algebra

$\frac{30}{30}$

MARSHALL BALL
mmb2249

① find the Galois gps of

ⓐ (x^3-3x^2+1) this and the following amounts to finding the discriminant and det. if it is square in $\mathbb{Q}$.
& irred. b/c irred. in $\mathbb{F}_2$.

$$(x+1)^3-3(x+1)^2+1 = x^3+\cancel{3x^2}+\cancel{3x}+\cancel{1}-\cancel{3x^2}-\cancel{6x}^{3}-\cancel{1}+1$$
$$= x^3-3x+1 \rightsquigarrow \Delta = -4(-3)^3-27(1)^2$$
$$= 27(4-1) = 81 = 9^2 \Rightarrow Gal = A_3$$

ⓑ $(x^3+x^2-2x+1) \leftarrow$ irred. b/c irred. in $\mathbb{F}_2$.

$$\rightsquigarrow (x-\tfrac{1}{3})^3+(x-1/3)^2-2(x-1/3)+1$$

$$-\tfrac{1}{27}+\tfrac{3}{27}+\tfrac{18}{27}+\tfrac{27}{27}=\tfrac{47}{27}$$

$$= x^3-x^2+\frac{x}{3}-1/27+x^2-\tfrac{2}{3}x+1/9-2x+2/3+1$$
$$= x^3-7/3\,x+\tfrac{47}{27} \rightsquigarrow \Delta = -4(-7/3)^3-27(47/27)^2$$
$$= \tfrac{1}{27}(4\cdot 7^3-47^2) = -\frac{837}{27} = -31 \text{ not a square}$$

and prime! <0

$\Downarrow$

$Gal = S_3$!

② let $\mathbb{Q}\subset K$ be the splitting field of x^3-3x+1. show that $Gal(K/\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$ but $K \neq \mathbb{Q}(\alpha)$ for any $\alpha\in K$ st $\alpha^3\in\mathbb{Q}$.

$\circledast$ irred b/c by Gauss' lemma any linear factor is also integral. $\Rightarrow$ poss. roots: $\pm 1 \leftarrow$ must divide 1 in $\mathbb{Z}$ (neither work) no linear factors in cubic $\Rightarrow$ irred.

$$\Delta(x^3-3x+1) = 81 \quad (\text{as in ⓐ}) \Rightarrow Gal(K/\mathbb{Q}) = \underset{\langle(123)\rangle}{\overset{\shortparallel}{A_3}} \cong \mathbb{Z}/3\mathbb{Z}.$$

let $\alpha\in K$ st $\alpha^3\in\mathbb{Q} \Rightarrow \alpha$ sat. $x^3-\alpha^3$. $\Rightarrow \alpha\zeta_3$ and $\alpha\zeta_3^2$ sat. $x^3-\alpha^3$.

recall $Gal(K/\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z} \Rightarrow K\subseteq\mathbb{R}$ ($\Rightarrow \alpha\in\mathbb{R}$.)

$x^3-\alpha^3 \in \mathbb{Q}[x]$ fixed under $Gal(K/\mathbb{Q})$: but $\alpha\zeta_3^2, \alpha\zeta_3 \notin \mathbb{R} \Rightarrow \alpha\zeta_3, \alpha\zeta_3^2 \notin K$

$\Rightarrow \alpha$ fixed under $\forall$ $Gal(K/\mathbb{Q}) \Rightarrow \alpha\in\mathbb{Q} \Rightarrow \mathbb{Q}(\alpha)=\mathbb{Q}$.

③ let $p(x) = x^3-2x+2$. use symm. functions to find the monic poly whose roots are squares of the roots of $p(x)$.

in some $K\supset\mathbb{Q}$

$$x^3-2x+2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) = x^3-\underbrace{(\alpha_1+\alpha_2+\alpha_3)}_{s_1=0}x^2+\overbrace{(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_1\alpha_3)}^{s_2=-2}x \underbrace{-\alpha_1\alpha_2\alpha_3}$$

$$(x-\alpha_1^2)(x-\alpha_2^2)(x-\alpha_3^2) = x^3-\underbrace{(\alpha_1^2+\alpha_2^2+\alpha_3^2)}_{a}x^2+\underbrace{(\alpha_1^2\alpha_2^2+\alpha_2^2\alpha_3^2+\alpha_1^2\alpha_3^2)}_{b}x-\underbrace{\alpha_1^2\alpha_2^2\alpha_3^2}_{c=s_3^2=4} \quad (-2=s_3)$$

$$\text{note: } s_1^2 = \overbrace{\alpha_1^2+\alpha_2^2+\alpha_3^2}^{a}+2s_2 \Rightarrow a = s_1^2-2s_2 = 4$$

$$s_2^2 = \alpha_1^2\alpha_2^2+\alpha_1\alpha_2^2\alpha_3+\alpha_1^2\alpha_2\alpha_3+\alpha_1\alpha_2^2\alpha_3+\alpha_2^2\alpha_3^2+\alpha_1\alpha_2\alpha_3^2+\alpha_1^2\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_3^2+\alpha_1^2\alpha_3^2$$
$$= b+2s_3s_1 \Rightarrow b = s_2^2-2s_3s_1 = 4 \Rightarrow \boxed{x^3-4x^2+4x-4}$$

(4) Let $p(x) \in \mathbb{Q}[x]$ be an irred. monic quartic poly w/ roots $\alpha_1 \cdots \alpha_4$. Set

$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$, $\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$.

Show that $r(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3)$ has coeff in $\mathbb{Q}$.

$p(x)$ irred. $\Rightarrow K = \mathbb{Q}(\alpha_1 \cdots \alpha_4)$ is Galois (b/c $p(x)$ is aut. separable in char 0). (and moreover no $\alpha_i \in \mathbb{Q}$.)

and moreover, $Gal(K/\mathbb{Q}) \subseteq S_4$. $r(x)$ obviously factors in K. ✓

5

so to show $r(x) \in \mathbb{Q}[x]$, sts $\forall \sigma \in Gal(K/\mathbb{Q})$, σ permutes $\{\beta_1, \beta_2, \beta_3\}$. (*)

transpositions (of roots) generate S_4 so sts an arb. τ_{ij} transposition permutes

eg: $\tau_{12}(\beta_1) = \beta_1$, $\underset{\alpha_2\alpha_3+\alpha_1\alpha_4}{\tau_{12}(\beta_2) = \beta_3}$, $\tau_{12}(\beta_3) = \underset{\alpha_2\alpha_4+\alpha_1\alpha_3}{\beta_2}$ ✓

in general for τ_{ij} if $\beta_m = \alpha_i\alpha_j + \alpha_\ell\alpha_k$ then $\tau_{ij}(\beta_m) = \beta_m$

ow if $\beta_n = \alpha_i\alpha_\ell + \alpha_j\alpha_k$ then $\tau_{ij}(\beta_n) = \alpha_j\alpha_\ell + \alpha_i\alpha_k = \beta_r$ □

(*) why is this true b/c coeff. of $r(x)$ are eltry. symmetric functions in $\beta_1, \beta_2, \beta_3$ ✓

(5) Let $p(x) \in \mathbb{Q}[x]$ be an irred. monic quartic poly whose resolvent cubic $r(x) \in \mathbb{Q}[x]$ is irred. Show that the Galois group of $p(x)$ is either A_4 or S_4. Exhibit quartic poly with Galois gps A_4 + S_4.

first note: if K is the galois extension of some $f(x) \in \mathbb{Q}(x)$ w/ deg $f = n$ and $g(x) \overset{\in \mathbb{Q}[x]}{=} (x-\alpha_1)\cdots(x-\alpha_\ell)$ in K and suppose $\exists \alpha_i$ st $\mathcal{O}_{\alpha_i}$, the orbit of α_i under G (the gal. group of K), is $\{\alpha_{i_1}, \cdots \alpha_{i_k}\}$ where $k \underset{(\neq)}{\le} \ell$ (note: $k \mid \ell$). then, $g_0(x) = (x-\alpha_{i_1})\cdots(x-\alpha_{i_k})$

is fixed under $\forall G$ so $g_0(x) \in \mathbb{Q}[x]$ and $g_0(x) \mid g(x) \Rightarrow g(x)$ is reducible. so, in conclusion we get the contrapositive:

$f(x) \overset{\in \mathbb{Q}(x)}{}$ irred and f splits in K, galois $/\mathbb{Q}$, w/ galois gp G. $\Rightarrow \forall \alpha$ st $f(\alpha) = 0$, ($\mathcal{O}_\alpha = \{\beta \mid f(\beta) = 0\}$. by orbit-stabilizer thm: $|G_\alpha||\mathcal{O}_\alpha| = |G|$)

$\Rightarrow \deg(f) \mid |G|$ ✓ (obviously, for other reasons as well)

so, given $p(x)$, w/ $r(x)$ both irred, G, the galois group of G must be transitive on roots ... $\Rightarrow G \in \{S_4, A_4, D_4, C_4, \dots\}$ but $3 \mid |G| \Rightarrow G \in \{S_4, A_4\}$ ✓

now finding poly's quick calculation (done on scratch) show that the only V_4 = klein-4 (group of double transpositions) fixes $\beta_1, \beta_2, \beta_3$ and this sg is normal.

$S_4/V_4 = S_3$ and $A_4/V_4 = A_3$ so we have some idea of what resolvents should look like.

I've seen this last sem.

unfortunately solving for α's does not seem easy...

suppose we have $p(x) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4$ w/ roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$

$r(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3) = x^3 - s_1'x^2 + s_2'x - s_3'$ where primes are in terms of β's.

wolfram alpha $\leadsto$ $r(x) = x^3 - s_2 x^2 + (s_1s_3 - 4s_4)x + (4s_4s_2 - s_3^2 - s_4s_1^2)$

$\underset{-s_3'}{\shortparallel}$

<u>to get S_4:</u> lets force eisenstein on $p(x)$ st $r(x)$ has odd s_2', s_3' $\hookrightarrow$ irred in $\mathbb{F}_2[x]$ (and an easy discriminant)

take $p_{S_4}(x) = x^4 - 3x^3 + 3x + 6$ $\leftarrow$ irred by eisenstein

$\Rightarrow r_{S_4}(x) = x^3 + (-9 - 4\cdot 6)x + (-9 - 6\cdot 9) = x^3 - 33x - 63$. $\leftarrow$ irred. by $\mathbb{F}_2$

$\Delta_p = \Delta_r = -4(33)^3 - 27(63)^2 < 0 \Rightarrow \sqrt{\Delta_p} \notin \mathbb{Q}$ ✓

notice that $\beta_1 - \beta_2 = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)$ and similarly $(\beta_2 - \beta_3), (\beta_1 - \beta_3)$

<u>to get A_4:</u>

Lets start w/ a known cubic w/ Galois gp A_3: $x^3 - 3x^2 + 1$ (from (1)).

5

and try to derive a quartic via
$$\begin{cases} s_1' = 3 = -s_2 \Rightarrow s_2 = -3 \\ s_2' = 0 = s_1s_3 - 4s_4 \Rightarrow s_1s_3 = -4s_4 \\ s_3' = -1 = -4s_4s_2 + s_3^2 + s_4s_1^2 \end{cases}$$

$\Rightarrow -1 = 12s_4 + s_4s_1^2 + s_3^2 \Rightarrow s_4 < 0 \Rightarrow s_1, s_3$ have same sign
$= s_4(12 + s_1^2) + s_3^2$

$\leftarrow$ sadly this keeps giving me equations in $\mathbb{Q}[x,y,z]$ to ~~find~~ see if reducible

brute force { I wrote a simple java program to look for integer solutions, but I found nothing at least less than 1 billion...

(*) $\leadsto$ trying equations from Dummit and Foote exercises...

found one we near.

$x^4 + 8x + 12$ ✓ $\leadsto$ has no roots by Gauss, $(\beta x - \alpha) \in \mathbb{Z}$ would be $\Rightarrow \alpha \mid 12$
1, 2, 3, 4, 6 don't work. $\Rightarrow (\beta = \pm 1)$

the resolvent cubic is $x^3 - 48x - 64$. $\leadsto \Delta_r = +4\cdot 48^3 - 27(64)^2 = 331776$
Δ_p
$= 576^2$!

So $\sqrt{\Delta} \in \mathbb{Q} \Rightarrow$ only even perms ✓

So sts $x^3 - 48 - 64$ is irred. ($x^4 + 8x + 12$ has no roots
$\Rightarrow$ if it splits in $\mathbb{Q}$ it does so into quad factors, but $3 \nmid 2, 4$ so we can infer that it is irred).

if $x^3 - 48x - 64$ then red. then by Gauss it has lin. factor in $\mathbb{Z}[x]$

$\therefore$ galois gp is A_4

⑥ Show that D_2, C_4, D_8, A_4, S_4 can arise as Galois gps of quartics.

Infact, we have seen and proved these all on previous hws

$D_2 \leftarrow (x^2-2)(x^2-3)$ ✓ (see 9.5)

$C_4 \leftarrow x^4+x^3+x^2+x+1$ ✓ (class generator: $\langle \zeta_5 \to \zeta_5^g \rangle$ where g gen. $\mathbb{F}_5^\times$)

$D_8 \leftarrow x^4-2$ ✓ (see 9.7)

$S_4 \longleftarrow x^4-3x^3+3x+6$ (see above)

$A_4 \longleftarrow x^4+8x+12$ (again above).

(A) x^3-3x-1 has $\Delta = 9^2$! and is irred. b/c again by Gauss, ± 1 are not roots.

$\Rightarrow \begin{cases} s_2' = -3 = s_1 s_3 - 4 s_4 \\ s_3' = 1 = s_3^2 + s_4 s_1^2 \end{cases}$. take $s_1 = 0 \Rightarrow s_4 = 3/4$
$\Rightarrow s_3 = \pm 1$

giving us $x^4+x+3/4$. again, irred. resolvent $\Rightarrow$ irred. if no roots (in this quartic case)

but again by Gauss: $4x^4+4x+3$ can only have the following roots: $\pm 1, \pm 1/2, \pm 1/4, \pm 3/2, \pm 3/4$. none of which are solutions!

$((p/q)$ st $p|3, q|4)$
$\leftrightarrow (qx-p) \in \mathbb{Z}$.

$\therefore$ Galois gp is A_4