Project report on some basic topics of Galois Theory

Jishu Das
Indian Institute of Science Education and Research (IISER), Kolkata
E-mail Id- jd13ms109@iiserkol.ac.in

July 29, 2016

Abstract

This is an project report about some basic concepts in Galois Theory, which I studied under Dr. B. Sury of Indian Statistical Institute, Bangalore as a guide during the period of time from 18th May 2016 to 30 June 2016. I would like to thank Dr. B. Sury by giving his valuable time to guide me.

Signature of Guide
Dr. B. Sury

Signature of Student
Jishu Das

0.1 Finite fields

Definition 1 :- A field with finitely many elements is called a finite field.

Proposition 1 :- Let F be a finite field. Characteristics of F is always a prime number.

Proof :- F is a finite field, so for each $a \in F$ in the group $(F, +)$, $|F|.a = 0$. Which assures characteristics of F is finite. Let char$(F) = n$ for some $n \in N$. Suppose characteristics of F is a composite number. There exists $1 < n_1 < n$ and $1 < n_2 < n$ such that $n = n_1 n_2$. Let $a_0 \in F$ such that $n_1 a_0 \neq 0$. Such an a_0 exists since char$(F) = n$.
$\Rightarrow 0 = n.a_0 = (n_1 n_2).a_0 = a_0 n_2.a_0 + n_2.a_0 + ...$ (n_1 times) $+ n_2.a_0 = n_2.a_0.1 + n_2.a_0.1 + ...$ (n_1 times) $+ n_2.a_0.1 = n_2.a_0.(1+1...$ (n_1 times) $+1) = (n_2.a_0).(n_1.1)$

Note that $n_1.1 \neq 0$ if not then for $a \in F$, $n_1.a = n_1.(1 + 1 + ...$ (finite times) $+1) = n_1.1 + n_1.1 + ...$ (finite times) $+ n_1.1 = 0$, which implies $n =$char$(F) \leq n_1 < n$, a contradiction.
This shows that $n_1.a_0$ is a zero divisor, a contradiction since a field does not have any zero divisor.

Proposition 2 :- Let F be a field. Intersection of any family of subfields of F is a subfield of F.

Proof :- Easy.

Definition 2 :- A field containing no proper subfield is called a prime field. The intersection of all subfields of a field F is called the prime subfield of F. Indeed it follows from definition and proposition 2 that the prime subfield of F is a prime field.

Proposition 3 :- Let F be a finite field with characteristics p. The prime subfield of F is isomorphic to $\mathbb{F}_p$

Proof :- Consider $\phi : \mathbb{Z} \to F$ defined by $\phi(n) = n.1$. Clearly ϕ is an ring homomorphism. If $a \in p\mathbb{Z}$, then $a = mp$ for some $m \in \mathbb{Z}$. This would imply $\phi(a) = \phi(mp) = \phi(m).\phi(p.1) = 0$, i.e. $a \in \ker \phi$. Conversely let $b \in \ker \phi$, then $\phi(b) = 0$ i.e. $b.1 = 0$. Clearly $b = np$ for some $n \in \mathbb{Z}$ if not, then $b = np + m$ for some $m \in \{1, 2, ...p - 1\}$. Now $b.1 = (np + m).1$ which simplifies to $m.1 = 0$ which is a contradiction as char$(F) = p$. So $b \in p\mathbb{Z}$ and $\ker \phi = p\mathbb{Z}$. By first isomorphism theorem we have $\phi(\mathbb{Z})$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ as a ring. Since $\mathbb{Z}/p\mathbb{Z}$ is a field isomorphic to $\mathbb{F}_p$, $\phi(\mathbb{Z})$ is also a field. Let P be the prime subfield of F. P contains 0 and 1 and is closed under addition, so $n.1 \in P$ for all $n \in \mathbb{Z}$ and $\phi(\mathbb{Z}) \subset P$. $\phi(\mathbb{Z})$ is a subfield of F hence contains P. Therefore $P = \phi(\mathbb{Z})$ is isomorphic to $\mathbb{F}_p$.

Proposition 4:- Let F be a finite field. K be a subfield of F with $|K| = q$. Then $|K| = q^m$ where $m = [F : K]$.

Proof :- F is a vector space over K. Since F is finite $[F : K] = m$ for some

$m \in \mathbb{N}$. Let $\{a_1, a_2, ..., a_m\}$ be a basis for F over K. Therefore every $a \in F$ can be written uniquely as $a = \alpha_1.a_1 + ... + \alpha_m.a_m$ where $\alpha_1, ...\alpha_m \in K$. Each α_i ,for $i \in \{1, 2, ..., m\}$, has q many choices, for each $a \in F$ we have a unique combination of $\alpha_1, ..., \alpha_m$ and conversely. Therefore $|F| = |\{(\alpha_1, ..., \alpha_m) : \alpha_1, \alpha_2, ..., \alpha_m \in K\}| = q^m$.

Proposition 5 :- Let F be a finite field. $|F| = p^m$ with p being a prime number and $m = [F : \mathbb{F}_p]$.

Proof :- Let P be the prime subfield of F. From proposition 3, F_p can be regarded as a subfield of F. The assertion then follows from Proposition 4 by taking F for F and $\mathbb{F}_p$ for K.

Note 1:- We can also prove that for a finite field F, $|F| = p^m$ where p =char(F) and m is some natural number, by using group theoretic argument. Proof is as follows. $(F, +)$ is an abelian group with $|F| = n$ for some $n \in \mathbb{N}$. For a fixed $a \in F$ char$(F).a = 0$, also $n.a = 0$ along with char$(F) \leq n$ imply that char(F) divides n. char$(F) = p$, where p is a prime number by proposition 1. Since $p|n$ and p is a prime number, there exists a subgroup of order p by Cauchy's theorem for abelian groups. Suppose q be a prime number other than p that divides n, again there exists a subgroup H of order q. Since q is a prime number, H is cyclic, which means there exists $c \in F$ such that $H = (c)$. $|(c)| = q$, also $p.c = 0$, this implies q divides p. Hence $q = p$ a contradiction. Hence p is the only prime number that divides n, so $n = p^m$ where m is some natural number.

Proposition 6 :- Let F be a finite field. $(F^* = F - \{0\}, .)$ is a cyclic group.

Proof :- Let $|F^*| = m$ and exp(F^*)=n. Since there exists $a \in F^*$ such that order$(a) = n$. By Lagrange's Theorem n divides m, so $n \leq m$. Consider the polynomial $x^n - 1$ in F[x]. For all $a \in F^*$, $a^n = 1$ as n=exp(G) and $x^n - 1$ can have at most n roots, hence $m \leq n$. Therefore m=n=order(a), so $(a) = F^*$.

Lemma 1 :- Let H be a finite group of order n, 1 be the identity of H. If for all divisor d of n, the set $S_d = \{x \in H : x^d = 1\}$ has at most d elements, Then H is cyclic.

Proof :- Let d be a divisor of n. Suppose $a \in H$ has order d. $(a) = \{1, a, ..., a^{d-1}\}$ is the cyclic subgroup generated by a. Note that for $b \in (a)$ satisfy $b^d = 1$, so $(a) \subset S_d$. As $|(a)| = d$ and S_d can have at most d elements, we have $(a) = S_d$. All the elements of H of order d belongs to S_d and consequently in (a). (a) has $\phi(d)$ elements of order d. Also (a) has $\phi(d)$ no of elements of order d. Hence the number of elements of H of order d is 0 or $\phi(d)$.
Suppose for some d_0 dividing n has no elements of order d_0, then $n = \sum_{d|n} \phi(d) > \sum_{d|n, d \neq d_0} \phi(d)$ (as $\phi(d_0) > 0$) $= n$ (as there is no element in H of order d_0), a contradiction. Hence for each d dividing n has element of order d, in particular there is an element of order n. Hence H is cyclic.

Alternative Proof of Proposition 6 :- Let $H = F^*$, $n = |F| - 1$. Let $x \in F^*$ and

d divides n. Clearly $x^d = 1$ has at most d solutions in F^*, so F^* is cyclic.

Proposition 7 :- Let F be a finite field with $\mathrm{char}(F) = p$. Let $|F| = p^n$. Then
(i) F is a splitting field of the separable polynomial $x^{p^n} - x$ over $\mathbb{F}_p$. Thus $F/\mathbb{F}_p$ is Galois.
(ii) If σ is defined as $\sigma(a) = a^p$ for $a \in F$, then $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$
(iii) $(\sigma) = \mathrm{Gal}(F/\mathbb{F}_p)$.

Proof :- For $a = 0$, $a^{p^n} = a$ and for $a \in F^*$, $a^{|F^*|} = 1$ by Lagrange's theorem. So $a^{p^n-1} = 1$ or $a^{p^n} = a$. The elements of F are roots of $x^{p^n} - x$ and these are the possible roots of $x^{p^n} - x$ since $x^{p^n} - x$ can have at most p^n roots. Hence F is a splitting field over $\mathbb{F}_p$ and F is normal over $\mathbb{F}_p$. $(x^{p^n} - x)' = p^n.x^{p^n-1} - 1 = p.(p^{n-1}.x^{p^n-1}) - 1 = -1$ imply $\gcd(x^{p^n} - x, (x^{p^n} - x)') = 1$, so $x^{p^n} - x$ does not have repeated roots and $x^{p^n} - x$ is separable over $\mathbb{F}_p$. Thus $F/\mathbb{F}_p$ is Galois.

Let $\sigma : F \to F$ defined by $\sigma(a) = a^p$. Now for $a, b \in F$, $\sigma(ab) = (ab)^p = a^p.b^p = \sigma(a)\sigma(b)$ and
$\sigma(a+b) = (a+b)^p = a^p + C(p,1)a^{p-1}b + ... + C(p,p-1)ab^{p-1} + b^p = a^p + b^p = \sigma(a) + \sigma(b)$ (as $C(p,r)$ is a multiple of p for $r = 1, 2, .., r-1$ and $\mathrm{char}(F) = p$)
σ being a field homomorphism, is injective and is surjective as F is finite as well. For $c = 0$ $\sigma(0) = 0^p = 0$ and for $c \in \mathbb{F}_p^*$, by Lagrange's theorem $c^{p-1} = 1$ or $\sigma(c) = c^p = c$. Hence $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$.

$F/\mathbb{F}_p$ is Galois, so $|\mathrm{Gal}(F/\mathbb{F}_p)| = [F : \mathbb{F}_p] = n$. It is sufficient if we show that order of σ (say m) is n. Suppose for $1 \leq m < n$, $\sigma^m = I$ where I is the identity map on F. Then for $a \in F$, $\sigma^m(a) = I(a)$ or $a^{p^m} = a$. $x^{p^m} - x$ can have maximum p^m no of roots however we have $p^n (> p^m)$ no of roots which is a contradiction and we are done.

Proposition 8 :- Any two finite fields of same cardinality are isomorphic.

Proof :- Let F and L be two finite fields such that $|F| = |L| = p^n$ for some prime number p and natural number n. By proposition 7 Both F and L are splitting fields of $x^{p^n} - x$ over $\mathbb{F}_p$. By isomorphism extension theorem it follows that F and L are isomorphic.

Proposition 9 :- Let F and K be two finite fields and K be an extension of F. Then
(i) K/F is Galois.
(ii) Moreover if $\mathrm{char}(F) = p$, $|F| = p^n$ and $\tau : K \to K$ be such that $\tau(a) = a^{p^n}$, then $(\tau) = \mathrm{Gal}(K/F)$.

Proof :- $K/\mathbb{F}_p$ is Galois by proposition 7. Hence $K/\mathbb{F}_p$ is both normal and separable over $\mathbb{F}_p$. As $\mathbb{F}_p \subset F \subset K$, K is both normal and separable over F, equivalently K is Galois over F.

Clearly $\mathrm{Gal}(K/F) \leq \mathrm{Gal}(K/\mathbb{F}_p)$. Hence $\mathrm{Gal}(K/F)$ cyclic. Let $[K : F] = m = \mathrm{Gal}(K/F)$ (as K/F is Galois) , $[K : \mathbb{F}_p] = t = \mathrm{Gal}(K/\mathbb{F}_p)$ (as $K/\mathbb{F}_p$ is Galois). As m divides t, $\mathrm{Gal}(K/\mathbb{F}_p)$ has exactly one subgroup of order m, which is

$(\sigma_0^{\frac{t}{m}})$ where (σ_0) =Gal$(K/\mathbb{F}_p)$. $\sigma : K \to K$ defined by $\sigma(a) = a^p$ is a generator of Gal$(K/\mathbb{F}_p)$ from proposition 7. Thus Gal$(K/F) = (\sigma^{\frac{t}{m}}) = (\sigma^{[F:\mathbb{F}_p]})$ where $\frac{[K:\mathbb{F}_p]}{[K:F]} = [F : \mathbb{F}_p] = n$ (as $|F| = p^n$). Gal$(K/F) = (\sigma^n)$. By induction on n we can show that $\sigma^n(a) = a^{p^n} = \tau(a)$.

Proposition 10 :- Let N be an algebraic closure of $\mathbb{F}_p$. Then
(i) given any positive integer n, there is a unique subfield of N of order p^n.
(ii) If K and L are subfields of N of orders p^m and p^n respectively, then $K \subset L$ iff m divides n.
(iii) When this(ii) happens, L is Galois over K with Galois group generated by $\tau(a) = a^{p^m}$

Proof :- Consider a positive integer n. The set of roots of the polynomial (say S) $x^{p^n} - x$ over $\mathbb{F}_p$ belonging to N has p^n elements. Now if $\alpha, \beta, \beta^{-1} \in S$, then $\alpha^{p^n} = \alpha$ and $(\beta^{-1})^{p^n} = \beta^{-1}$, which implies $(\alpha\beta^{-1})^{p^n} = \alpha^{p^n}(\beta^{-1})^{p^n} = \alpha\beta^{-1}$ or equivalently $\alpha\beta^{-1} \in S$ and $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha^{p^n} + \beta^{p^n}$ (as char$(N) = p$) $= \alpha + \beta$ or equivalently $\alpha + \beta \in S$. S is a subfield of N with order p^n. This asserts that there exists a subfield of N with order p^n. Let $F \subset N$ be a field of order p^n. By proposition 7, F is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Hence F contains all the roots of $x^{p^n} - x$ or equivalently $S \subset F$. Every $a \in F$ satisfy $a^{p^n} - a = 0$, which implies $F \subset S$. Therefore there is a unique subfield of N of order p^n.

Let $K \subset L \subset N$. $[L : \mathbb{F}_p] = [L : K][K : \mathbb{F}_p]$, so $[K : \mathbb{F}_p]$ divides $[L : \mathbb{F}_p]$ or equivalently m divides n. Conversely let m divides n, if $b \in K$, then $b^{p^m} = b$ and $b^{p^n} = b^{p^{mk}}(t \in \mathbb{N}) = b^{(p^m)^t} = b^{p^m.p^m\ldots(ktimes).p^m} = ((((b^{p^m})^{p^m})^{p^m})^{\ldots(t-1times)})^{p^m} = b$ (as $b^{p^m} = b$). Hence $b \in L$ by (i) of proposition 10.

when proposition $10(ii)$ happens, we are done by taking L for K and K for F in proposition 9.

0.2 Galois groups

Definition 1:- Let F be a field. K be a field extension of F. A automorphism τ of K is said to be F-automorphism if τ fixes all the elements in F, i.e., $\tau(a) = a$ for all $a \in F$.
The Galois group K over F is denoted by Gal(K/F) and is defined as the set of all F-automorphisms of K.

Example 1:- Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{2})$. Let $\sigma \in$ Gal$(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, for $a, b \in \mathbb{Q}$, $\sigma(a + b\sqrt{2}) = a + b\sigma(\sqrt{2})$ (as σ fixes all elements in F, in particular a and b). σ is an homomorphism, so $(\sigma(\sqrt{2}))^2 = \sigma((\sqrt{2})^2) = \sigma(2) = 2$. We have two possible values $\sigma(\sqrt{2})$ one is $\sqrt{2}$ and $-\sqrt{2}$. Conversely, if $\sigma(a+b\sqrt{2}) = a+b\sqrt{2}$ or $a - b\sqrt{2}$, σ is F-automorphism of K. Hence Gal$(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\sigma_1, \sigma_2\}$, where $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ and $\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$.

Proposition 1 :- Let $K = F(X)$ be a field extension of F which is generated by X. If $\sigma, \tau \in$ Gal(K/F) with $\sigma|_X = \tau|_X$, then $\sigma = \tau$.

Proof :- Let $a \in K$. Then there exists $n \in \mathbb{N}$ and $a_1, a_2, ..., a_n \in X$ such that $a \in F(a_1, a_2, ..., a_n)$. So there exists $f, g \in F[x_1, x_2, ..., x_n]$ with $a = \frac{f(a_1,a_2,...,a_n)}{g(a_1,a_2,...,a_n)}$ and $g(a_1, a_2, ..., a_n) \neq 0$.
Let $f(x_1, x_2, ..., x_n) = \sum b_{i_1,i_2,...,i_n} x_1^{i_1} x_2^{i_2} ... x_n^{i_n}$ and
$g(x_1, x_2, ..., x_n) = \sum c_{i_1,i_2,...,i_n} x_1^{i_1} x_2^{i_2} ... x_n^{i_n}$ where each coefficient lies in F.

$\sigma(a) = \sum \frac{b_{i_1,i_2,...,i_n} \sigma(a_1)^{i_1} \sigma(a_2)^{i_2} ... \sigma(a_n)^{i_n}}{c_{i_1,i_2,...,i_n} \sigma(a_1)^{i_1} \sigma(a_2)^{i_2} ... \sigma(a_n)^{i_n}}$

$= \sum \frac{b_{i_1,i_2,...,i_n} \tau(a_1)^{i_1} \tau(a_2)^{i_2} ... \tau(a_n)^{i_n}}{c_{i_1,i_2,...,i_n} \tau(a_1)^{i_1} \tau(a_2)^{i_2} ... \tau(a_n)^{i_n}}$ (since σ and τ fix F , preserve addition and multiplication)$= \tau(a)$.

Proposition 2 :- Let K and L be two field extensions of F. $\tau : K \to L$ be an F-automorphism. Let $\alpha \in K$ be algebraic over F. If $f(x)$ is a polynomial over F with $f(\alpha) = 0$ then
(i) $f(\tau(\alpha)) = 0$. In particular τ permutes the roots of $\min(F, \alpha)$
(ii) $\min(F, \alpha) = \min(F, \tau(\alpha))$.

Proof :- Let $f(x) = a_0 + a_1 x + ... + a_n x^n$. $\tau(f(\alpha)) = \tau(0) = \sum_{i=0}^{n} \tau(a_i)(\tau(\alpha))^i = \sum_{i=0}^{n} a_i (\tau(\alpha))^i = 0$ (as τ is a F-homomorphism, $\tau(a_i) = a_i$, $\tau(0) = 0$)
Hence $f(\tau(\alpha)) = 0$
$\min(F, \tau(\alpha))$ divides $\min(F, \alpha)$ as $\min(F, \alpha)(\tau(\alpha)) = 0$. $\min(F, \alpha)$ is irreducible and is not a constant polynomial, which implies $\min(F, \alpha)$=$\min(F, \tau(\alpha))$.

Proposition 3 :- If $[K : F]$ is finite, then $\mathrm{Gal}(K/F)$ is finite.

Proof :- Let $\{\alpha_1, ..., \alpha_n\}$ be a basis of K over F (where $[K : F] = n$). The every element of K is a unique linear combination of $\alpha_1, ..., \alpha_n$ which implies $K \subset F(\alpha_1, ...\alpha_n)$. Further more $\alpha_1, ...\alpha_n \in K$ and $F \subset K$, so $F(\alpha_1, ...\alpha_n\} \subset K$. $K = F(\alpha_1, ...\alpha_n)$. By proposition 1 any F-automorphism of K is determined by where it sends α_i, $i \in \{1, 2, ..., n\}$. Let $\tau \in \mathrm{Gal}(K/F)$ and a fixed i, from proposition 2 it follows that τ permutes the roots $\min(F, \alpha_i)$. $\tau(\alpha_i)$ can take at most $\deg(\min(F, \alpha_i))$ values, also choices of i is finite, which shows that there are finitely choices of F-automorphism of K. Hence $\mathrm{Gal}(K/F)$ is finite.

0.3 Some solved questions

Q1 :- Let $n \in \mathbb{N}$. Show that K is a splitting field over F for a set $\{f_1, f_2, ..., f_n\}$ of polynomials in $F[x]$ if and only if K is a splitting field over F for the single polynomial $f_1 f_2 ... f_n$.

Proof :- Let $S = \{f_1, f_2..., f_n\}$ and X be the set of all roots of all polynomial in S. K be a splitting field over F for S. Then $K = F(X)$ and for each $i \in \{1, 2, ..., n\}$, f_i splits over F. i.e. $f_i = a_i \prod_{j(i)} (x - \alpha_{j(i)})$ where $j(i) \in \{1, ...\deg(f_i)\}$, $a_i \in F$ and $\alpha_{j(i)} \in K$. $f = f_1 f_2 ... f_n$ (say) $= \prod_i \prod_{j(i)} (x - \alpha_{j(i)})$. Since each factor of f is linear f splits over F.
If $\alpha \in K$ is a root of f then $f(\alpha) = 0$ i.e. there exists one k such that $f_k(\alpha) = 0$

where 0 is the additive identity of F which implies $\alpha \in X$. Conversely if $\alpha \in X$, for some k $f_k(\alpha) = 0$ which shows $f(\alpha) = 0$. This shows that the set of all roots of f(say Y) is equals to X. Hence $K = F(Y)$.
K is a splitting field of f.

Let K be a splitting field of f. let $f_i = a_i \prod_{j(i)}(x - \alpha_{j(i)})$ where $a_i \in F$ and $\alpha_{j(i)} \in L$, L is a splitting field of S. f_i divides f, $(x - \alpha_{j(i)})$ divides f i.e. $(x - \alpha_{j(i)})$ is a linear factor of f. Since f splits over K , it implies $\alpha_{j(i)} \in K$. f_i splits over K. Also set of all roots of f is same as X. Hence K is a splitting field of S.

Q2 :- Let K be a splitting field of a set S of polynomials over F. If L is a subfield of K containing F for which each $f \in S$ splits over L, Show that $L = K$.

Proof :- Let X be the set of all roots of all $f \in S$. Since K is a splitting field of F , $K = F(X)$. $f \in S$ splits over L, implies all roots of f lies in L i.e. $X \subset L$. $L(X) = \cup\{L(a_1, a_2, ..., a_n) : a_1, a_2..., a_n \in X\} = \cup L = L$ since $X \subset L$ we have $L(a_1, a_2..., a_n) = L$.
$K = F(X) \subset L(X) = L \subset K \Rightarrow L = K$

Q3 :- If $F \subseteq L \subseteq K$ are fields and if K is a splitting field of $S \subseteq F[x]$ over F , show that K is also a splitting field for S over L.

Proof :- Let $f \in S \subseteq F[x] \subseteq L[x]$, since K is a splitting field of S over F $f = a\prod_i(x - \alpha_i)$ for some $\alpha_i \in K$ and $a \in F \subseteq L$. Hence $f \in S \subseteq L[x]$ splits over K. Let X be the set of all roots of all $f \in S$, then $K = F(X)$. $f \in S$ splits over K this implies all roots of f lies in L i.e. $X \subset K$. $K = F(X) \subseteq L(X) \subseteq K(X) = K$ as $X \subset K$. $\Rightarrow K = L(X)$. K is a splitting field for S over L.

Q4(a) :- Let K be algebraically closed field extension of F. Show that algebraic closure of F in K defined as $\{a \in K : a \text{ is algebraic over } F\}$ is an algebraic closure of F.
(b) If $\mathbb{A} = \{a \in \mathbb{C} : a \text{ is algebraic over } \mathbb{Q}\}$, then assuming that $\mathbb{C}$ is algebraically closed, show that $\mathbb{A}$ is an algebraic closure of $\mathbb{Q}$.

Proof :- Let $\overline{F} = \{a \in K : a \text{ is algebraic over } F\}$. Clearly $F \subset \overline{F}$ since for $a \in F \subset K$, $f(x) = x - a \in F[x]$ with $f(a) = 0$. Let $a, b \in \overline{F}$. Then $F(a, b)$ being a finite extension of F, is algebraic over F. So $F(a, b) \subset L(a, b) = L$ and since $a + b, a - b, ab, a/b \in F(a, b)$, L is closed under the field operations. Let M be an proper algebraic extension. M is an algebraic extension since $\overline{F}$ is algebraic over F. Then there exists $c \in M$ $\overline{F}$ such that c is algebraic over F. $c \in K$ since $\min(c, F)$ splits over K as K is an algebraically closed field extension of F. This implies $c \in \overline{F}$, which is a contradiction. Hence $\overline{F}$ does not have any algebraic extension other than itself. Hence $\overline{F}$ is an algebraic closure of F.
(b) We are done by taking $F = \mathbb{Q}$ and $K = \mathbb{C}$ in 4(a).

Q5 :- Give an example of fields $F \subset K \subset L$ where L/K and K/L are normal but L/F is not normal.

Answer :- Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, $L = \sqrt[4]{2}$. $[K : F] = 2$ since $\min(\mathbb{Q},\sqrt{2}) = x^2 - 2$. $[L : F] = 4$ since $\min(\mathbb{Q}(\sqrt[4]{2}) = x^4 - 2$

Q6 :- Let $f(x)$ be an irreducible polynomial over F of degree n and let K be an field extension of F such that $[K : F] = m$. If $\gcd(n, m)$=1, then show that f is irreducible over K.

Proof :- If $n = 1$, then clearly f is irreducible over K. Without loss of generality we can assume that $n > 1$. Let α be a root of $f(x)$. Consider $K(\alpha)$ as an extension of K and $F(\alpha)$ as an extension of F. Note that $\deg(\min(c, F)) = n$ if not then $\deg(\min(\alpha, F)) < n$. $f(\alpha) = 0$ implies that $\min(\alpha, F)$ divides f. Hence $f(x)$ =$\min(\alpha, F)(x)g(x)$ where $g \in F(x)$ and $\deg(g) > 0$, which is a contradiction since f is irreducible over F. n =$\deg(\min(\alpha, F) = [F(\alpha) : F]$.
Now $[K(\alpha) : F] = [K(\alpha) : F(\alpha)][F(\alpha) : F] = [K(\alpha) : K][K : F]$
$\Rightarrow n[K(\alpha) : F(\alpha)] = m[K(\alpha) : K]$
$\Rightarrow [K(\alpha) : F(\alpha)] = \frac{m[K(\alpha):K]}{n}$
$\Rightarrow n$ divides $[K(\alpha) : K] = \deg(\min(\alpha, K)) = t$(say) ($n$ does not divide m if not 1 =$\gcd(m, n) = n > 1$ a contradiction) $\Rightarrow n \leq t$.

Suppose f is reducible over K then there exists some $f_1(x), f_2(x) \in K[x]$ such that $f(x) = f_1(x)f_2(x)$ and $0 <\deg(f_1)$, $\deg(f_2) < n$. Since $f(\alpha) = 0$ without loss of generality we can assume $f_1(\alpha) = 0$. This implies $\min(\alpha, K)$ divides f_1, hence $\deg(\alpha, K) \leq \deg(f_1) <\deg(f)$ =$\deg(\min(\alpha, F) \leq \deg(\min(\alpha, K)$
i.e. $t \leq \deg(f_1) < n \leq t$ a contradiction. Hence f is irreducible over K.

Q7 :-Show that $x^5 - 9x^3 + 15x + 6$ is irreducible over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Proof :- By taking 3 as a prime we see by Eisenstein's criterion that $x^5 - 9x^3 + 15x + 6$ is irreducible over $\mathbb{Q}$. $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2})] = 2[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$ since $\min(\sqrt{2}, \mathbb{Q}) = x^2 - 2$. $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$ (as $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$) $= 2$ since $\min(\sqrt{2} + \sqrt{3}, \mathbb{Q}(\sqrt{2}))(x) = (x - \sqrt{2})^2 - 3$.
$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : Q] = 4$. We are done by taking $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $f(x) = x^5 - 9x^3 + 15x + 6$ in Q6.