Assignment-IIA

Galois Theory

Trishan Mondal

(1) Let $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ denote the automorphism of the cyclotomic field of nth roots of unity which maps ζ_n to ζ_n^a, where $(a,n)=1$, ζ_n being a primitive nth root of unity. Show that $\sigma_a(\zeta)=\zeta^a$ for every nth root of unity.

Let, μ_n be the set of all n^{th} roots of unity. μ_n is a multiplicative Subgroup of the field $\mathbb{Q}(\zeta_n)$. Thus μ_n is cyclic (as it is finite). Since, ζ_n is primitive n^{th} root of unity μ_n should be generated by ζ_n. So any n^{th} root of unity ζ can be written as,

$$\zeta = \zeta_n^k \quad \text{(for Suitable choice of } k)$$

Thus, $\sigma_a(\zeta) = \sigma_a(\zeta_n^k) = \sigma_a(\zeta_n)^k = \zeta_n^{ak} = (\zeta_n^k)^a = \zeta^a$ ■

(2) Let p be a prime and ϵ_i, $1 \le i \le p-1$ denote the primitive pth roots of unity. Let $p_n = \sum_{i=1}^{p-1} \epsilon_i^n$. Prove that $p_n = -1$ if p does not divide n, and that $p_n = p-1$ if p divides n.

We know that if ζ is a primitive p^{th} root of unity, ζ^a is also primitive p^{th} root of unity iff $\gcd(a,p)=1$. Since, p is a prime We can say ζ^a is primitive p-th root of unity for $1 \le a \le p-1$.

WLOG, $\epsilon_i = \zeta^i$ for $1 \le i \le p-1$. We must have,

$$\sum_{i=1}^{p-1} \epsilon_i^n = \sum_{i=1}^{p-1} \zeta^{in} = \sum_{i=1}^{p-1} (\zeta^n)^i$$

$$= \Phi_p(\zeta^n) - 1$$

(Where $\Phi_p(x) = x^{p-1} + \cdots + 1$ Cyclotomic polynomial)

$$= \begin{cases} \Phi_p(1) - 1 & \text{if } p \mid n \\ \Phi_p(\zeta^k) - 1 & \text{if } p \nmid n \end{cases}$$

$$= \begin{cases} p-1 & \text{if } p \mid n \\ -1 & \text{if } p \nmid n \end{cases}$$

(ζ^n will be a primitive p-th root and hence $\Phi_p(\zeta^n) = 0$)

(3) Prove that the primitive n-th roots of unity form a basis over $\mathbb{Q}$ for the cyclotomic field of n-th roots of unity iff n is squarefree (ie. n is not divisible by the square of any prime).

($\Rightarrow$) Let, Primitive n^{th} roots forms a basis of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. (Where ζ is n-th primitive root of unity). Let p be a prime with $p^2 \mid n$. Let $k = n/p$. $\omega = \zeta^k$ Satisfy $\omega^K = 1$ and obviously $\omega \neq 1$. If $\Phi_p(x)$ is Cyclotomic polynomial for p,

$$\Phi_p(\omega) = 0$$

$$\Rightarrow \zeta\, \Phi_p(\omega) = 0$$

$$\Rightarrow \zeta(1 + \zeta^k + \cdots + \zeta^{(p-1)k}) = 0$$

Note that, $\gcd(\frac{n}{p}j+1, n) = 1$ for $0 \leq j \leq p-1$. Thus each terms in the above Sum is primitive roots of unity (n^{th}). Thus the Set of primitive elements is not linearly idependent. But by assumption it is not possible. So $\nexists$ prime p such th $p^2 \mid n$. So, n is Squarefree.

($\Leftarrow$) Let, n is Square-free. We Can write $n = p_1 p_2 \cdots p_r$. Let $n_i = p_1 \cdots p_i$. We will induct on i to Show n_i^{th}- primitive roots of unity forms a basis for the extension $\mathbb{Q}(\zeta_{n_i})|\mathbb{Q}$. For $i=1$, $n_1 = p_1$. Note that the extension $\mathbb{Q}(\zeta_{p_1})|_{\mathbb{Q}}$ is Simple so, $\{1, \zeta_{p_1}, \ldots, \zeta_{p_1}^{p_1-2}\}$ is basis of $\mathbb{Q}(\zeta_{p_1})|_{\mathbb{Q}}$. Since, $1 = -(\zeta_{p_1} + \cdots + \zeta_{p_1}^{p_1-1})$, we Can say the Set: $\{\zeta_{p_1}, \ldots, \zeta_{p_1}^{p_1-1}\}$ is basis of $\mathbb{Q}(\zeta_{p_1})|_{\mathbb{Q}}$.

Suppose we have proved it for the case $i=k$, the n_k^{th} primitive roots of unity forms a basis for the extension $\mathbb{Q}(\zeta_{n_k})|\mathbb{Q}$. We know, $n_{k+1} = n_k p_{k+1}$ Since $\gcd(n_k, p_{k+1}) = 1$, $\mathbb{Q}(\zeta_{n_k}, \zeta_{p_{k+1}}) = \mathbb{Q}(\zeta_{n_{k+1}})$ (This was proved in class).

We also know $B_{n_k} = \{ \zeta_{n_k}^{a} : \gcd(a, n_k) = 1 \}$ and $B_{p_{k+1}} = \{ \zeta_{p_{k+1}}^{a} : 1 \gcd(a, p_{k+1}) = 1 \}$ are basis of the extensions $\mathbb{Q}(\zeta_{n_k}) | \mathbb{Q}$ and $\mathbb{Q}(\zeta_{p_{k+1}}) | \mathbb{Q}$ respectively. We will use the following theorem to conclude $\{ \zeta_{n_k}^{i} \zeta_{p_{k+1}}^{j} : \gcd(i, n_k) = \gcd(j, p_{k+1}) = 1 \}$ is basis of $\mathbb{Q}(\zeta_{n_{k+1}}) | \mathbb{Q}$

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_{n_k}, \zeta_{p_{k+1}}) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dashed, no head] & \\
\mathbb{Q}(\zeta_{n_k}) \arrow[dr, dash] & & \mathbb{Q}(\zeta_{p_{k+1}}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Theorem: Let, L and K are finite galois extension over F. Let, $\{k_i\}$ be the basis of $K|_F$ and $\{l_j\}$ is basis of $L|_F$. If $L \cap K = F$ Then $LK|_F$ has basis $\{k_i l_j\}$.

With the above setup I claim that,

Claim — $\mathbb{Q}(\zeta_{n_k}) \cap \mathbb{Q}(\zeta_{p_{k+1}}) = \mathbb{Q}$

Note that,

$$[\mathbb{Q}(\zeta_{n_k p_{k+1}}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{n_k}, \zeta_{p_{k+1}}) : \mathbb{Q}]$$
$$= [\mathbb{Q}(\zeta_{n_k}, \zeta_{p_{k+1}}) : \mathbb{Q}(\zeta_{p_{k+1}})] [\mathbb{Q}(\zeta_{p_{k+1}}) : \mathbb{Q}]$$
$$\Rightarrow [\mathbb{Q}(\zeta_{n_k}, \zeta_{p_{k+1}}) : \mathbb{Q}(\zeta_{p_{k+1}})] = \phi(n_k p_{k+1}) / \phi(p_{k+1}) = \phi(n_k) \text{ [as gcd is 1]}$$

If $\mathbb{Q}(\zeta_{n_k}) \cap \mathbb{Q}(\zeta_{p_{k+1}}) \neq \mathbb{Q}$ we must have,

$$\underbrace{[\mathbb{Q}(\zeta_{n_k}) : \mathbb{Q}]}_{= \phi(n_k)} = [\mathbb{Q}(\zeta_{n_k}) : \mathbb{Q}(\zeta_{n_k}) \cap \mathbb{Q}(\zeta_{p_{k+1}})] [\mathbb{Q}(\zeta_{n_k}) \cap \mathbb{Q}(\zeta_{p_{k+1}}) : \mathbb{Q}]$$
$$\Rightarrow [\mathbb{Q}(\zeta_{n_k}) : \mathbb{Q}(\zeta_{n_k}) \cap \mathbb{Q}(\zeta_{p_{k+1}})] < \phi(n_k)$$

Also, $\phi(n_k) = [\mathbb{Q}(\zeta_{n_k}, \zeta_{p_{k+1}}) : \mathbb{Q}(\zeta_{p_{k+1}})] \leq [\mathbb{Q}(\zeta_{n_k}) : \mathbb{Q}(\zeta_{n_k}) \cap \mathbb{Q}(\zeta_{p_{k+1}})]$

Which is a contradiction. Done

By the above theorem we can say $\{ \zeta_{n_k}^{i} \zeta_{p_{k+1}}^{j} : \gcd(i, n_k) = \gcd(j, p_{k+1}) = 1 \}$ is basis of $\mathbb{Q}(\zeta_{n_{k+1}}) | \mathbb{Q}$. Since $\zeta_{n_k}^{i}$ and $\zeta_{p_{k+1}}^{j}$ are primive roots of respective order. $\zeta_{n_k}^{i} \zeta_{p_{k+1}}^{j}$ is n_{k+1}-th primitve root. The above

Set has $\phi(n_k)\phi(P_{k+1}) = \phi(n_{k+1})$ Cardinality and no two elements are are equal. So, the set is equal to the set of all n_{k+1}-th primitive roots of 1. Thus our induction step is done and hence for $n = P_1 \cdots P_r$ the set of all primitve n-th roots forms a basis for the extension $\mathbb{Q}(\zeta_n)|\mathbb{Q}$. ∎

> (4) Find the Galois groups (over $\mathbb{Q}$) of:
> (i) $x^4 + 2x^2 + 5$
> (ii) $x^4 + 3x^3 - 3x - 2$
> (iii) $x^4 + 8x + 12$.

(i) $x^4 + 2x^2 + 5 = f(x)$. Roots of $f(x)$ are $\pm\sqrt{-1 \pm 2i}$. Thus, $\mathbb{Q}(\sqrt{-1+2i}, \sqrt{-1-2i})$ is splitting field of $f(x)$. Note that $\sqrt{-1-2i} \in \mathbb{Q}(\sqrt{-1+2i}, \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{-1+2i}, \sqrt{-1-2i}) \Rightarrow \mathbb{Q}(\sqrt{-1+2i}, \sqrt{-1-2i}) = \mathbb{Q}(\sqrt{5}, \sqrt{-1+2i})$

Let, $\alpha = \sqrt{-1+2i}$. The polynomial $f(x)$ is irreducible and it is satisfied by α. Thus $f(x)$ is minimal polynomial of α over $\mathbb{Q}$. So the extension $\mathbb{Q}(\alpha)|\mathbb{Q}$ has degree 4. Also note that $\sqrt{5} \notin \mathbb{Q}(\alpha)$ so, $\mathbb{Q}(\alpha, 2)|\mathbb{Q}$ has degree 8. Thus $|Gal(f)| = 8$. We also know $Gal(f) \hookrightarrow S_4$. The only order 8 subgroup of S_4 is $\simeq D_8$ (Fact from group theory)

So $Gal(f) \simeq D_8$.

(ii) $x^4 + 3x^3 - 3x - 2 = f(x)$, This polynomial don't have any root over $\mathbb{Q}$ by rational root theorem. By checking the case of quadratic factor we see, $f(x)$ is irreducible over $\mathbb{Q}$. In order to find the $Gal(f)$, we need to find the resolvent cubic

$$h(x) = x^3 + \frac{27}{4}x^2 + \frac{275}{32}x + \frac{9}{64}$$

$$= \frac{1}{64}\underbrace{(64x^3 + 432x^2 + 550x + 9)}_{\hookrightarrow \text{ call this } g(x)}$$

$$g(x) \pmod 5 = -x^3 + 2x^2 - 1 = -\underbrace{(x^3 - 2x + 1)}_{\hookrightarrow \text{ no root in } \mathbb{Z}/5\mathbb{Z}}$$

$\therefore$ $g(x)$ is irreducible over $\mathbb{Q}$, hence $h(x)$ is. Thus $12 \mid Gal(f) \Rightarrow Gal(f) = A_4$ or S_4

Now the discriminant of $f(x)$ = discriminant of $h(x) = -20183$, not a square in $\mathbb{Q} \Rightarrow \mathrm{Gal}(f) \nsubseteq A_4 \Rightarrow \mathrm{Gal}(f) = S_4$.

(iii) $x^4+8x+12 = f(x)$, This polynomial don't have any root over $\mathbb{Q}$ by rational root theorem. This polynomial is irreducible mod 5. Thus $f(x)$ is irreducible over $\mathbb{Q}$. The resolvent cubic of this polynomial is,

$$h(x) = x^3 - 48x + 64$$

This polynomial is $\bar{h}(x) = x^3 + 2x - 1$ mod 5. This do not have root modulo 5. Thus $h(x)$ is irreducible in $\mathbb{Q}$. So, $12 \mid \mathrm{Gal}(f) \Rightarrow \mathrm{Gal}(f) \cong A_4$ or S_4. The discriminant of $f(x)$ is 576^2. So, $\mathrm{Gal}(f) \cong A_4$. ■

(5) Prove that every finite group occurs as the Galois group of a field extension of the form $F(x_1, x_2, \ldots, x_n)/K$.

Every finite group G is a sub-group of S_n for some n. Let, F be a field then $^{*}F(x_1,\ldots,x_n) \big| F(s_1,\ldots,s_n)$ is a galois extension with Galois group S_n. (This was proved in class). Let $K = \mathcal{F}(G)$, fixed field of the subgroup $G \leq S_n \cong \mathrm{Gal}(F(x_1,\ldots,x_n) \mid F(s_1,\ldots,s_n))$. By Galois Correspondance theorem $\mathrm{Gal}(F(x_1,\ldots,x_n) \mid K) = G$. ■

* $s_1,\ldots,s_n$ are Symmetric polynomials of $x_1,\ldots,x_n$: $s_1 = \sum_i x_i$, $s_2 = \sum_{i<j} x_i x_j, \ldots$ $s_n = x_1 \cdots x_n$

(6) Prove that the polynomial $x^4 - px^2 + q \in \mathbb{Q}[x]$ is irreducible for any distinct odd primes p and q and has Galois group D_8.

Let, $f(x) = x^4 - px^2 + q$. This polynomial has roots $\pm\alpha, \pm\beta$ where,

$$\alpha = \sqrt{\frac{p+\sqrt{p^2-4q}}{2}}, \quad \beta = \sqrt{\frac{p-\sqrt{p^2-4q}}{2}}$$

The polynomial don't have any linear factor as $^{*}f(q) \neq 0$, $f(-q) \neq 0$. By rational root theorem $f(x)$ don't have any linear factor.

* p and q are prime

$f(x)$ can have two quadratic factor only following factorisation is possible,

$$(x^2-\alpha^2)(x^2-\beta^2),\ (x^2-(\alpha-\beta)x-\alpha\beta)(x^2+(\alpha-\beta)x-\alpha\beta),\ (x^2-(\alpha+\beta)x+\alpha\beta)(x^2+(\alpha+\beta)x+\alpha\beta)$$

In the first case α^2 and $\beta^2 \in \mathbb{Q}$.

This means $\sqrt{p^2-4q} \in \mathbb{Q} \Rightarrow \sqrt{p^2-4q} \in \mathbb{N} \Rightarrow p^2-4q = z^2$, for some $z \in \mathbb{N}$.

But then, $p^2-z^2=4q \Rightarrow (p+z)(p-z)=2^2 \cdot q$, look at the following cases,

$p+z$	$p-z$	p	z	
q	2^2	$\frac{q+4}{2}$	—	$\rightarrow$ Not possible
$2q$	2	$q-1$	—	$\longrightarrow$ "
$4q$	1	$\frac{4q+1}{2}$	—	$\longrightarrow$ "

Thus the first factorisation is not possible. For other cases, $\alpha\beta \in \mathbb{Q}$ but then $\sqrt{q} \in \mathbb{Q}$. Not possible. So $f(x)$ is irreducible over $\mathbb{Q}$.

Note that, $\mathbb{Q}(\alpha, \sqrt{q})$ is splitting field of polynomial $f(x)$. Also, $\sqrt{q} \notin \mathbb{Q}(\alpha)$, thus $[\mathbb{Q}(\alpha,\sqrt{q}):\mathbb{Q}]=8$. Now resolvant cubic of $f(x)$ is,

$$h(x) = x^3+2px^2+(p^2-4q)x$$
$$= x\,(\underbrace{x^2+2px+(p^2-4q)}_{\text{Roots are } -p\pm 2\sqrt{q}\ \notin \mathbb{Q}})$$

Thus $Gal(f)$ can be $\simeq D_8$ or $\mathbb{Z}/4\mathbb{Z}$. The later case isn't possible as $|Gal(f)|=8$

So, we can conclude $Gal(f) \simeq D_8$. ∎

(7) Prove that the polynomial $x^4+px+p \in \mathbb{Q}[x]$ is irreducible for every prime p, and for $p \neq 3, 5$ has Galois group S_4. Prove that the Galois group for $p=3$ is D_8 and for $p=5$ is cyclic of order 4.

Let, $f(x)=x^4+px+p$ By Eisenstine critation modulo p we can say $f(x)$ is irreducible. The resolvent cubic is,

$$h(x) = x^3 - 4Px + P^2$$

By rational root theorem $h(x)$ don't have root in $\mathbb{Q}$ unless $p=3,5$.

For $p \neq 3,5$, $h(x)$ is irreducible. The discrimnents

$$D = 256p^3 - 27p^4 = (256-27P)P \cdot P^2$$

For $p=2$ it's not a Square

For $p \neq 2$, $(256-27p)\,p$ is not a square as $p \nmid 256-27p$

$$\Rightarrow \sqrt{D} \notin \mathbb{Q}$$

So, $\mathrm{Gal}(f) \cong S_4$.

- For $P=3$, $h(x) = x^3 - 12x + 9 = (x-3)(x^2+3x-3)$ and discriminat

$$D = 3^3 \cdot 5^2 \cdot 7 \Rightarrow \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{21})$$

$f(x) = x^4 + 3x + 3$ is not reducible in $\mathbb{Q}(\sqrt{21}) \Rightarrow \mathrm{Gal}(f) \cong D_8$

- For $p=3$, $h(x) = x^3 - 20x + 25 = (x+5)(x^2-5x+5)$ and discriminant

$$D = 5^3 \cdot 11^2 \Rightarrow \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{21}).$$

$f(x) = x^4 + 5x + 5 = (x^2 - \sqrt{5}x + \sqrt{5} + 5)(x^2 + \sqrt{5}x - \sqrt{5} + 5)$ in $\mathbb{Q}(\sqrt{5})$. So, $\mathrm{Gal}(f) \cong \mathbb{Z}/4\mathbb{Z}$ ■

(8) Find the Galois group over $\mathbb{Q}$ of the polynomial $x^4 + 8x^2 + 8x + 4$. Find which subfields of the splitting field are Galois over $\mathbb{Q}$, and for these, determine a polynomial for each over $\mathbb{Q}$ for which they are the splitting fields.

Let, $f(x) = x^4 + 8x^2 + 8x + 4$. By rational root theorem $x = \pm 1, \pm 2, \pm 4$ are only possible rational roots But $f(\pm 1), f(\pm 2), f(\pm 4) \neq 0$. So, $f(x)$ don't have any linear factor over $\mathbb{Q}$. Let see if f has two quadratic factor. Let,

$$f(x) = (x^2 + a_1 x + a_2)(x^2 + b_1 x + b_2) = x^4 + \underbrace{(a_1+b_1)}_{=0} x^3 + \underbrace{(a_1 b_1 + a_2 + b_2)}_{=8} x^2 + \underbrace{(a_1 b_2 + a_2 b_1)}_{=8} x + \underbrace{a_2 b_2}_{=4}$$

$$= (a_2 - b_2) b_1$$

b_1	a_1	a_2-b_2	a_2+b_2	a_2	b_2	Possible?
1	-1	8	4	6	-2	×
2	-2	4	4	4	0	×
4	-4	2	4	3	1	×
8	-8	1	4	$5/2$	$3/2$	×
						×

Similarly for $-1, -2, -4, -8$.

Thus, $f(x)$ is irreducible over $\mathbb{Q}$. The resolvent cubic is,

$$h(x) = x^3 - 16x^2 + 48x + 64$$

By rational root theorem this polynomial is irreducible. Now discriminant of this polynomial $h(x)$ is, $D = 200704 = (7 \cdot 12^6)^2$. Thus, $Gal(f) = A_4$.

- The normal subgroup of A_4 is $\{e\}, V_4, A_4$. Note that $[A_4 : V_4] = 3$, corresponding field is cubic. Splitting field of f contains splitting field of h. Note that, $[L : \mathbb{Q}] = 3$, where $L = Split(h)$ as $\sqrt{D} \in \mathbb{Q}$ (shown above). So, L must correspond to $\mathcal{F}(V_4)$. Hence, L is splitting field of $h(x)$. ■

(9) Let L/F be a root extension, and let M be an intermediate extension. Show that M/F need not be a root extension.

Solution. Let, $\omega = \zeta_7$, then the extension $\mathbb{Q}(\omega)|_{\mathbb{Q}}$ is a root extension. We know, ω will satisfy the quadratic $x^2 - 2\cos\frac{2\pi}{7}x + 1$ as $\cos\frac{2\pi}{7} = \frac{1}{2}(\omega + \omega^{-1})$. Since $\mathbb{Q}(\cos\frac{2\pi}{7}) \in \mathbb{R}$ we can say, the degree of the extension $\mathbb{Q}(\omega)/\mathbb{Q}(\cos\frac{2\pi}{7})$ is two. But then, $\mathbb{Q}(\cos\frac{2\pi}{7})/\mathbb{Q}$ has degree 3. Since $\text{Gal}(\mathbb{Q}(\omega)|\mathbb{Q})$ is isomorphic to $\mathbb{Z}_6$ we can say any subgroup of this Galois group is normal thus $\mathbb{Q}(\cos\frac{2\pi}{7})/\mathbb{Q}$ is Galois extension of dgree 3. If $\mathbb{Q}(\cos\frac{2\pi}{7})/\mathbb{Q}$ was a root extension it must be an extension of type $\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}$ as 3 is a prime(here $a \in \mathbb{Q}$). But then $\mathbb{Q}(\cos\frac{2\pi}{7})$ and $\mathbb{Q}(\sqrt[3]{a})$ can't be equal as the former one is Galois extension but later one is not. So, $\mathbb{Q}(\omega)/\mathbb{Q}$ is a root extension but $\mathbb{Q}(\cos\frac{2\pi}{7})/\mathbb{Q}$ is not. ■

(10) Solve the equation

$$x^6 + 2x^5 - 5x^4 + 9x^3 - 5x^2 + 2x + 1$$

in terms of radicals. (Hint: Substitute $y = x + \frac{1}{x}$).

We have to solve the following equation

$$x^6 + 2x^5 - 5x^4 + 9x^3 - 5x^2 + 2x + 1 = 0$$

$$\Rightarrow x^3 + \frac{1}{x^3} + 2\left(x^2 + \frac{1}{x^2}\right) - 5\left(x + \frac{1}{x}\right) + 9 = 0$$

($x = 0$ is not a solution, so divide the eq^n by x^3)

$$\Rightarrow \left(x + \frac{1}{x}\right)\left(x^2 + \frac{1}{x^2} - 1\right) + 2\left(x + \frac{1}{x}\right)^2 - 5\left(x + \frac{1}{x}\right) + 5 = 0$$

$$\Rightarrow y(y^2 - 3) + 2y^2 - 5y + 5 = 0 \qquad \left[\text{Here } y = x + \frac{1}{x}\right]$$

$$\Rightarrow y^3 + 2y^2 - 8y + 5 = 0$$

$$\Rightarrow (y-1)(y^2 + 3y - 5) = 0$$

$\Rightarrow$ solution to the cubic in y is, $y = 1, \dfrac{-3 \pm \sqrt{29}}{2}$.

Let, $\alpha = \dfrac{-3 + \sqrt{29}}{2}$, $\beta = \dfrac{-3 - \sqrt{29}}{2}$.

We have to solve the following eq^{n}s :-

- $x + \frac{1}{x} = 1 \Rightarrow x^2 - x + 1 = 0$, $x = -\omega, -\omega^2$ (ω := cube root of unity)
- $x + \frac{1}{x} = \alpha \Rightarrow x^2 - \alpha x + 1 = 0$, $x = \dfrac{\alpha \pm \sqrt{\alpha^2 - 4}}{2}$
- Similar for $x + \frac{1}{x} = \beta$.

$\therefore$ Solution to the given 6 degree polynomial are, $-\omega, \omega^2$; $\dfrac{\alpha \pm \sqrt{\alpha^2 - 4}}{2}$, $\dfrac{\beta \pm \sqrt{\beta^2 - 4}}{2}$

Where, $\alpha = \dfrac{-3 + \sqrt{29}}{2}$, $\beta = \dfrac{-3 - \sqrt{29}}{2}$. ∎

(11) Show that for each $n \in \mathbb{N}$, $x^n - 1$ is solvable by radicals over $\mathbb{Q}$.

Solution. Let, ζ_n be n-th primitive roots of unity and μ_n be the group of all n-th roots of unity. We know μ_n is isomorphic to the group $\mathbb{Z}/n\mathbb{Z}$ with it's generator ζ_n. Thus $\mathbb{Q}(\zeta_n)|_{\mathbb{Q}}$ is the Galois extension for $f(x) = x^n - 1$, as it contains all the roots of f and all the roots are distinct (by checking f'). Thus we have,

$$\mathrm{Gal}(f) \simeq \mathrm{Aut}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$$

If $n = 2^{a_0} p_1^{a_1} \cdots p_k^{a_k}$, where p_i are odd primes, we must have

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/2^{a_0}\mathbb{Z})^* \times \cdots \times \left(\mathbb{Z}/p_k^{a_k}\mathbb{Z}\right)^*$$

Now consider the following composition series,

$$\{e\} \trianglelefteq (\mathbb{Z}/2^{a_0}\mathbb{Z})^* \trianglelefteq (\mathbb{Z}/2^{a_0}\mathbb{Z})^* \times (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^* \cdots \trianglelefteq (\mathbb{Z}/n\mathbb{Z})^*$$

Except the first term quotient of consecutive terms are isomorphic to $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^{ast}$, for odd primes p_i this is a cyclic group. We also know from group theory $\left(\mathbb{Z}/2^t\mathbb{Z}\right)^{ast}$ is solvable. Thus, the above composition series is solvable series. Hence, $(\mathbb{Z}/n\mathbb{Z})^*$ is solvable. Thus $\mathrm{Gal}(f)$ is solvable and hence $x^n - 1$ is solvable by radicals. ■

(12) Let $p(x) = x^6 - 3x^3 - 1$. Show that $p(x)$ is solvable by radicals over $\mathbb{Q}$.

Solution. We will explicitly write down the roots,

$$\begin{aligned} x^6 - &3x^3 - 1 = 0 \\ x^3 &= \frac{3 \pm \sqrt{13}}{2} \\ x &= \sqrt[3]{\frac{3 \pm \sqrt{13}}{2}}, \sqrt[3]{\frac{3 \pm \sqrt{13}}{2}}\omega, \sqrt[3]{\frac{3 \pm \sqrt{13}}{2}}\omega^2 \end{aligned}$$

where, $\omega = \frac{-1+i\sqrt{3}}{2}$ is the cube root of unity. Thus, all the roots of the polynomial are solvable by radicals. ■

(13) Show that $x^5 - x - 1$ is not solvable by radicals.

Solution. We will show, $f(x) = x^5 - x - 1$ is irreducible in $\mathbb{Q}$. To show this check this polynomial in $\mathbb{Z}/5\mathbb{Z}$. If this polynomial was reducible over $\mathbb{Q}$ it must have been reducible over $\mathbb{Z}/5\mathbb{Z}$. We claim the following:

Claim— The polynomial $x^p - x - 1$ is irreducible over $\mathbb{F}_p$, for a prime p

Proof. This result was proved in Assignment-1A.

Using the above result we can say $x^5 - x - 1$ is irreducible over $\mathbb{Z}/5\mathbb{Z}$ and hence irreducible over $\mathbb{Q}$. This means Galois group of f contains a 5-cycle. We can write this polynomial as $(x^3 + x^2 + 1)(x^2 + x + 1)$ in $\mathbb{Z}/2\mathbb{Z}$. By Dedekind's theorem $\mathrm{Gal}(f)$ contains as $(3, 2)$-cycle. By taking cube of this element we get a transposition. Thus $\mathrm{Gal}(f) \subseteq S_5$ contains a transposition and a 5-cycle, by the group structure of S_5 we know, $\mathrm{Gal}(f) = S_5$. We know a polynomial is solvable by radicals iff it's Galois group is solvable. But S_5 is not solvable. So the given polynomial is not solvable by radicals. ■

(14) Show that if K is a subfield of $\mathbb{C}$ and L/K is a root extension which is also normal, then the Galois group of L/K is solvable.

Solution. As L is a root extension of K, that is, it is obtained as a chain of simple radical extensions, and K is a subfield of $\mathbb{C}$, we get L is separable over K. Further, L is normal over K and hence, L/K is a Galois extension. Now, it is a result proved in Assignment 1, that an extension is normal iff it is a splitting field of a (single) polynomial f. Hence, we have a Galois extension L/K which is the splitting field of a polynomial $f \in K[x]$, and is given to be a root extension. By definition, this means all roots of f are expressible by radicals. We now use the result that a polynomial is solvable by radicals iff it has a solvable Galois group to conclude $\mathrm{Gal}(L/K)$ is a solvable group. ■

(15) Show that of n is an integer such that $n > 1$, and p is a prime then the quintic $x^5 - npx + p$ cannot be solved by radicals.

Solution. Let, $f(x) = x^5 - npx + p$. By Eisenstein criteria for p we get, this is irreducible. So, $\mathrm{Gal}(f)$ contains a 5-cycle. Now note that,

$$f(0) = p > 0, f(1) = 1 + p(1-n) < 0 \text{ (as } n > 1)$$
$$\lim_{x\to\infty} f(x) \to \infty, \lim_{x\to-\infty} f(x) \to -\infty$$

Thus $f(x)$ has three roots in the region, $(-\infty, 0)$,$(0, 1)$ and $(1, \infty)$ respectively. Also note, $f'(x) = 5x^4 - np$ has two real solutions and $f\left(\pm\sqrt[4]{\frac{np}{5}}\right)$ is non-zero. So these are the only real roots of $f(x)$. Thus, $f(x)$ has exactly two complex roots. Let α be a complex root of f, then $\bar{\alpha}$ is the other complex root. There is an element σ in $\mathrm{Gal}(f)$ such that $\sigma(\alpha) = \bar{\alpha}$ thus σ has order 2 in the Galois group. Thus $\mathrm{Gal}(f) \subseteq S_5$ contains a 5-cycle and a transposition and hence $\mathrm{Gal}(f) = S_5$. Again this group is not solvable. So f is not solvable by radicals. ■