2. P.T. any constructible complex number is algebraic over $\mathbb{Q}$ of degree a power of 2.

Sol: Let $\mathbb{Q}$ be field of rational numbers.
Let a be constructible.

Then we can find complex numbers $a_1, a_2 \ldots a_n$

$a_1^2 \in \mathbb{Q}$, $a_2^2 \in \mathbb{Q}(a_1)$, $a_3^2 \in \mathbb{Q}(a_1, a_2)$ . . .

$a_n^2 \in \mathbb{Q}(a_1 a_2 \ldots a_{n-1})$

& $a \in \mathbb{Q}(a_1 a_2 \ldots a_n)$

Let $F_0 = \mathbb{Q}$

$F_1 = \mathbb{Q}(a_1)$

$F_2 = \mathbb{Q}(a_1, a_2)$

— — — —

$F_i = \mathbb{Q}(a_1, a_2 \ldots, a_i)$

— — — —

$F_n = \mathbb{Q}(a_1, a_2 \ldots, a_n)$

$[F_{i-1}(a_i) : F_{i-1}] = [F(a_1, a_2 \ldots a_{i-1})(a_i) : F_{i-1}]$

$= [F(a_1 a_2 \ldots a_i) : F_{i-1}]$

$= [F_i : F_{i-1}]$

≤ 2

$[F_n : F_0] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \ldots [F_1 : F_0]$

$= 2^m$, $m \leq n$

$[F_n : \mathbb{Q}] = 2^m$

Hence $a \in F_n = \mathbb{Q}(a_1 a_2 \ldots a_n)$ finite ext. of $\mathbb{Q}$ of degree, power of 2.

4. F be field of ch zero Contain all roots of unity. Then Polynomial $p(x) \in F[x]$ is solvable by radicals iff Galois group over F is solvable group.

S.1:

Step I Let $p(x)$ be Solvable by radicals.

Let E be splitting field over F.

$\exists$ sequence of fields,

$F_0 = F \subseteq F_1$ [$F_0 \subseteq F_1$

$F_1 = F_0(\omega_1) \subseteq F_2$ $F_1 \subseteq F_2$

$F_2 = F_1(\omega_2) \subseteq F_3$ $F_2 \subseteq F_3$

— — — —

$F_{K-1} \subseteq F_K$]

$F_{K-1} = F_{K-2}(\omega_{K1}) \subseteq F_K$

$F_K = F_{K-1}(\omega_K)$

$\omega_i \in F_i$, $E \subseteq F_K$

$\therefore F_K$ is normal Ext. of F

$\Rightarrow$ F_K is normal Ext. of Field F_i

Each F_i is normal Ext. of F_{i-1}.

By fundamental Thm of Galois Theory,

$G(F_K, F_i)$ is normal subgroup of $G(F_K, F_{i-1})$

Now $G(F_K, F_0) \supseteq G(F_K, F_1) \supseteq G(F_K, F_2) \cdots$

$\supseteq G(F_K, F_{K-1}) \supseteq I$

— (1)

step II By fund. Thm of G.T,

$$G(f_i, F_{i-1}) \cong \frac{G(f_k, F_{i-1})}{G(F_k, F_i)}$$

E is normal Ext. of F, $E \subseteq F_k$

$G(F_k, E)$ is normal subgp of $G(F_k, F)$

& $$G(E, F) \cong \frac{G(F_k, F)}{G(F_k, E)}$$

$\Rightarrow$ $G(E, F)$ is homomorphic image of $G(F_k, F)$ is solvable group.

$\therefore$ $G(E, F)$ is solvable

Hence Galois Group of Given Polynomial is Solvable.

Converse :- Let $G(E, F)$ is Solvable.

step III $\exists$ subnormal series

$$G_0 = G(E, F) \supseteq G_1 \supseteq G_2 \cdots \supseteq G_{k-1} \supseteq G_k = I$$

Let F_i be fixed field under G_i

G_i - Group of all F automorphism of F_k

$$G_i = G(E, F_i)$$

F_{i+1} is normal Ext. of F_i

$$G(F_{i+1}, F_i) \cong \frac{G_i}{G_{i+1}}$$

$\therefore$ $G(F_{i+1}, F_i)$ is cyclic.

Step IV

F_i Contain all Primitive roots of unity

$\exists\ a_i \in F_i$

$\exists\ n_i$ integer

$x^{n_i} - a_i$ is irreducible over F_i

Let w_i be any root of $x^{n_i} - a_i$

$$F_{i+1} = F_i(w_i)$$

$$F = F_0 \subseteq F_1 \subseteq F_2 \ldots \subseteq F_k = E$$

Hence E is ext. of F by radicals.

$\therefore p(x)$ is solvable by radicals.

5:

C.H Moore Theorem

statement :- P.T for Every Prime number p and $n \in N$ $\exists$ a unique field having p^n Elements.

Proof :- Consider polynomial

$$f(x) = x^{p^n} - x \ , f(x) \in Z_p[x]$$

Z_p field of integers.

Let F be splitting field of $f(x)$ over Z_p

T.P F is field having p^n Elements

$$f'(x) = p^n x^{p^n - 1} - 1$$

$ch(\mathbb{Z}_p) = p$

i.e. $pa = 0 \quad \forall\ a \in \mathbb{Z}_p$

$p = 0$

So $p^n = 0$

$\therefore f'(x) = p^n x^{p^n - 1} - 1$

$= 0 - 1 \neq 0$

$f(x)$ & $f'(x)$ have no common factor of +ve degree.

$\Rightarrow$ $f(x)$ has no multiple roots.

$x^{p^n} - x = (x - a_1)(x - a_2) \cdots (x - a_{p^n})$

Let $a, b \in F$

$a^{p^n} = a, \quad b^{p^n} = b \quad - (1)$

$ch(F) = p$

Now $(a-b)^{p^n} = a^{p^n} - b^{p^n} \quad [\because (a \mp b)^p = a^p - b^p]$

$= a - b \quad (\text{By } (1))$

$= (a - b) \in F$

Also let $a, b \in F, b \neq 0$

$(b^{p^n})^{-1} = b^{-1} \Rightarrow (b^{-1})^{p^n} = b^{-1}$

$\Rightarrow b^{-1} \in F$

Also. $(ab^{-1})^{p^n} = a^{p^n} (b^{-1})^{p^n} \quad [\because (ab)^p = a^p b^p]$

$= a b^{-1} \in F$

Hence F is Field with p^n Elements.