb{Q}] = 2 \cdot 2 = 4$

$\mathrm{Aut}(K/\mathbb{Q})$ sends $\sqrt{a}$ to $\sqrt{a}$ or $-\sqrt{a}$ and $\sqrt{b}$ to $\sqrt{b}$ or $-\sqrt{b}$.

There are 4 possibilities so $|\mathrm{Aut}(K/\mathbb{Q})| = 4$

$|\mathrm{Aut}(K/\mathbb{Q})| = [K:\mathbb{Q}] \Rightarrow K/\mathbb{Q}$ is Galois ✓

Let $\sigma: K \to K$, $\sqrt{a} \mapsto -\sqrt{a}$, $\sqrt{b} \mapsto \sqrt{b}$ and $\tau: K \to K$, $\sqrt{a} \mapsto \sqrt{a}$, $\sqrt{b} \mapsto -\sqrt{b}$. $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$

$\mathrm{Gal}(K/\mathbb{Q})$ has no element of order 4, so it is not cyclic.

The Klein-four group $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ is the only non-cyclic group of order 4. ✓

$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

For all cases, $K/\mathbb{Q}$ is Galois and $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ∎

5

$Gal(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0),(1,0),(0,1),(1,1)\}$

There are 3 different non-trivial subgroups $(\{(0,0),(1,0)\}$, $\{(0,0),(0,1)\}$, and $\{(0,0),(1,1)\}$ all of which are isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Take any one of these subgroups (let it be called A).

By the main Galois theorem, $\exists$ a subfield $E, \subset K$ that corresponds to A.

Because $|A|=2$, $|K:E|=2$. This means K/E is an extension of degree 2.

Then there exists an irreducible quadratic that creates this extension. Furthermore it must be of the form x^2-a where $a \in \mathbb{Q}$ and $\sqrt{a} \notin \mathbb{Q}$. Thus $E(\sqrt{a})=K$.

Next take one of the remaining subgroups (let it be called B). B combined with A creates $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

By the main Galois theorem, $[E:\mathbb{Q}] = [\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} : A] = 2$.

Again an irreducible quadratic with the form x^2-b is required to create this extension.

Thus $\mathbb{Q}(\sqrt{b}) = E$

$\Rightarrow K = \mathbb{Q}(\sqrt{a},\sqrt{b})$ ∎

✓

5

6) ζ_p satisfies $x^{p-1}+x^{p-2}+\dots+x+1$ (its min polynomial).

Thus $\mathbb{Q}(\zeta_p)$ is an extension of order $(p-1)$.

Let $K=\mathbb{Q}(\zeta_p)$, Consider $Aut(K/\mathbb{Q})$.

Its elements send ζ_p to $\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$.

Let $\sigma: \zeta_p \mapsto \zeta_p^2$. By composing σ, we can get every element in $Aut(K/\mathbb{Q})$

Furthermore $\sigma^{p-1}: \zeta_p \mapsto \zeta_p^{2^{(p-1)}} = \zeta_p$ $(2^{p-1} \equiv 1 \mod p)$

Thus $Aut(K/\mathbb{Q}) = \langle\sigma\rangle$ (a cyclic group of order $p-1$) ✓

Consider $\tau: \zeta_p \mapsto \zeta_p^4$. $\tau^{(p-1)/2}: \zeta_p \mapsto \zeta_p^{4^{(p-1)/2}} = \zeta_p^{2^{(p-1)}} = \zeta_p$

Thus $\langle\tau\rangle$ is a cyclic group of order $\frac{p-1}{2}$ (unique) and a subgroup of $\langle\sigma\rangle$.

Thus by the main Galois theorem, there is a unique corresponding quadratic extension ∎

✓

7) i satisfies x^2+1 (the min polynomial)

$2^{1/4}$ satisfies x^4-2 (the ~~min~~ polynomial)

Thus $[K:\mathbb{Q}]=8$

$Aut(K/\mathbb{Q})$ has elements that are automorphisms that send $2^{1/4}$ to $2^{1/4}, i2^{1/4}, -2^{1/4}, -i2^{1/4}$

i to i, or $-i$

Thus by counting $|Aut(K/\mathbb{Q})|=8$. ✓

Thus $K/\mathbb{Q}$ is Galois. ✓

4

Let $x: 2^{1/4} \mapsto 2^{1/4}$ and $y: 2^{1/4} \mapsto i2^{1/4}$
$\quad i \mapsto -i \qquad\qquad\qquad i \mapsto i$

Note that $x^2=1$, $y^4=1$, and $xy=y^3x$ work?

These are exactly the multiplication rules for D_4.

$|Gal(K/\mathbb{Q})| = |D_4| = 8$. ✓

Thus $Gal(K/\mathbb{Q}) \cong D_4$ ∎