<u>**Solvability by Radicals Prepared by**</u>

Dr. A.Lourdusamy M.Sc., M.Phil., B.Ed., Ph.D.

Reader in mathematics,

St.Xavier's College (Autonomous),

Palayamkottai-627002.

Ref: Topics in Algebra By I.N. Herstein

5 .7 Solvability by Radicals

Given $x^2 + 3x + 4$ over the field of rational numbers F_0 ,

the roots are $(-3 \pm \sqrt{-7}\ ) / 2$

$\therefore$ The field $F_o(\sqrt{7}\ i\ )$ is the splitting field of $X^2 + 3x + 4$ over F_o .

$$\boxed{F_0(\omega) = F_0(\sqrt{b^2-4ac})}$$

i.e. , $\exists\ \gamma = -7$ in F_o such that the extension field $F_0(\omega)$ where $\omega^2 = \gamma$,

($\omega^2 = b^2 - 4ac = 9 - 16 = -7$) is such that it contains all the roots of x^2+3x+4 .

From a slightly different point of view , given the general quadratic polynomial $p(x) = x^2 + a_1x + a_2$ over F , we can consider it as a particular polynomial over the field F (a_1 , a_2) of rational functions in a_1, a_2 over F ; in the extension obtained by adjoining ω to F (a_1,a_2) where

$\omega^2 = a_1^2 - 4a_2 \in F\ (a_1 ,a_2)$, we find all the roots of p(x) .

($b^2 - 4ac$ in $x^2 + bx + c$)

$\therefore$ There is a formula which expresses the roots of $p(x)$ in terms of a_1, a_2 and square roots of rational functions of these.

Similarly for cubic polynomials formulas are available to express roots in terms of co-efficients and square roots and cube roots of co-efficients. Consider $x^3 + a_1x^2 + a_2 x + a_3$ .Adjoin a certain square root & then a cube root to $F(a_1, a_2, a_3)$, we reach a field in which $p(x)$ has its roots .

For 4^{th} degree polynomials also , we can express the roots in terms of combinations of radicals (surds) of rational functions of the co-efficients.

For polynomials of degree 5 & higher , no such universal radical formula can be given , for we shall prove that it is <u>impossible</u> to express their roots , in general , in this way .

Definition: Given a field F & a polynomial $p(x) \in F[x]$, we say that $p(x)$ is **solvable by radicals over F** if we can find a finite sequence of fields

$F_1 = F(w_1)$, $F_2 = F_1(w_2) = F(w_1, w_2)$, - - - ,

$F_k = F_{k-1}(w_k) = F(w_1, w_2, \ldots, w_k)$ s .t .

$w_1^{r_1} \in F$, $w_2^{r_2} \in F_1, \ldots, w_k^{r_k} \in F_{k-1}$ s .t . the roots of p(x) all lie in F_k .(as in n =2 , $w^2 = \nu = -7 \in F$, the field of rational numbers)

Note: Difference between 1) splitting field & 2)solvability.

1) existence of fields in which roots exist.

2) solving exactly, i. e. roots are expressed in terms of co- efficients

.i.e. Formulae for roots are given in terms of radicals of rational function of co-efficients .

Note: If K is splitting field of p(x) over F , then p(x) is solvable by radicals over F if we can find a sequence of fields as above such that K C F_k

Remark:

If such an F_k can be found , we can ,without loss of generality , assume it to be a normal extension of F . (By the general polynomial of degree n over F,

$p(x) = x^n + a_1x^{n-1} + \dots + a_n$, we mean the following:

Let $F(a_1, \dots, a_n)$ be the field of rational functions, in n variables $a_1,\dots,a_n$ over F & consider the particular polynomial $p(x) = x^n+a_1x^{n-1}+\dots+a_n$ over the field $F(a_1,\dots,a_n)$.

We say that it is solvable by radicals if it is solvable by radicals over $F(a_1,\dots, a_n)$

This really expresses the intuitive idea of "finding a formula" for the roots of p(x) involving combination of m^{th} roots, for various m's , of rational functions in $a_1, \dots, a_n$. For n = 2 , 3, 4, this can always be done .

For $n \geq 5$, Abel proved that this cannot be done .

In fact, we shall give a criterion for this in terms of the Galois group of the polynomial. But first we must develop a few purely group theoretical results.

Definition: A group G is solvable if we can find a finite chain of subgroups $G = N_0 \supset N_1 \supset N_2 \supset .... \supset N_k = (e)$, where each N_i is a normal subgroup of N_{i-1} and such that every factor group N_{i-1}/N_i is abelian.

Result 1 Every abelian group is solvable.

Proof **:** Take $N_0 = G$ & $N_1 = (e)$

$\therefore \exists$ a finite chain of subgroups $G=N_0 \supset N_1 = (e)$.

where N_1 is a normal subgroup of N_0

$(gng^{-1}=geg^{-1} \quad \because N_1=(e)$

$=gg^{-1}=e \in N_1, \ \forall g \in G \ \ \forall e \in N_1)$

& $N_0/N_1 = G/(e) \approx G$ is abelian.

$\therefore$ Every abelian group is solvable.

Result 2 : S_3 is solvable.

Proof: $S_3 =\{ (1), (1,2), (2,3), (3,1), (1,2,3),(1,3,2)\}$

$A_3= \{(1),(1\ 2\ 3), (1\ 3\ 2)\}$

Take $N_0=S_3$, $N_1=A_3$, $N_2=\{(1)\}$

Then $\exists$ a finite chain of subgroups

$S_3 = N_0 \supset N_1 \supset N_2 = (e)$, (is a solvable series for S_3).

We know that A_3 is a normal subgroup of $P_3=S_3$

$\therefore$ N_1 is a normal subgroup of N_0

Also $(1) = N_2$ is a normal group of N_1

The quotient groups N_0/N_1 & N_1/N_2 are of orders 2&3 respectively.

We know that "all groups of order 2&3 are abelian"

$\therefore$ N_0/N_1 & N_1/N_2 are abelian

$\therefore \exists$ a finite chain of subgroups $S_3 = N_0 \supset N_1 \supset N_2 = (e)$,

such that N_0/N_1 & N_1/N_2 are abelian .

Hence S_3 is a solvable.

Show that S_4 is solvable.

Proof:

Let A_4 be the alternating group of permutations of degree 4.

A_4 is a normal subgroup of $P_4=S_4$

Let V_4 = {e, (1 2) (3 4) , (1 3) (2 4), (1 4) (2 3)}

Clearly V_4 is a normal subgroup of A_4.

Take $N_0=S_4$, $N_1=A_4$,$N_2=V_4$, & $N_3=(e)$

Claim: $S_4 = N_0 \supset N_1 \supset N_2 \supset N_3 = (e)$ is a solvable series for $P_4=S_4$ .Clearly (e) is a normal subgroup of N_2.

The quotient groups S_4/N_1,N_1/N_2, &N_2/N_3 are of orders 2,3 &4 respectively.

We know that "all groups of order up to order 5 are abelian"

$\therefore$ S_4/N_1,N_1/N_2, &N_2/N_3 are abelian

$\therefore \exists$ a finite chain of subgroups of $S_4 = N_0 \supset N_1 \supset N_2 \supset N_3 = (e)$ such that

s.t N_0/N_1, N_1/N_2, &N_2/N_3 are abelian

$\therefore$ It is a solvable series.

Hence S_4 is solvable.

Note:For $n \geq 5$ we show in T 5.7.1 below that S_n is not solvable.

Alternative description for solvability.

Definition: Given the group G and elements a,b in G, then the commutator of a&b is the element $a^{-1}b^{-1}ab$.

The commutator subgroup, G^1 ,of G is the subgroup of G generated by all the commutators in G. i.e., G^1 is generated by{ $a^{-1}b^{-1}ab/a,b \in G$ }

Note: 1. We can also define the commutator of a&b to be $aba^{-1}b^{-1}$. In this case, G^1 is generated by $\{aba^{-1} b^{-1} / a, b \in G\}$.

2. The commutator subgroup G^1 of a group is the smallest subgroup of G containing the set of all commutators in G.

Result: Let G^1 be the commutator subgroup of a group

Then G is abelian iff $G^1 = (e)$.

Theorem: Let G be a group & G^1 be the commutator subgroup of G. Then

(i) G^1 is normal in G.

(ii) G / G^1 is abelian

(iii) If N is any normal subgroup of G, then G / N is abelian iff $G^1 \subseteq N$

(iv) If H is a subgroup of G, such that $H \supseteq G'$, H is a normal subgroup of G.

Proof: Let $U = \{aba^{-1}b^{-1} / a,b \in G\}$. If G^1 is the commutator subgroup of G,

then G^1 is the smallest subgroup of G containing U.

(i) Let $x \in G \;\&\; c \in G'$

Now $x c x^{-1} = (x c x^{-1}) c^{-1} c$

$$= (x c x^{-1} c^{-1}) c$$

Now $x, c \in G \Rightarrow x c x^{-1} c^{-1} \in G'$

$\therefore x c x^{-1} c^{-1} \in G' \;\&\; c \;\; \in G'$

$\Rightarrow (x c x^{-1} c^{-1}) c \in G'$

$\Rightarrow x c x^{-1} \in G^1 \; \forall c \in G'$

$x \in G$

$\therefore G^1$ is normal in G.

(ii) $a, b \in G \Rightarrow G^{'}a, G^{'}b \in G / G^{1}$

We have $ab\, a^{-1}\, b^{-1} \in U$

$\Rightarrow ab\, a^{-1}\, b^{-1} \in G^{'} \quad (\because U \subset G^{'})$

$\Rightarrow (ab)\,(ba)^{-1} \in G^{'}$

$\Rightarrow G^{'}(ab) = G^{'}(ba)$

$\Rightarrow (G^{'}a)(G^{'}b) = (G^{'}b)(G^{'}a)$

$\Rightarrow G/G'$ is abelian

(iii)Let N be any normal subgroup of G.

Let a,b $\in G \Rightarrow$ Na,Nb $\in G/N$

Let G/N be abelian.

Then (Na) (Nb) = (Nb) (Na)

$\Rightarrow Nab = Nba$

$\Rightarrow (ab)(ba)^{-1} \in N$

$\Rightarrow aba^{-1}b^{-1} \in N \Rightarrow U \subseteq N$

($\because aba^{-1}b^{-1}$ is any element of U)

$\therefore$ N is the sub group of G containing U.

But G^1 is the smallest subgroup of G containing U.

$\Rightarrow N \supseteq G'$

Conversely, let $G' \subseteq N$

Now G' is the Smallest subgroup of G Containing U & $G' \subseteq N$

$\Rightarrow U \subseteq G^1 \subseteq N$

$\Rightarrow U \subseteq N$

$\Rightarrow aba^{-1} b^{-1} \in N$

$\Rightarrow (ab)(ba)^{-1} \in N$

$\Rightarrow Nab = Nba$

$\Rightarrow (Na)(Nb) = (Nb)(Na)$

$\Rightarrow G/N$ is abelian

(iv) **Given**

H is a subgroup of G such that $H \supseteq G^1$

Let $g \in G$ & $h \in H$

Then $ghg^{-1} = (ghg^{-1})(h^{-1}h)$

$$= (ghg^{-1}h^{-1})h$$

Now $ghg^{-1}h^{-1} \in G'$

$\Rightarrow ghg^{-1}h^{-1} \in H$

$\therefore ghg^{-1}h^{-1} \in H$ & $h \in H$

$\Rightarrow (ghg^{-1}h^{-1})h \in H$

$\Rightarrow ghg^{-1} \in H \; \forall \; g \in G, h \in H$

$\therefore$ H is the normal sub group of G.

Note: G' is a group in its own right, so we can speak of its commutator subgroup $G^{(2)} = (G^1)^1$

i.e., $G^{(2)}$ is the subgroup of G generated by all elements

$a^1 b^1 (a^1)^{-1} (b^1)^{-1}$ or $(a^1)^{-1} (b^1)^{-1} a^1 b^1$ where $a^1, b^1 \in G'$

We know G^1 is normal in G.

$\therefore\ (G^1)^1 = G^{(2)}$ is normal in G'. It can be easily proved that $G^{(2)}$ is normal in G as well.

Continuing in this way we can define higher commutator subgroup $G^{(m)}$ by $G^{(m)} = (G^{(m-1)})^!$

This $G^{(m)}$ is called m^{th} commutator sub group or m^{th} derived subgroup of G. It is easy to see that $G^{(m)}$ is a normal subgroup of G.

We know G/G' is abelian.

$\therefore G^{(m-1)} / G^{(m)}$ is abelian.

(In terms of higher commutator subgroups of a group G we have a very succinct (important) criterion for solvability of G.)

L 5.7.1 A group G is solvable it $G^{(k)} = (e)$ for some integer k.

Proof : The 'if' part

Let $G^{(k)} = (e)$ for some integer k.

To Prove G is solvable.

Let $N_0 = G, N_1 = G^1, N_2 = G^{(2)}, \ldots, N_k = G^{(k)} = (e)$

Then $G = N_o \supseteq N_1 \supseteq N_2 \supseteq \ldots \supseteq N_k = (e)$

we know G^1 is a normal subgroup of G.

$\therefore G^{(i)} = (G^{(i-1)})'$ is a normal sub group of $G^{(i-1)}$ for each i.

$\Rightarrow N_i$ is a normal subgroup of N_{i-1} for each i.

Also $\dfrac{N_{i-1}}{N_i} = \dfrac{G^{(i-1)}}{G^{(i)}} = \dfrac{G^{(i-1)}}{(G^{(i-1)})'}$

we know that G / G' is abelian

$\therefore \dfrac{G^{(i-1)}}{(G^{(i-1)})^1}$ is abelian

$\Rightarrow N_{i-1} / N_i$ is abelian for each i.

$\therefore \exists$ a finite chain of subgroups.

$G = N_o \supseteq N_1 \supseteq N_2 \supseteq \ldots \supseteq N_k = (e)$, where each N_i is a normal subgroup of N_{i-1} and such that every factor group N_{i-1} / N_i is abelian.

$\therefore$ G is solvable.

<u>'only if'</u> part

Let G be a solvable Group.

$\therefore \exists$ a finite chain of subgroups $G = No \supseteq N_1 \supseteq N_2 \supseteq \ldots \supseteq N_k = (e)$,

where each N_i is a normal subgroup of N_{i-1} and such that every factor group N_{i-1} / N_i is abelian.

we know "If N is normal subgroup of G, then G/N is abelian iff

$G^1 \subset N$"

So N_{i-1} / N_i is abelian $\Rightarrow N^1{}_{i-1} \subset N_i$

$\therefore \mathrm{Ni} \supset \mathrm{Ni}' - 1$ for each i. Hence

$$
\begin{aligned}
&N_1 \supset N_0' = G' \\
&N_2 \supset N_1' \supseteq (G')^1 = G^{(2)} \\
&N_3 \supset N_2' \supset (G^{(2)})^1 = G^{(3)} \\
&\ldots \quad \ldots \quad \ldots \quad \ldots \\
&N_i \supset G^{(i)} \\
&\ldots \quad \ldots \quad \ldots \quad \ldots \\
&N_k \supset G^{(k)}
\end{aligned}
$$

$$\left.\begin{array}{l} \text{For some k, } (e) = N_k \supseteq G^{(k)} \\ \text{But } (e) \subseteq G^{(k)} \text{ always.} \\ \text{Hence } G^{(k)} = (e). \end{array}\right\}$$

Corollary: If G is a solvable group and if $\overline{G}$ is a homomorphic image of G,

then $\overline{G}$ is solvable.

Proof : $\overline{G}$ is a homomorphic image of G

$\Rightarrow (\overline{G})^{(k)}$ is the image of $G^{(k)}$

Now G is solvable $\Rightarrow G^{(k)} =$ (e) for some k.

$\Rightarrow (\overline{G})^{(k)} = (e)$ for the same k.

($\because$ a homomorphism maps identity to identity)

$\therefore \overline{G}$ is solvable.

Next lemma is the key step in proving that S_n , $n \geq 5$ is not solvable).

L 5.7.2 $\left.\begin{array}{l}\text{Let } G = S_n \text{ where } n \geq 5\text{; then } G^{(k)} \text{ for} \\ k = 1,2,\ldots, \text{contains every 3-cycle of } S_n\end{array}\right\}$

Proof: We know "If N is a normal subgroup of a group G, then the commutator subgroup N' of N is also normal subgroup of G."

Claim: If N is a normal subgroup of $G = S_n$ where $n \geq 5$,

which contains every 3- cycle in S_n ,

then N' must also contain every 3- cycle.

Suppose a = (1 2 3) , b = (1 4 5) are in N.

Then $a^{-1} b^{-1} ab = (3\ 2\ 1)\ (5\ 4\ 1)\ (1\ 2\ 3)\ (1\ 4\ 5) = (1\ 4\ 2)$

Also $a^{-1} b^{-1} ab \in N'$ (as a commutator of elements of N)

$\Rightarrow (1\ 4\ 2) \in N' \Rightarrow \Pi^{-1} (1\ 4\ 2)\ \Pi \in N'\ \ \forall \Pi \in S_n$ ($\because N'$ is normal)

Now let (i_1,i_2,i_3) be any 3- cycle in S_n

where i_1,i_2,i_3 are any 3 distinct integers between 1&n.

Choose Π in S_n Such that $\Pi\ (1) = i$, $\Pi(4) = i_2$ & $\Pi(2) = i_3$.

Then $\Pi^{-1} (1\ 4\ 2)\ \Pi = (i_1,i_2,i_3)$ (i_1 goes to 1 under Π^{-1}

1 goes to 4 under (1 4 2)

4 goes to i_2 under Π

So i_1 goes to i_2 under $\Pi^{-1} (1\ 4\ 2)\ \Pi$.

Similarly i_2 goes to i_3, i_3 goes to i_1).

$\Rightarrow (i_1, i_2, i_3) \in N^1$.

$\Rightarrow$ N' contains all 3-cycles.

Let N = G.

G is normal in G & contains all 3- cycles

$\Rightarrow G'$ contains all 3- cycles.

Similarly G' is normal in G

$\Rightarrow (G^1)'$ contains all 3- cycles.

Similarly $G^{(2)}$ is normal in G.

$\Rightarrow (G^2)^1 = G^{(3)}$ contains all 3- cycles.

Continuing in this way, we conclude that $G^{(K)}$ contains all 3- cycles for arbitrary k.

(A direct consequence of this lemma is the interesting group theoretic result)

T 5.7.1 S_n is not solvable for $n \geq 5$

Proof If $G = S_n$, $G^{(K)}$ contains all 3-cycles in S_n for every k where $n \geq 5$

$\Rightarrow G^{(k)} \neq (e)$ for any k.

$\Rightarrow G = S_n$, $n \geq 5$, is not solvable.

(Interrelating the solvability by radicals of p(x) with the solvability of the Galois roup of p(x). But first we need a result about the Galois group of a certain type of olynomial.)

L 5.7.3 Suppose that the field F contains all the n^{th} roots of unity (for some particular n) & suppose that $a \neq 0$ in F. Let x^n-a $\in$ F[x] & let K be its splitting field over F. Then (1) K = F(u) where u is any root of x^n-a.

(2) The Galois group of x^n-a over F is abelian.

Proof: F has all n^{th} roots ($e^{2\Pi ir/n}$, r = 0 to n-1) of unity.

$\Rightarrow$ F has $\xi = e^{2\Pi i/n}$

Note $\xi^n = 1$ but $\xi^m \neq 1$ for 0 < m < n.

Let u $\in$ K be any root of x^n-a.

$\Rightarrow u, \xi u, \xi^2 u, ..., \xi^{n-1} u$ are all the roots of x^n-a.

These roots are distinct, for,

$$\xi^i u = \xi^j u \text{ with } 0 \le i < j < n$$

$$\Rightarrow (\xi^i - \xi^j)\, u = 0$$
$$\Rightarrow \xi^i - \xi^j = 0 \qquad (\because u \neq 0)$$
$$\Rightarrow \xi^i = \xi^j$$
$$\Rightarrow \xi^{j-i} = 1 \Rightarrow\Leftarrow \text{ to } 0 < j-1 < n$$

$\therefore\ \xi \in F \Rightarrow \xi \in F(u)$

$\therefore$ all of $u, \xi u, \ldots, \xi^{n-1} u$ are in F(u)

$\Rightarrow$ F(u) splits x^n-a

Also no proper subfield of F (u) which contains F also contains u.

$\Rightarrow$ No proper subfield of F (u) can split x^n-a.

$\therefore$ F(u) is the splitting field of x^n-a.

Hence K = F (u)

To Prove G (K, F) is abelian.

Let $\sigma, \tau \in G(K, F)$

$\Rightarrow \sigma \,\&\, \tau$ are automorphisms of K = F(u) leaving every element of F fixed.

$\Rightarrow$ $\sigma(u) \,\&\, \tau(u)$ are roots of $x^n - a$ ($\because$ u is a root of x^n-a)

$\Rightarrow \sigma(u) = \xi^i u \,\&\, \tau(u) = \xi^j u$ for some i& j.

$$\therefore \sigma\tau(u) = \sigma(\xi^j u) = \xi^j \sigma(u) \qquad (\because \xi^j \in F))$$

$$= \xi^j \xi^i u = \xi^{i+j} u.$$

$$|||^{ly}\ \tau\sigma(u) = \xi^{i+j} u.$$

$$\therefore \sigma\tau(u) = \tau\sigma(u)\ \forall\, u \in K.$$

$$\therefore \sigma\tau = \tau\sigma\ \forall\, \sigma, \tau \in G(K, F)$$

$\Rightarrow$ The Galois group G(K,F) is abelian.

Note: From the Lemma, if F has all n^{th} roots of unity,

then adjoining one root of x^n-a to F, where $a \in F$,

gives us the splitting field of x^n-a &

K = F(u) i.e., the splitting field is a normal extension of F.

T 5.7.2 Let F be a field which contains all n^{th} roots of unity for every integer n.

If $p(x) \in F[x]$ is solvable by radicals over F,

then the Galois group ,over F,

of p(x) is a solvable group.

Proof.

Let K be the splitting field of p(x) over F

$\therefore$ the Galois group of p(x) over F is G(K,F).

Given: p(x) is solvable by radicals

$\Rightarrow\ \exists$ a sequence of fields

$$F \subset F_1 = F(w_1) \subset F_2 = F_1(w_2) \subset \ldots \subset F_k = F_{k-1}(w_k)$$

where $w_1^{r_1} \in F, w_1^{r_2} \in F_1, \ldots, w_k^{r_k} \in F_{k-1} \,\&\, K \subset F_k$

(by note of L.5.7.3) Without Loss of Generality, assume that F_k is normal extension of F.

Also F_k is normal extension of each F_i.

(Again by note) Each F_i is a normal extension of F_{i-1}, & since F_k is normal over F_{i-1}, by F T G T (T 5.6.6)

$G(F_k, F_i)$ is a normal sub group in $G(F_k, F_{i-1})$

Consider the chain $G(F_k, F) \supset G(F_k, F_1) \supset G(F_k, F_2) \supset \ldots \supset G(F_k, F_{k-1}) \supset (e)$. - - -> (1)

Note that each subgroup in this chain is a normal subgroup in the one proceeding it.

By F T G T, $G(F_i,F_{i-1}) \approx G(F_k,F_{i-1}) / G(F_k, F_i)$

(L 5.7.3) we know The Galois group $G\left(F_i, F_{i-1}\right)$ is abelian

$\Rightarrow$ each quotient group $G(F_k, F_{i-1}) / G(F_k,F_i)$ of the chain (1) is abelian

$\Rightarrow G\left(F_k, F\right)$ is solvable.

Now $K \subset F_K$ & K is a normal extension of F(being a splitting field)

$\Rightarrow G(F_k, K)$ is a normal subgroup of $G(F_k,F)$ &

$G(K,F) \approx G(F_k, F) / G(F_k,K)$ (by F T G T)

$\Rightarrow G(K,F)$ is a homomorphic image of $G(F_k,F)$

$\Rightarrow G(K,F)$ is solvable

($\because G(F_k, F)$ is solvable &

homomorphic image of a solvable group is solvable)

$\therefore$ The Galois group of p(x) over F is solvable.

Note: 1 The converse of above theorem is true

2. Theorem & its converse are true even if F does not contain roots of unity.

Meaning of the general polynomial of degree n.

Let $F(a_1,....,a_n)$ be the field of rational functions in the n invariables $a_1,\ldots,a_n$ over F.

$p(x) = x^n + a_1 x^{n-1} +...+a_n$ over the field $F(a_1, a_2,...,a_n)$ is called the general polynomial of degree n over the field F.

P(x) is solvable by radicals if it is solvable by radicals over $F(a_1, a_2,...,a_n)$.

It is easy to show that the Galois group of

$$p(x) = x^n + a_1 x^{x-1} +...+a_n \quad \text{over} \quad F(a_1,...,a_n) \quad \text{is} \quad S_n.$$

T 5.7.3 (Abel's theorem) The general polynomial of degree $n \geq 5$ is not solvable by radicals.

Proof. (T 5.6.3) If $F(a_1,...,a_n)$ is the field of rational functions in the n variables $a_1,...,a_n$ then the Galois group of

$p(t) = a_0 + a_1t^{n-1}+...+a_n$ over $F(a_1, a_2,...,a_n)$ is S_n.

(T 5.7.1) S_n is not a solvable group when $n \geq 5$.

(T 5.7.2) $\therefore$ $p(t)$ is not solvable by radicals over $F(a_1,...,a_n)$ when $n \geq 5$.

7.1 finite fields

L 7.1.1 Let F be a finite field with q elements &suppose that $F \subset K$ where K is also a finite field. Then K has q^n elements where n = [K: F]

Proof; $F \subset K$ & K is finite

$\Rightarrow$ K is a finite dimension vector space over F

$\Rightarrow$ [K: F] = n

Let a basis of K over F be $v_1, v_2, \ldots, v_n$

Then every element in K has a unique representation in the form $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$

where $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$

$\therefore$ Number of elements in K= the number of $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$ as the $\alpha_1, \alpha_2, \ldots, \alpha_n$ range over F & |F| = q

$\therefore$ |K| = q^n since each co-efficient can have q values.

Corollary:1

Let F be a finite field. Then F has p^m elements where the prime number p is the characteristic of F

Proof:

F has a finite number of elements

$\Rightarrow$ f 1 = 0 where f = | F | $\left(a^{o(G)} = e\right)$ (if G is finite.)

$\Rightarrow$ F has characteristic p for some prime number p

$\Rightarrow$ F contains a field $F_0 \approx J_p$. Note F_0 has p elements

$\Rightarrow$ F has p^m elements where m = [F: F_0] (by L 7.1.1)

Corollary: 2 If the finite field F has p^m elements, then every a $\in$ F satisfies $a^{p^m} = a$

Proof; If a = 0 then clearly $a^{p^m} = a$

On the other hand, the non zero elements of F form a group under multiplication

of order $p^m - 1$

$\therefore a^{p^m - 1} = 1 \ \forall \ a \neq 0$ in F. ($a^{o(G)} = e$) (if G is finite.)

$\Rightarrow a^{p^m} = a$

(From corollary 2 we can easily pass to)

L.7.1.2

If the finite field F has p^m elements, then the polynomial $x^{p^m} - x$ in F[x] factors in F[x] as

$$x^{p^m} - x = \prod_{\lambda \in F} (x - \lambda)$$

Proof:

we know that $(L\,5.3.2)$ "A polynomial of degree n over a field can have atmost n roots in any extension field."

$\therefore$ $x^{p^m} - x$ has at most p^m roots in F.

We know that $(\text{cor}\quad 2\,\text{to}\,L\,7.1.1)$ If the finite field F has p^m elements, then every a $\in$ F satisfies $a^{p^m} = a$"

$\therefore$ all the p^m elements of F are roots of $x^{p^m} - x$.

Also we know that $(\text{cor to}\, L\,5.3.1)$ If a $\in$ K is a root of $p(x) \in F[x]$, where F $\subset$ K, then in $K[x]$, (x-a) | p(x)."

$\therefore$ For each $\lambda \in F, (x - \lambda) \mid x^{p^m}$ - x.

$$\therefore x^{p^m} - x = \prod_{\lambda \in F} (x - \lambda)$$

Corollary; l

If the field F has p^m elements, then F is the splitting field of the polynomial $x^{p^m} - x$

Proof;

By L 7.1.2, $x^{p^m} - x$ certainly splits in F. However, it cannot split in any smaller field for that field would have to have all the roots of this polynomial & so would have to have at least p^m elements. Thus F is the splitting field of $x^{p^m} - x$.

L 7.1.3

Any two finite fields having the same number of elements are isomorphic

Proof:

Let these fields have p^m elements.

Then (by the above corollary) they are both splitting fields of the polynomial $x^{p^m} - x$ over J_p.

$\Rightarrow$ The fields are isomorphic ($\because$ any 2 splitting fields are isomorphic)

L7.1.4

For every prime number p and every positive integer m, $\exists$ a field having p^m elements.

Proof

Consider the polynomial $x^{p^m} - x$ in J_p[x], the ring of polynomials. in x over J_p, the field of integers mod p.

Let K be the splitting field of this polynomial.

In K, let $F = \{a \in K / a^{p^m} = a\}$

Clearly the elements of F are the roots of $x^{p^m} - x$.

We know "(cor 2to L5.5.2) If F is a field of characteristic $p \neq 0$, then the polynomial $x^{p^n} - x \in F[x]$, for $n \geq 1$,has distinct roots."

$\therefore$ The elements of F are distinct roots of $x^{p^m} - x$.

$\Rightarrow$ F has p^m elements.

To Prove

F is a field.

Let $a,b \in F$

$\Rightarrow a^{p^m} = a$ & $b^{p^m} = b$

$\therefore (ab)^{p^m} = a^{p^m} b^{p^m} = ab$

$\Rightarrow ab \in F$

Also $(a \pm b)^{p^m} = a^{p^m} \pm b^{p^m}$ ($\because$ the char is p)

$= a \pm b$

$\Rightarrow a \pm b \in F$

$\therefore$ ab, a – b $\in$ F $\forall$ a, b $\in$ F

$\therefore$ F is a subfield of K & so is a field.

$\therefore$ We have exhibited the field F having p^m elements.

T. 7.1.1

For every prime number p & every positive integer m $\exists$ a unique field having p^m elements.

Proof: Follows from L7.1.3 & L 7.1.4

Note; The unique field having p^m elements is called the Galois field G F $[p^m]$