Galois Theory.

0. Introduction.

Field: A set where $+, -, \times, \div$ are just as in ordinary arithmetic.
E.g: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$. (In $\mathbb{Z}/6\mathbb{Z}$, $2 \neq 0$, $3 \neq 0$, but $2.3 = 0$ - not a field).

An extension of fields is just a pair of fields, one inside the other.
Eg: $\mathbb{Q} \hookrightarrow \mathbb{R}$, $\mathbb{Q} \hookrightarrow \mathbb{C}$, $\mathbb{R} \hookrightarrow \mathbb{C}$.
We write "L/K is an extension" to mean L, K are fields and $K \subseteq L$.
Galois Theory is the study of the symmetry of such a picture.

Definition: If L/K is an extension, then its automorphism group is
$$\mathrm{Aut}(L/K) = \{ s : s: L \to L \text{ is an automorphism}, \ s(x) = x \ \forall x \in K \}$$

Verify: $1 \in \mathrm{Aut}(L/K)$; $s, t \in \mathrm{Aut} \Rightarrow$ so do $s.t$ and s^{-1}; $s, t, u \in \mathrm{Aut} \Rightarrow s(tu) = (st)u$.
Just check: s^{-1}. s is a bijection, so $s^{-1}: L \to L$ exists as a map of sets.
Know $s(x+y) = s(x) + s(y)$, so $x + y = s^{-1}(s(x) + s(y))$. Now take arbitrary $X, Y \in L$. Since s is a bijection, $\exists\, x, y \in L$ with $X = s(x)$, $Y = s(y)$.
Equivalently, $s^{-1}(X) = x$, $s^{-1}(Y) = y$. Substitute: $s^{-1}(X) + s^{-1}(Y) = s^{-1}(X+Y)$. Etc.

Suppose L/K is an extension. Then the degree of L/K, written $[L:K]$, is just the dimension of L as a vector space over K. Say that L/K is finite if the degree is finite.
Galois Theory is the study of field extensions and their automorphism groups, especially when the extension is finite.

Definition: A number field is a finite extension of $\mathbb{Q}$

Galois Theory $\to$ algebraic number theory $\to$ Proof of Fermat's Last Theorem ...
Galois Theory $\to$ algebraic geometry, eg finite extensions of $\mathbb{C}(t)$ $\to$ Proof of Fermat's Last Theorem ...

($\mathbb{C}(t)$ = field of fractions of polynomial ring $\mathbb{C}[t]$).
A finite extension of $\mathbb{C}(t)$ is the same as the function field of a complex algebraic curve, or compact Riemannian surface.

Example: Given $\alpha \in \mathbb{C}$, $\mathbb{Q}(\alpha) = \left\{ \begin{array}{l} z \in \mathbb{C} : z \text{ can be written, not necessarily uniquely, as the} \\ \text{ratio of two polynomials in } \alpha, \text{ each have coefficients in } \mathbb{Q} \end{array} \right\}$

This is the subfield of $\mathbb{C}$ generated by α over $\mathbb{Q}$ - "$\mathbb{Q}$ adjoin α".

Questions: (i) What is $[\mathbb{Q}(\alpha) : \mathbb{Q}]$?, (ii) What is $\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})$?

Structure of $\mathrm{Aut}(L/K)$ as a group tells us in certain circumstances about the nature of the extension L/K from a purely field-theoretic point of view.

1. Field Extensions.

Definition / Proposition 1.1 - Suppose L/K is an extension and $\alpha \in L$. Then, there is a homomorphism $\rho: K[X] \to L$ such that $\rho(x) = \alpha$. $\rho(\Sigma a_i x^i) = \Sigma a_i \alpha^i$ for $a_i \in K$.
$K[X]$ is a PID, so $\ker \rho = (f)$, say.

(1.1.1): α is algebraic over K if $f \neq 0$. Then f is irreducible and is unique subject to being monic. In this case, $K(\alpha) = K[\alpha]$.
$K(\alpha) = \{ z \in L : z = p/q,\ p, q \text{ polynomials in } \alpha, \text{ coefficients in } K \}$
$K[\alpha] = \{ z \in L : z \text{ is a polynomial in } \alpha, \text{ coefficients in } K \}$
So, $K[\alpha] = \text{image}(\rho)$. Reason - if R is a PID, and $f \in R$ is irreducible, not a unit, not zero, then $R/(f)$ is a field.
This f is the minimal polynomial of α over K.

(1.1.2): $\alpha \in L$ is transcendental if it is not algebraic over K.

(1.1.3): α is separable if it is algebraic and its minimal polynomial $f \in K[X]$ has no repeated roots in any extension field whatsoever.

(1.1.4): L/K is algebraic if every $\alpha \in L$ is algebraic over K. L/K is finite if the dimension of L as a vector space over K is finite.

Exercise: L actually is a vector space over K.

If L/K is finite, we write $[L:K]$ for the degree of L/K.

Example: If $\alpha \in L$ then $K(\alpha)/K$ is finite $\Leftrightarrow$ α is algebraic over K.

In this case, if f is the minimal polynomial of α, then $[K(\alpha):K] = \deg f$.

Lemma 1.2: If $\deg f = n$, then $\{1, \alpha, .., \alpha^{n-1}\}$ is a K-basis of $K(\alpha)$

Proof: Recall that if α is algebraic, then $K(\alpha) = K[\alpha] \cong K[X]/(f)$.
If $f = \sum_{i=0}^{n} a_i x^i$, $a_n = 1$, then $\alpha^n = -\sum_{i=0}^{n-1} a_i \alpha^i$. Use this relation to show that every α^r $(r \geqslant n)$ can be written in terms of $\{1, \alpha, .., \alpha^{n-1}\}$.
So $\{1, \alpha, .., \alpha^{n-1}\}$ span $K(\alpha)$ over K.
L.I.: If $\sum_{i=0}^{n-1} \lambda_i \alpha^i = 0$ $(\lambda_i \in K)$, this is a polynomial in α of degree $< n$ - # to minimality of f.

If L/K is finite then it is algebraic, because if $\alpha \in L$, then $K \hookrightarrow K(\alpha) \hookrightarrow L$.
So $K(\alpha)$ is a sub-K-vector space of L. So $\dim_K K(\alpha)$ is finite, so α is algebraic.
Conversely, an algebraic extension need not be finite, eg: $K = \mathbb{Q}$, $L = \bigcup_{n \geqslant 0} \mathbb{Q}(2^{1/2^n})$
Then L/K is algebraic but not finite.

Theorem 1.3 (Tower Law): If M/L and L/K are extensions, then $[M:K] = [M:L].[L:K]$.
In particular, M/K finite $\Leftrightarrow$ M/L and L/K finite.

Proof: Say $\{a_i\}_{i \in I}$ is a K-basis of L, and $\{b_j\}_{j \in J}$ is an L-basis of M.
Claim $\{a_i b_j\}_{(i,j) \in I \times J}$ is a K-basis of M.

(i) Spanning M over K: Let $m \in M$, so $m = \sum_{j \in J} \lambda_j b_j$ ($\lambda_j \in L$, only finitely many $\lambda_j \neq 0$). Now, $\lambda_j = \sum_{i \in I} K_{ji} a_i$ ($K_{ji} \in K$, only finitely many $K_{ji} \neq 0$).
Then, $m = \sum_{i,j} K_{ji}(a_i b_j)$ – so they span.

(ii) L.I: if $\sum K_{ji} a_i b_j = 0$ then $\sum_j \left(\sum_i K_{ji} a_i \right) b_j = 0$.
Now, b_j are L.I., so $\sum_i K_{ji} a_i = 0 \ \forall j$, but a_i are LI, so $K_{ji} = 0 \ \forall i, j$.

2. Splitting Fields.

K a field, $f \in K[X]$. Then, $\exists$ extension L/K such that f splits completely in L, say $f = \prod_{i=1}^{n} (X - \alpha_i)$ and $L = K(\alpha_1, .., \alpha_n)$.
"All roots of f lie in L, and L is generated by those roots".

Theorem 2.1: Splitting fields exist and are unique up to isomorphism.
More precisely, if $\varphi : K \to K_1$ is an isomorphism, then φ extends to an isomorphism $K[X] \to K_1[X]$, ($\varphi(x) = x$), and if L/K is a splitting field for f, and L_1/K_1 is a splitting field for $\varphi(f)$, then $\varphi : K \to K_1$ can be extended to an isomorphism $\Phi : L \to L_1$. Φ is not necessarily unique.

$$\begin{tikzcd} K \arrow[r, "\varphi{,} \cong"] \arrow[d, hook] & K_1 \arrow[d, hook] \\ L \arrow[r, "\Phi{,} \cong"] & L_1 \end{tikzcd}$$

Proof: See "Rings and Modules."

3. Separable Extensions.

Definition: A finite extension L/K is separable if every $\alpha \in L$ is separable over K.
I.e, if the minimal polynomial f of α has no repeated roots in a splitting field of f.

Lemma 3.0: If L/K is finite and $\operatorname{char} K = 0$ then L/K is separable.
($\operatorname{char} K = 0$ means $\mathbb{Q} \hookrightarrow K$. The alternative is $\operatorname{char} K = p$, prime. Then, $\mathbb{F}_p \hookrightarrow K$)

Proof: Omitted.

So there are lots of separable extensions. Eg: $K = \mathbb{Q}$, $L =$ algebraic number field
$K = \mathbb{C}(t)$, $L = K(\sqrt{t^3+1})$

Lemma 3.1: Suppose L/K is a field extension and $F, G \in K[X]$. Suppose $H = \operatorname{hcf}(F, G)$ in $K[X]$. Then H is still the hcf in $L[X]$.

Proof: We have $F = H.a$, $G = H.b$, where $a, b \in K[X]$ and are coprime. ($K[X]$ a PID $\Rightarrow$ UFD).
Then, $1 = ap + bq$, some p, q in $K[X]$. So, $H = Hap + Hbq = Fp + Gq$.
Suppose $R \in L[X]$ divides F and G. So, F/R and G/R are polynomials.
$\therefore \frac{H}{R} = \frac{F}{R} p + \frac{G}{R} q \in L[X]$, so $R \mid H$. That is, $H = \operatorname{hcf}(F, G)$ in $L[X]$.

Theorem 3.2 (Theorem of the Primitive Element): Suppose L/K is finite and separable. Then, $\exists\, \theta \in L$ with $L = K(\theta)$. (θ is a primitive element, not necessarily unique).

Proof: If $\{\alpha_1, .., \alpha_n\}$ is a K-basis of L, then $L = K(\alpha_1, .., \alpha_n)$, ie, any element of L is a quotient of polynomials in $\alpha_1, .., \alpha_n$.

Suppose $L = K(\beta_1, .., \beta_m)$, where $\{\beta_1, .., \beta_m\}$ is arbitrary subject to generating L as a field over K. Put $M = K(\beta_1, .., \beta_{m-1})$, so M/K is separable.

If $m=1$, done, so assume $m>1$ and that the result is true for all separable extensions generated by $\leq m-1$ elements.

So, $M = K(\theta)$, by induction hypothesis. So $L = K(\theta, \beta_m)$, and it suffices to prove the theorem for $m=2$. Reduced problem to $L = K(\alpha, \beta)$.

Take $f, g \in K[x]$, minimal polynomials of α, β, respectively, and let M be the splitting field over L of fg.

f, g both factor as products of linear terms in $M[X]$, say, roots of f are $\alpha = \alpha_1, .., \alpha_r \in M$, roots of g are $\beta = \beta_1, .., \beta_s \in M$. (Note, $i \neq j \Rightarrow \beta_i \neq \beta_j$)

Assume K infinite (Finite case later).

Then, $\exists\, c \in K$ such that all elements $\alpha_i + c\beta_j \in M$ are distinct. ($c \neq \frac{\alpha_i - \alpha_k}{\beta_j - \beta_l}$, $\forall i, j, k, l$)

Put $\theta = \alpha + c\beta$, and define $F(X) = f(\theta - cX) \in K(\theta)[X]$

We have $g(\beta) = 0$ and $F(\beta) = f(\theta - c\beta) = f(\alpha) = 0$.

Take hcf H of g, F in $K(\theta)[X]$. Then H is the hcf in $M[X]$, by lemma 3.1.

β is a zero of H, since $g(\beta) = F(\beta) = 0$. The zeroes of g are $\beta = \beta_1, .., \beta_s$.

Suppose $\beta_i \neq \beta$. Then $F(\beta_i) = f(\theta - c\beta_i)$. We chose c so that $\theta - c\beta_i$ is not equal to any α_j. So $F(\beta_i) \neq 0$, so in M, β is the only common zero of g, F.

Now, g is separable (no repeated roots) and is a product of distinct linear terms, so H is a product of some subset of this set of linear terms. But $H \in K(\theta)[X]$, $\beta \in K(\theta)$, so $\alpha = \theta - c\beta \in K(\theta)$, as $H(X) = X - \beta$.

So, $L = K(\alpha, \beta) \subseteq K(\theta) \subseteq K(\alpha, \beta)$. (Have used only that β is separable).

Proposition 3.3: If char $K = 0$, then any algebraic extension L/K is separable.

Note: Given $f \in K[X]$, $f = \sum a_i X^i$, can define $df/dx = \sum i a_i X^{i-1} =: f'$

Lemma 3.4: If $f \in K[X]$ is separable, then f, f' are coprime in $M[X]$.

Proof: M/K, splitting field of f. Want to show $(f, f') = 1$ in $M[X]$.

$f = \prod (X - \alpha_i)$, $\alpha_i \in M$, so if $(f, f') \neq 1$, then $f'(\alpha_i) = 0$ some i. Let $f = (X - \alpha_i) g$, with $g = \prod_{j \neq i} (X - \alpha_j)$. Apply Liebnitz: $f' = g + (X - \alpha_i) g'$.

By assumption, $(X - \alpha_i) | f' \Rightarrow (X - \alpha_i) | g$, so α_i is a repeated root of f - ⨳.

Proof of Proposition 3.3: Suppose $\alpha \in L$, minimal polynomial $f \in K[X]$. Suppose $(f, f') \neq 1$.

f is irreducible, and $\deg f' < \deg f$. But, f irreducible $\Rightarrow$ f coprime to every non-zero polynomial of strictly less degree. So $f' = 0$, identically.

If $f = \sum_{n=1}^{N} a_n X^n$, then $f' = \sum n a_n X^{n-1}$, so $a_n = 0$ $\forall n$. In particular, $N = 0$ in K.

Ie, char $K = p > 0$, $p | N$. But char $K = 0$ - ⨳ (In char $K = p > 0$, have $f = \sum a_n X^{pn} \in K[X]$).

4. Galois Extensions - First Properties.

Definition: Suppose L is a field and G is a finite group of automorphisms of L. Define the field of invariants, $L^G = \{x \in L : s(x) = x \ \forall s \in G\}$
(Exercise: L^G is a subfield of L)

Definition 4.1: A field extension L/K is Galois if $\exists$ finite group G of automorphisms of L with $K = L^G$

Remark: If $G \subseteq Aut(L)$, then $G \subseteq Aut(L[X])$. ($s(X) = X \ \forall s \in G$; s acts on coefficients one by one)

Exercise: If $K = L^G$ then $K[X] = (L[X])^G$.

From now on, assume given $L, G, K = L^G$ as above.

Lemma 4.2: Every $\alpha \in L$ is algebraic over K, of degree at most $\#G$.
(Note: $\deg(\alpha) = \deg$ (minimal polynomial) $= [K(\alpha):K]$).

Proof: Put $f = \prod_{s \in G}(X - s(\alpha)) \in L[X]$. Any $t \in G$ just permutes the factors of f, since $t(X - s(\alpha)) = X - (ts)(\alpha)$. Hence f is G-invariant, so $f \in K[X]$.
$\deg f = \#G$, and $f(\alpha) = 0$, so minimal polynomial of α divides f.

Lemma 4.3: L/K is separable.

Proof: Suppose $\alpha \in L$. Consider the set $\{s(\alpha) : s \in G\}$. Suppose $\alpha = \alpha_1, \ldots, \alpha_r$ are the distinct members of this set. So the α_i are distinct and are permuted by G. So, $g = \prod_i (X - \alpha_i)$ is G-invariant, so $g \in K[X]$. Now, $\alpha_1 = \alpha$, so $g(\alpha) = 0$, so minimal polynomial f of α divides g. g has distinct roots, so f does too.

Lemma 4.4: L/K is finite.

Proof: By lemma 4.2, $[K(\alpha):K] \leq \#G$, $\forall \alpha$. Pick $\alpha \in L$ such that $[K(\alpha):K]$ is maximal. Assume $\beta \in L - K(\alpha)$. (If $\nexists \beta$, done). Now, $[K(\alpha,\beta):K(\alpha)] = \deg$ (minimal polynomial of β over $K(\alpha)$) $\leq \deg$ (minimal polynomial of β over K) $= [K(\beta):K] \leq \#G$.
So, by the Tower Law, $K(\alpha,\beta)/K$ is finite.
Now, by lemma 4.3, $K(\alpha,\beta)/K$ is separable, so $K(\alpha,\beta) = K(\theta)$, some θ.
Then, $[K(\alpha,\beta):K] \leq [K(\alpha):K]$ by maximality of α. But, $[K(\alpha,\beta):K(\alpha)] = \frac{[K(\alpha,\beta):K]}{[K(\alpha):K]} \leq 1$, by the Tower Law. So $K(\alpha,\beta) = K(\alpha)$. So $\nexists \beta \in L - K(\alpha)$, and $[L:K] = [K(\alpha):K] \leq \#G$.

Theorem 4.5: $[L:K] = \#G$.

Proof: By lemmas 4.3 and 4.4, L/K is separable and finite, so $L = K(\alpha)$, some α.
So, $f = \prod_{s \in G}(X - s(\alpha))$ is G-invariant, so $f \in K[X]$. So, the minimal polynomial g of α divides f since $f(\alpha) = 0$. So $[L:K] = \deg g \leq \deg f = \#G$. So, enough to show that f is irreducible, so $g = f$. So suppose $f = f_1 f_2$, $f_i \in K[X]$.
$L[X]$ a UFD, so $\exists$ decomposition $G = G_1 \cup G_2$ into disjoint subsets, with $f_i = \prod_{s \in G_i}(X - s(\alpha))$. Wlog, $1 \in G_1$. Choose $t \in G_2$. Since $f_i \in K[X]$, have $t(f_i) = f_i$.
However, $X - t(\alpha)$ is a factor of $t(f_1)$, but not of f_1. - #

Lemma 4.6: If $s_1, .., s_n \in Aut(L)$ are distinct, then they are L.I. over L.
That is, if $l_1, .., l_n \in L$ such that $\sum l_i s_i(x) = 0 \ \forall x \in L$, then $l_i = 0 \ \forall i$.

Proof: Suppose $\sum_{i=1}^{n} s_i l_i = 0$ – ⊛, not all $l_i = 0$. Wlog, this is a shortest relation. Then, all $l_i \neq 0$ and $n \geq 2$. Since $s_1 \neq s_2$, $\exists y \in L$ such that $s_1(y) \neq s_2(y)$
Now, $\sum l_i s_i(yx) = 0 \ \forall x \in L$, so $\sum (l_i s_i(y)) s_i(x) = 0 \ \forall x \in L$, so $\sum_{i=1}^{n} (l_i s_i(y)) s_i = 0$ – (1)
Multiply ⊛ by $s_1(y)$ to get $l_1 s_1(y) s_1 + l_2 s_1(y) s_2 + \dots = 0$ – (2).
(1) – (2): $\sum_{i=2}^{n} l_i (s_i(y) - s_1(y)) s_i = 0$ – a shorter relation, so all $l_i(s_i(y) - s_1(y)) = 0$.
In particular, $l_2 (\underbrace{s_2(y) - s_1(y)}_{\neq 0}) = 0$, so $l_2 = 0$ – ⨳

Proposition 4.7: Suppose that L/K is an arbitrary finite extension. Then, $Aut(L/K)$ is finite.

Proof: By Theorem 4.5, if $G \leq Aut(L/K)$ is finite then we have $K \subset L^G \subset L$.
So, $[L:K] \geq [L:L^G] = \# G$. So every finite subgroup of $Aut(L/K)$ is of order at most $[L:K]$. Say $[L:K] = n$ and $\{x_1, .., x_n\}$ is a K-basis of L
If the result is false, $\exists$ distinct $s_1, .., s_{n+1} \in Aut(L/K)$.
Consider the $n \times n$ matrix $A = (s_j(x_i))$, $1 \leq i, j \leq n$. If $\det A = 0$ then its columns are linearly dependent, so $\exists m_1, .., m_n \in L$, not all zero, with $\sum_j m_j s_j(x_i) = 0 \ \forall i$.
Any $x \in L$ is $x = \sum \lambda_i x_i$ $(\lambda_i \in K)$, so $\sum_j m_j s_j(x) = \sum_{j,i} m_j s_j(x_i) \lambda_i = \sum_i \lambda_i \sum_j m_j s_j(x_i) = 0$
– ⨳ to lemma 4.6. So $\det A \neq 0$.
Then, $\exists l_1, .., l_n \in L$ such that $\sum l_j s_j(x_i) = s_{n+1}(x_i) \ \forall i$, from $A \begin{bmatrix} l_1 \\ \vdots \\ l_n \end{bmatrix} = \begin{bmatrix} s_{n+1}(x_1) \\ \vdots \\ s_{n+1}(x_n) \end{bmatrix}$
So, $\sum_{j=1}^{n} l_j s_j - s_{n+1} = 0$ – ⨳ to lemma 4.6

Corollary 4.8: If $G \leq Aut\, L$ and $K = L^G$, then $G = Aut(L/K)$

Proof: Let $H = Aut(L/K)$. Then, H is finite, and $G \leq H$. By Theorem 4.5, $\# G = [L:K] = \# H \Rightarrow G = H$.

Remark: We have taken a 'topdown' approach, starting with L, G, then defining $K = L^G$.
In applications, we usually start with L/K and try to compute $Aut(L/K)$.

5. Galois Extensions and Separable Splitting Fields.

Theorem 5.1: (i) A finite extension is Galois iff it is separable and is the splitting field of some $f \in K[X]$.
(ii) L/K is Galois iff it is the splitting field of some separable $f \in K[X]$.

Proof: (i) ($\Leftarrow$) Assume L/K separable and is the splitting field of $f = f_1 \cdots f_r$, $f_i \in K[X]$ irreducible. So each f_i is separable, and we may assume they are distinct.
Use induction on $\deg f$. $\deg f = 1 \Leftrightarrow L = K$, and we are done. So assume $\deg f > 1$.
If $\deg f_i = 1 \ \forall i$ then $L = K$. So, suppose $\alpha \neq \beta$ are roots in L of f_1.
Then, $\exists$ isomorphism $\psi: K(\alpha) \to K(\beta)$, with $\alpha \mapsto \beta$, and $\lambda \mapsto \lambda \ \forall \lambda \in K$.
Then, $L/K(\alpha)$ is a splitting field for $g := \frac{f}{x-\alpha} \in K(\alpha)[X]$, and $L/K(\beta)$ is a splitting field for $h := \frac{f}{x-\beta} \in K(\beta)[X]$. By induction, these are Galois.
Set $H = Aut(L/K(\alpha))$, $G = Aut(L/K)$, and $K_1 = L^G$. Clearly $H \subset G$.
So, as $K(\alpha) = L^H$, have $K_1 \leq K(\alpha)$. Similarly, $K_1 \leq K(\beta)$.
Assume $K_1 \neq K$. Then, $[K(\alpha):K_1] < [K(\alpha):K] = \deg f_1$, so f_1 factorises over K_1.

Say $f_1 = p.q.r$, with p, q irreducible. Since f_1 is separable, p, q, r are pairwise coprime. So we may choose α to be a root of p, and β of q. Note that $K_1(\alpha) = K(\alpha)$ and $K_1(\beta) = K(\beta)$. Let $\Psi: L \to L$ be the extension of ψ. Then Ψ induces an isomorphism $K_1(\alpha) \to K_1(\beta)$ such that $\alpha \mapsto \beta$, but $\Psi(x) = x \ \forall x \in K_1$, since $\Psi \in Aut(L/K)$. Hence α, β have the same minimal polynomial over K_1 – #. So $K_1 = K$.

($\Rightarrow$) Suppose L/K is Galois. Then it is separable, by Lemma 4.3, so $L = K(\alpha)$. Let $\alpha_1, .., \alpha_r$ be the distinct elements of $\{s(\alpha): s \in G\}$, and set $f = \prod_i (x - \alpha_i)$. f is G-invariant, so $f \in K[X]$, $f(\alpha) = 0$, and f is separable, by construction. $L \supseteq K(\alpha_1, .., \alpha_r) \supseteq K(\alpha_1) = L$, hence equality throughout.
So $L = K$(roots of f) = splitting field for f.

(ii) Assume L/K is a splitting field for separable $f \in K[X]$. Say the roots of f are $\{\alpha_1, .., \alpha_r\}$, so $L = K(\alpha_1, .., \alpha_r)$. Set $L_i = K(\alpha_1, .., \alpha_i)$, so $L_i = L_{i-1}(\alpha_i)$. Each α_i is separable over K since f is, so α_i is separable over L_{i-1}. By corollary 3.7 (see handout: L/K, M/L separable $\Rightarrow$ M/K separable), have L/K separable, and so Galois by part (i).

6. The Fundamental Theorem of Galois Theory

Theorem 6.1: Assume L/K is a finite Galois extension. Let $G = Aut(L/K)$

(i) $\exists$ bijection between {subgroups of G} and {fields between K and L}, described as follows:

(a) Given subgroup H, the corresponding field is $H' = L^H = \{x \in L : h(x) = x \ \forall h \in H\}$,

(b) Given $K \subset M \subset L$, the corresponding subgroup is $M' = \{s \in G : s(x) = x \ \forall x \in M\}$

We have $H'' = H$, $M'' = M$.

(ii) This correspondance reverses inclusions: $H_1 \subseteq H_2 \Leftrightarrow H_1' \supseteq H_2'$, $M_1 \subseteq M_2 \Leftrightarrow M_1' \supseteq M_2'$.

(iii) If $H_1 \subset H_2$ are subgroups of G, and $M_i = H_i'$, then $[M_1 : M_2] = [H_2 : H_1]$.

(iv) Given any $H \subseteq G$, the extension L/H' is Galois, with $Aut(L/H') = H$.

(v) H is a normal subgroup of G iff H'/K is Galois.
If this happens then $Aut(H'/K) \cong G/H$, ie, $\exists$ group homomorphism $\varphi: G \to Aut(H'/K)$ such that (a) φ is surjective, (b) $\ker \varphi = H$.

Proof: (i) Suppose $K \subset M \subset L$. Let $H = M' \subset G$. Note that $H = Aut(L/M)$. [$\subseteq$ is clear. Any $s \in Aut(L/M)$ acts on L, so trivially on $M \supset K$, so $s \in Aut(L/K) \subset H$].
By Theorem 5.1, L/K is a separable splitting field, say for $f \in K[X]$.
So L/M is also a splitting field for $f \Rightarrow L/M$ is Galois. $\Rightarrow M = L^H = H' = M''$
Conversely, suppose $H \subset G$. Put $M = H'$. By definition, L/M is Galois, with $Aut(L/M) = H$, by Proposition 4.7. So $M' = \{s \in G : s \text{ fixes } M\} = H$, ie, $M' = H'' = H$.
So, the maps $H \mapsto H'$ and $M \mapsto M'$ are inverse to each other, so done.

(ii) Obvious.

(iii) Suppose $K \subset M_1 \subset M_2 \subset L$, $H_i = M_i'$; $H_1 \supset H_2$. L/M_i is Galois, group H_i. So, $\#H_i = [L : M_i]$, by Theorem 4.5. So, $[H_1 : H_2] = \#H_1 / \#H_2 = [L:M_1]/[L:M_2] = [M_2 : M_1]$, by the Tower law.

(iv) Follows from Corollary 4.8.

(v) Suppose $H \subset G$ and $M = H'$. Let $s \in G$, $x \in M$, $h \in H$. So, $s^{-1}hs(s^{-1}(x)) = s^{-1}(h(x)) = s^{-1}(x)$.
So $s^{-1}Hs$ acts trivially on $s^{-1}(M) \subset L$, so $s^{-1}Hs \subset (s^{-1}(M))'$.
But, $[s^{-1}(M) : K] = [M : K]$, so $s^{-1}Hs = (s^{-1}(M))'$.
Now, suppose H is normal, then $s^{-1}Hs = H$, so $s^{-1}(M) = M$, by part (i).
So, $\exists$ map $\varphi : G \to \mathrm{Aut}(M/K)$, given by $\varphi(s)(x) = s(x)$. Clear that φ is a homomorphism, and that $\ker \varphi = H$. And, φ is surjective, since: $\# \mathrm{Aut}(M/K) \leq [M:K] = [L:K]/[L:M] = \#G/\#H = \#(G/H)$.
Conversely, suppose M/K is Galois. Then, M/K is the splitting field of some separable $f \in K[X]$. Suppose that α is a root of f and $s \in G$. Then, $0 = s(0) = s(f(\alpha)) = f(s(\alpha))$, so that G permutes the roots of f. But M is generated over K by the roots of f, so G preserves M. Ie, $\exists$ homomorphism $\varphi : G \to \mathrm{Aut}(M/K)$, given by $\varphi(s)(x) = s(x)$. By definition, $\ker \varphi = M' = H$, so that $\#G/\#H = [L:M] = \#\mathrm{Aut}(M/K)$, so φ is surjective.

Corollary: Given L/K Galois, $\exists < \infty$ intermediate fields.
Proof: A finite group has $< \infty$ subgroups.

Notation: If L/K is Galois then one frequently writes $\mathrm{Gal}(L/K)$ for $\mathrm{Aut}(L/K)$

Theorem 6.2: Given M/K separable and finite, $\exists$ minimal Galois extension L/K with $L \supset M$. L is unique up to isomorphism.
Proof: Say $M = K(\theta)$. Let L = splitting field over M of the minimal polynomial of θ, say $f \in K[X]$. L/K is separable, and so Galois, by Theorem 5.1. Suppose L_1/K is Galois and $L_1 \supset M$.
Claim: f splits completely over L.
Proof: Let $G = \mathrm{Aut}(L_1/K)$. Suppose $\theta = \theta_1, .., \theta_r$ are the distinct elements of $\{s(\theta) \in L_1 : s \in G\}$. Put $g = \prod_i (X - \theta_i)$. Any $s \in G$ permutes the θ_i, so $g \in K[X]$.
Now, $g(\theta) = 0$, so $f | g$. But g splits completely over L_1, so f does too.
So L_1 contains a splitting field L_2 over M of f. So, by uniqueness of splitting fields, $\exists$ isomorphism $\varphi : L \to L_2$ with $\varphi(x) = x \ \forall x \in M$. But, L_1 minimal $\Rightarrow L_1 = L_2$.

Definition: This extension L/K is the Galois closure of M/K.

Theorem 6.3: If L/K is Galois and $f \in K[X]$ is irreducible, then f splits completely in L if it has a root in L.
Proof: Suppose $\alpha \in L$ is a root of f. Note that $f(s(\alpha)) = 0 \ \forall s \in G := \mathrm{Gal}(L/K)$.
Suppose $\beta_1, .., \beta_r$ are the distinct elements of $\{s(\alpha) : s \in G\}$. Put $g = \prod_i (X - \beta_i)$.
So, g is G-invariant, so $g \in K[X]$. Now, $g | f$ in $L[X]$, since every root of g is a root of f and g has no repeated roots. Hence, by lemma 3.1, $g | f$ in $K[X]$.
But f is irreducible, so $f = g$.

Definition: If $f \in K[X]$ is separable, then the Galois group of f is $\mathrm{Aut}(L/K)$, where L/K is a splitting field for f.

7. Composites.

Assume given subfields K, L of a field M. Then, the composite of K, L (in M), denoted KL, is the smallest subfield of M containing both K and L.
Concretely, if $K = k(\alpha_1, .., \alpha_r)$, $L = k(\beta_1, .., \beta_s)$, then $KL = k(\alpha_1, .., \alpha_r, \beta_1, .., \beta_s)$.

Example: $k = \mathbb{Q}$, $M = \mathbb{C}$. $K = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(3^{1/3})$, $KL = \mathbb{Q}(\sqrt{2}, 3^{1/3})$

Theorem 7.1: k, K, L, M as before. Assume L/k, K/k are finite Galois extensions, $G = \mathrm{Aut}(K/k)$, $H = \mathrm{Aut}(L/k)$. Then KL/k is Galois and its Galois group S is a subgroup of $G \times H$ such that each projection $pr_1 : S \to G$; $pr_1(g,h) = g$ and $pr_2 : S \to H$ is surjective.

Proof: Say K/k is a splitting field for $f \in k[x]$, and L/k a splitting field for $g \in K[x]$. Then, KL/k is a splitting field for fg. Moreover, K/k and L/k are separable, so KL/k is separable (Proposition 3.6). So KL/k is Galois by Theorem 5.1.
Let $S = \mathrm{Aut}(KL/k)$. By Theorem 6.1, K and L correspond to subgroups K', L' of S. Moreover, since K, L are Galois over k, Theorem 6.1 says that K', L' are normal subgroups of S, and $\exists$ surjective homomorphisms $\varphi : S \to \mathrm{Aut}(K/k) = G$, $\ker \varphi = K'$, and $\psi : S \to \mathrm{Aut}(L/k) = H$, $\ker \psi = L'$. So, get $(\varphi, \psi) : S \to G \times H$. Let $\omega = (\varphi, \psi)$.
By construction, $pr_1 \circ \omega = \varphi$, $pr_2 \circ \omega = \psi$ (surjective). Suppose $s \in \ker \omega$.
Then s acts trivially on K and L, so trivially on KL, ie $s = 1$. So ω injective.

Examples: (i) Suppose $n \in \mathbb{Z}$, not a square. Let $K = \mathbb{Q}(\sqrt{n})$. Minimal polynomial of $\sqrt{n}$ is $x^2 - n$.
So, $[K : \mathbb{Q}] = 2$. $K/\mathbb{Q}$ is separable and it is a splitting field for $x^2 - n$ since it contains both roots $\pm\sqrt{n}$. So $K/\mathbb{Q}$ is Galois. Let $G = \mathrm{Aut}(K/\mathbb{Q})$.
So, $\# G = 2$, so $G \cong C_2$. Say $G = \langle \sigma \rangle$, $\sigma^2 = 1$, $\sigma \neq 1$. σ is determined by its effect on $\sqrt{n}$. Say $\sigma(\sqrt{n}) = \theta$. Then $\theta^2 = \sigma(\sqrt{n}^2) = \sigma(n) = n$, since $\sigma(x) = x \ \forall x \in \mathbb{Q}$.
So $\theta = \pm\sqrt{n}$. But $\theta = \sqrt{n} \Rightarrow \sigma = 1$ - #. So $\sigma(\sqrt{n}) = -\sqrt{n}$, and $\sigma(\alpha + \beta\sqrt{n}) = \alpha - \beta\sqrt{n} \ \forall \alpha, \beta \in \mathbb{Q}$.

(ii) Suppose $p_1, .., p_r$ are distinct primes; let $K = \mathbb{Q}(\sqrt{p_1}, .., \sqrt{p_r})$.
Show that $K/\mathbb{Q}$ is Galois with group $(C_2)^r$ and that $K = \mathbb{Q}(\Sigma \sqrt{p_i})$
Use induction on r. $r = 1$, see example (i). Suppose $r \geq 2$, and that result holds for $p_1, .., p_{r-1}$. Let $K_i = \mathbb{Q}(\sqrt{p_1}, .., \sqrt{p_i})$, $G_i = \mathrm{Aut}(K_i/\mathbb{Q})$.
By Theorem 7.1, $K/\mathbb{Q}$ is Galois and $G \hookrightarrow \prod_{i=1}^{r} \mathrm{Aut}(\mathbb{Q}(\sqrt{p_i})/\mathbb{Q}) \cong (C_2)^r$ by part (i).
Have $\mathbb{Q} \hookrightarrow K_{r-1} \hookrightarrow K$, $[K_{r-1} : \mathbb{Q}] = 2^{r-1}$ (induction), $[K : K_{r-1}] \leq 2$.
By Theorem 7.1, $G \hookrightarrow G_{r-1} \times C_2$. Assume $[K : K_{r-1}] = 1$, ie, $\sqrt{p_r} \in K_{r-1}$.
So, $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{p_r}) \hookrightarrow K_{r-1}$. So, by Theorem 6.1, $\mathbb{Q}(\sqrt{p_r})$ corresponds to an index 2 subgroup of G_{r-1}. Next, count all index 2 subgroups of G_{r-1}.
Now, $C_2^{r-1} = \mathbb{F}_2^{r-1} = V$, say, an $(r-1)$-dimensional vector space over $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.
Then, index-2 subgroup = subspace of V of dimension $r-2$.
Then, {subspaces of V} $\leftrightarrow$ {subspaces of V^* of dimension 1}.
$V \hookleftarrow U \leftrightarrow U^\circ \hookrightarrow V^*$
$\#$(Lines in V^*) = $\#$(non-zero vectors in V^* modulo non-zero scalars) = $\#$(non-zero vectors in V^*)
$= 2^{r-1} - 1 = \#$(non-empty subsets of a set with $r-1$ elements)

Next, count subfields of K_{r-1} quadratic over $\mathbb{Q}$. Here are some: take any non-empty subset $\{j_1, .., j_s\}$ of $\{1, .., r-1\}$ and consider $\mathbb{Q}(\sqrt{p_{j_1} \cdots _{j_s}})$.
Suppose $\mathbb{Q}(\sqrt{p_{j_1} \cdots p_{j_s}}) = \mathbb{Q}(\sqrt{p_{k_1} \cdots p_{k_t}})$ and $\{j_1, .., j_s\} \neq \{k_1, .., k_t\}$.
Wlog, $k_t \notin \{j_1, .., j_s\}$.
Now, $G_{r-1} = \mathrm{Aut}(K_{r-1}/\mathbb{Q}) = \prod_{i=1}^{r-1} \mathrm{Aut}(\mathbb{Q}(\sqrt{p_i})/\mathbb{Q})$. So $\forall i$, $\exists\, \sigma_i \in G$ such that $\sigma_i(\sqrt{p_i}) = -\sqrt{p_i}$, by induction hypothesis, and $\sigma_i(\sqrt{p_j}) = \sqrt{p_j}$, $i \neq j$, $i, j \leq k-1$.
Then, $\sigma_{k_t}(\sqrt{p_{k_1} \cdots p_{k_t}}) = -\sqrt{p_{k_1} \cdots p_{k_t}}$, $\sigma_{k_t}(\sqrt{p_{j_1} \cdots p_{j_s}}) = \sqrt{p_{j_1} \cdots p_{j_s}}$.
So the fields are distinct, contrary to assumption. So $\nexists$ any more quadratic extensions of $\mathbb{Q}$ inside K_{r-1}.
But, $\mathbb{Q}(\sqrt{p_r}) \hookrightarrow K_{r-1}$, so $\mathbb{Q}(\sqrt{p_r}) = \mathbb{Q}(\sqrt{p_{j_1} \cdots p_{j_s}})$, some $\{j_1, .., j_s\}$.
Say $\mathrm{Gal}(\mathbb{Q}(\sqrt{p_r})/\mathbb{Q}) = \sigma_r$. We know $\sigma_r(\sqrt{p_r}) = -\sqrt{p_r}$, so $\sigma_r(\sqrt{p_{j_1} \cdots p_{j_s}}) = -\sqrt{p_{j_1} \cdots p_{j_s}}$.
Say $\sqrt{p_r} = \alpha + \beta\sqrt{p_{j_1} \cdots p_{j_s}}$. Apply σ_r: $-\sqrt{p_r} = \alpha - \beta\sqrt{p_{j_1} \cdots p_{j_s}}$.
So $\alpha = 0$ and $\beta = \sqrt{\frac{p_r}{p_{j_1} \cdots p_{j_s}}} \in \mathbb{Q}$ - #, by Pythagoras' argument.
So, $[K_r : K_{r-1}] = 2$, and $[K_r : \mathbb{Q}] = 2^r$, and so the map $G_r \hookrightarrow (C_2)^{r-1} \times C_r$ is an isomorphism.
If $\mathbb{Q}(\Sigma\sqrt{p_i}) \neq K$, then $\exists\, s \in G$, $s \neq 1$, with $s(\Sigma\sqrt{p_i}) = \Sigma\sqrt{p_i}$. But, $s(\sqrt{p_i}) = \pm\sqrt{p_i}$ $\forall i$, so $\exists\, j$ such that $s(\sqrt{p_j}) = -\sqrt{p_j}$. But if $x_1, .., x_r \in \mathbb{R}$, $x_i > 0$, cannot have $\Sigma x_i = \Sigma \pm x_i$ unless all signs are $+$.

Definition: Suppose L/K is an algebraic extension. Then, $\theta, \varphi \in L$ are conjugate w.r.t K, or K-conjugate if their minimal polynomials are the same (over K). Equivalently, $\exists$ a K-isomorphism $s: K(\theta) \to K(\varphi)$, $s(\theta) = \varphi$.

Note: The definition is independent of L.

Remark: If L/K is Galois, group G, then θ, φ conjugate $\Leftrightarrow$ $\exists\, t \in G$ with $t(\theta) = \varphi$.
Proof: $(\Rightarrow)$ $\exists\, t: K(\theta) \to K(\varphi)$, $\theta \to \varphi$. Now, L/K is a splitting field, say for $f \in K[X]$. So $L/K(\theta)$ is a splitting field for f, as is $L/K(\varphi)$.
By uniqueness of splitting fields, t extends to $t: L \to L$, thus $t \in G$.
$(\Leftarrow)$ Easy exercise.

Theorem 7.2: Suppose $L = K(\theta_1, .., \theta_r)$ and that L/K is finite and separable.
Then, L/K is Galois $\Leftrightarrow$ L contains every conjugate of each θ_i.
Proof: $(\Leftarrow)$ Assume L contains all conjugates of each θ_i. Say $f_i \in K[X]$ is the minimal polynomial of θ_i. By definition, L contains all root of $f = \prod f_i$. So L contain a splitting field L_1 of f. But all $\theta_i \in L_1$, so $L \subseteq L_1$, so $L = L_1$. So L is a separable splitting field over K. So it is Galois.
$(\Rightarrow)$ From Chapter 6.

Proposition 7.3: Assume K given and "conjugate" $\equiv$ "K-conjugate". Assume also all finite extensions of K are separable - true if char $K=0$ or if K is finite.

(i) Suppose $a_1,\dots,a_r$ and $b_1,\dots,b_s$ are the conjugates of a and b respectively. Then, the conjugates of $a+b$ are a subset of $\{a_i+b_j\}$. Similarly for $a-b$, ab, a/b.

(ii) If a_1, a_2 are conjugate and $f\in K[X]$, then $f(a_1)$ and $f(a_2)$ are conjugate.

(iii) Suppose $a_1,\dots,a_r$ are the conjugates of a, and suppose $\forall i$, a_n is the root $a_i^{1/n}$ of a_i. Suppose also given an n^{th} root $a^{1/n}$ of a. Then, the conjugates of $a^{1/n}$ form a subset of $\{\zeta^j a_i^{1/n}\}$, where ζ is a primitive n^{th} root of 1.

[Consider splitting field K_1/K of X^n-1, then inside K_1, the set of roots of 1 form a cyclic group. By definition, a primitive nth root of 1 is a generator.
Example: $K=\mathbb{Q}$. The nth roots of 1 are $(e^{2\pi i/n})^j$. $\zeta=e^{2\pi i/n}$ is one primitive root.]

Proof: (i) Pick a Galois extension L/K containing all a_i, b_j (say, a splitting field for f,g, the minimal polynomials of a,b). Then, the a_i, b_j are the images of a_i, b_j, respectively, under the elements of $G=\mathrm{Aut}(L/K)$. Then G permutes the linear factors of $F=\prod_{i,j}(x-(a_i+b_j))$, and $F(a+b)=0$. So, the minimal polynomial of $a+b$ divides F. So, the conjugates of $a+b$ form a subset of the set Σ of roots of F. But, $\Sigma=\{a_i+b_j\}$.

(ii) $\exists$ K-isomorphism $s: K(a_1)\to K(a_2)$, $s(a_1)=a_2$. So, $f(a_2)=f(s(a_1))=s(f(a_1))$, so $f(a_1)$ and $f(a_2)$ are conjugate.

(iii) Suppose θ is a conjugate of $a^{1/n}$. Then (by (ii) with $F(X)=X^n$), θ^n is a conjugate of a. So, $\theta^n=a_i$, some i. $\theta^n=(a_i^{1/n})^n$, so $\left(\frac{\theta}{a_i^{1/n}}\right)^n=1$, so $\frac{\theta}{a_i^{1/n}}=\zeta^j$, some j. So $\theta=\zeta^j a_i^{1/n}$.

Example: $\theta=\sqrt{(2+\sqrt{3})(3+\sqrt{6})}$, $K=\mathbb{Q}(\theta)$. Examine Galois properties of $K/\mathbb{Q}$.

$\theta^2=(2+\sqrt{2})(3+\sqrt{6})\in\mathbb{Q}(\sqrt{2},\sqrt{3})$. This is Galois over $\mathbb{Q}$, group $C_2\times C_2=\langle\sigma,\tau\rangle$, where $\sigma:\sqrt{2}\mapsto-\sqrt{2}$, $\sqrt{3}\mapsto\sqrt{3}$, and $\tau:\sqrt{2}\mapsto\sqrt{2}$, $\sqrt{3}\mapsto-\sqrt{3}$.

So, $\sigma(\theta^2)=(2-\sqrt{2})(3-\sqrt{6})\neq\theta^2$, $\tau(\theta^2)=(2+\sqrt{2})(3-\sqrt{6})\neq\theta^2$, $\sigma\tau(\theta^2)=(2-\sqrt{2})(3+\sqrt{6})\neq\theta^2$.

The proper subgroups of $C_2\times C_2$ are $\langle\sigma\rangle$, $\langle\tau\rangle$, $\langle\sigma\tau\rangle$, so $\mathbb{Q}(\theta^2)=\mathbb{Q}(\sqrt{2},\sqrt{3})$.

So, $\mathbb{Q}\xhookrightarrow{4}\mathbb{Q}(\sqrt{2},\sqrt{3})\xhookrightarrow{\le 2}\mathbb{Q}(\theta)$. Does $\theta\in\mathbb{Q}(\theta^2)$? If so, then $\theta\in\mathbb{Q}(\sqrt{2},\sqrt{3})$.

$\tau(\theta^2)/\theta^2=\frac{3-\sqrt{6}}{3+\sqrt{6}}=(\sqrt{3}-\sqrt{2})^2$, so $\frac{\tau(\theta)}{\theta}=\pm(\sqrt{3}-\sqrt{2})$. $\tau^2=1$. Apply τ: $\frac{\theta}{\tau(\theta)}=\pm(-\sqrt{3}-\sqrt{2})$.

Multiply: get $1=+(-1)$ – ※. So $\theta\notin\mathbb{Q}(\theta^2)$. So $[\mathbb{Q}(\theta):\mathbb{Q}]=8$.

Is $\mathbb{Q}(\theta)/\mathbb{Q}$ Galois? Enough to find whether $\mathbb{Q}(\theta)$ contains all conjugates of θ. By Proposition 7.3, conjugates of θ^2 are a subset of:

$\theta^2=(2+\sqrt{2})(3+\sqrt{6})$, $\varphi^2=(2+\sqrt{2})(3-\sqrt{6})$, $\psi^2=(2-\sqrt{2})(3+\sqrt{6})$, $\chi^2=(2-\sqrt{2})(3-\sqrt{6})$.

So, the conjugates of θ are a subset of $\{\pm\theta,\pm\varphi,\pm\psi,\pm\chi\}$. (+ve square roots)

Since $[\mathbb{Q}(\theta):\mathbb{Q}]=8$, all of these are in fact conjugates.

Then, $\theta/\varphi=\sqrt{\frac{3+\sqrt{6}}{3-\sqrt{6}}}=\frac{1}{\sqrt{3}-\sqrt{2}}$. But $\mathbb{Q}(\theta)\supseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$, so $\theta/\varphi\in\mathbb{Q}(\theta)$, so $\pm\varphi\in\mathbb{Q}(\theta)$.

$\theta/\psi=\sqrt{\frac{2+\sqrt{2}}{2-\sqrt{2}}}=\sqrt{\frac{(2+\sqrt{2})^2}{(2-\sqrt{2})(2+\sqrt{2})}}=\sqrt{\frac{(2+\sqrt{2})^2}{2}}=\sqrt{(\sqrt{2}+1)^2}=\sqrt{2}+1\in\mathbb{Q}(\theta)$. So $\pm\psi\in\mathbb{Q}(\theta)$

Finally, $\theta/\psi=\varphi/\chi$, so $\pm\chi\in\mathbb{Q}(\theta)$. So $\mathbb{Q}(\theta)/\mathbb{Q}$ is Galois.

Let $G=\mathrm{Aut}(\mathbb{Q}(\theta)/\mathbb{Q})$. What is G?

Fact: $\exists$ five groups of order 8: C_8, $C_4\times C_2$, $C_2\times C_2\times C_2$ (abelian), and D_8, Q_8.

Count the number of elements of order 2 in these groups.

C_8	$C_4 \times C_2$	$C_2 \times C_2 \times C_2$	D_8	Q_8
1	3	7	5	1

We have:

$$\begin{array}{l} \mathbb{Q}(\vartheta) = K \\ \quad \big| \; 2 \\ \mathbb{Q}(\vartheta^2) = \mathbb{Q}(\sqrt{2},\sqrt{3}) \\ \quad \big| \; 4 \quad \leftarrow \text{Galois.} \\ \mathbb{Q} \end{array}$$

Let $H = \mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \cong C_2 \times C_2$. Let $L = \mathbb{Q}(\sqrt{2},\sqrt{3})$. By the Fundamental Theorem of Galois Theory [FTGT], L' is of order 2 in G.

Moreover, since $L/\mathbb{Q}$ is Galois, group H, $\exists$ a surjective homomorphism $\pi: G \to H$ with kernel L'. So G cyclic $\Rightarrow$ H cyclic $-$ $\divideontimes$. So $G \not\cong C_8$.

Count $\{s \in G : s^2 = 1 \neq s\}$. $\exists$ 1 such in L. So suppose $s \in G$, $s^2 = 1 \neq s$.

Recall that $\pi(s)$ is "s acting on L", by construction of π.

$s(\vartheta)$ is a conjugate of ϑ. Suppose $s(\vartheta) = \varphi$, so $s(\vartheta^2) = \varphi^2$.

$s((2+\sqrt{2})(3+\sqrt{6})) = (2+\sqrt{2})(3-\sqrt{6})$.

Now, s sends $\sqrt{2} \mapsto \pm\sqrt{2}$, $\sqrt{3} \mapsto \pm\sqrt{3}$, so $s(\sqrt{2}) = \sqrt{2}$, $s(\sqrt{3}) = -\sqrt{3}$.

So, $\frac{\vartheta}{s(\vartheta)} = \frac{\vartheta}{\varphi} = \frac{1}{\sqrt{3}-\sqrt{2}}$. Apply s: $\frac{s(\vartheta)}{\vartheta} = \frac{-1}{\sqrt{3}+\sqrt{2}}$. Multiply, get $1 = -1$ $-$ $\divideontimes$.

We get a similar contradiction for $s(\vartheta) = -\varphi, \pm\psi, \pm\chi$ (similarly).

So $s(\vartheta) = \pm\vartheta$.

If $s(\vartheta) = \vartheta$, then $s = 1$, since $K = \mathbb{Q}(\vartheta)$. So $s(\vartheta) = -\vartheta$, so $s(\vartheta^2) = \vartheta^2$, so $\pi(s) = 1$.

So, $s \in L'$. So, G has a unique element of order 2, namely that lying in L'. So $G \cong Q_8$.

8. Symmetric Functions.

R, a commutative ring. S_n acts on $R[X_1, \dots, X_n]$ by permuting the X_i.

Definition: The ring of symmetric polynomials is the ring of invariants A^{S_n}.
The ith elementary symmetric polynomial is $e_i = \sum_{1 \le j_1 < \dots < j_i \le n} X_{j_1} \cdots X_{j_i}$.

Note: e_i depends on n. For example, $e_1 = X_1 + \dots + X_n$, $e_2 = X_1X_2 + X_1X_3 + \dots + X_{n-1}X_n$, $e_n = X_1 \cdots X_n$. Also, define $e_0 = 1$, and $e_i = 0$ for $i < 0$, $i > n$.

Lemma 8.1: T an indeterminate. Then, $\prod_{i=1}^{n} (T - X_i) = T^n - e_1 T^{n-1} + \dots + (-1)^n e_n = \sum_i (-1)^i e_i T^{n-i}$.

Proof: Obvious.

Theorem 8.2 (Newton): $A^{S_n} = R[e_1, \dots, e_n]$, and is isomorphic to a polynomial ring in n variables. That is, any symmetric polynomial can be written uniquely as a polynomial in the e_i, with coefficients in R.

Proof: Define the lexicographical order on the set of monomials $X_1^{m_1} \cdots X_n^{m_n} = \underline{X}^{\underline{m}}$, as follows: $\underline{X}^{\underline{m}} > \underline{X}^{\underline{p}}$ if $\exists$ index i such that $m_1 = p_1, \dots, m_{i-1} = p_{i-1}$, $m_i > p_i$.

This is a total ordering.

Suppose $f \in A^{S_n}$. We have $f = \sum_d f_d$, where f_d is homogeneous of degree d. Enough to show that $f_d \in R[e_1, \dots, e_n]$, ie, we may assume that f is homogeneous and $d \neq 0$.

Pick the largest monomial M appearing in f, say with coefficient $r \in R$.

Say $M = X_1^{m_1} \cdots X_n^{m_n}$. Note that, as f symmetric, we have $X_{\sigma(1)}^{m_1} \cdots X_{\sigma(n)}^{m_n}$ appearing in f $\forall\, \sigma \in S_n$. So, $m_1 \geq m_2 \geq \cdots \geq m_n$. Consider $E = e_1^{m_1-m_2} \cdots e_{n-1}^{m_{n-1}-m_n} e_n^{m_n}$. Note that the largest monomial in E is M, and appears in E with coefficient 1.

[Proof of this: largest monomial in e_i is $X_1 \cdots X_i$, with coefficient 1, so largest monomial in $e_i^{m_i-m_{i+1}}$ is $(X_1 \cdots X_i)^{m_i - m_{i+1}}$, again with coefficient 1. And, $(X_1)^{m_1-m_2}(X_1X_2)^{m_2-m_3} \cdots (X_1 \cdots X_{n-1})^{m_{n-1}-m_n}(X_1 \cdots X_n)^{m_n} = M$.]

So, in $F - rE$, every monomial is $< M$. But $F-rE$ is a symmetric polynomial, so $F - rE \in R[e_1, \dots, e_n]$, by induction.

[To be precise, at the start suppose F is a counterexample with minimal M. Then, $F - rE$ is a smaller counterexample.]

So $F \in R[\underline{e}]$, so $A^{S_n} \subseteq R[\underline{e}] \subseteq A^{S_n}$.

Now to prove the e_i are independent. Suppose $P(e_1, \dots, e_n) = 0$, with P a non-vacuous polynomial. By induction on n, if we set $X_n = 0$, then $P \equiv 0$. Then, $P = QX_n$, with $Q \in R[X_1, \dots, X_n]$. P is symmetric, so if divisible by X_n, then divisible by all X_i. So $P = Ue_n$.

Then, $U(e_1, \dots, e_n) = 0$, a polynomial of smaller degree. Having chosen P of minimal degree, get $U = 0$, hence $P = 0$. So the e_i are independent.

Definition: $\delta = \delta_n = \prod_{i>j}(X_i - X_j)$, and $\Delta = \Delta_n = \delta^2$.

Proposition 8.3: (i) (Vandermonde). $\delta = \det\begin{pmatrix} 1 & \cdots & 1 \\ X_1 & \cdots & X_n \\ \vdots & & \vdots \\ X_1^{n-1} & \cdots & X_n^{n-1} \end{pmatrix}$

(ii) $\forall\, s \in S_n$, $s(\delta) = \pm\delta$

(iii) Δ is a symmetric polynomial.

(iv) Δ is a function of $e_1, \dots, e_n$. By definition, Δ is the discriminant of $\sum (-1)^i e_i T^{n-i}$, as a polynomial in T. Then,
$\Delta = 0 \iff$ polynomial has repeated roots.

Proof: (i) Enough to prove the identity in $\mathbb{Z}[X_1, \dots, X_n]$. Call the determinant d.
This ring is a UFD, and each $X_i - X_j$ is irreducible in it.
If we set $X_i = X_j$, $(i \neq j)$, then $d = 0$, so d is divisible by $X_i - X_j$.
Strictly speaking, we have a homomorphism, $\varphi: \mathbb{Z}[X_1, \dots, X_n] \to \mathbb{Z}[X_1, \dots, \hat{X_j}, \dots X_n] =: B$, given by $\varphi(X_k) = X_k$ if $k \neq j$, $\varphi(X_j) = X_i$. φ is surjective. $\ker\varphi = (X_i - X_j)$.
Suppose $f \in \ker\varphi$. $f \in B[X_j]$, so $\frac{f}{X_i - X_j} = q$ remainder r.
$f = q(X_i - X_j) + r$, where $r \in B$ (Gauss). Then, $0 = \varphi(f) = \varphi(r)$, so $r = 0$.
So, $(X_i - X_j) \mid d$ $\forall\, i, j$. The $X_i - X_j$ are coprime, subject to $i > j$, so UFD $\Rightarrow \prod_{i>j}(X_i - X_j) \mid d$. Ie, $\delta \mid d$.
By inspection, $\deg(\delta) = \binom{n}{2}$ and $\deg(d) = 0 + 1 + \cdots + (n-1) = \binom{n}{2}$
Hence $\delta = dN$, some $N \in \mathbb{Z}$. To compute N, compare coefficients of $M := X_n^{n-1} \cdots X_3^2 X_2$. In δ, M is the least monomial appearing. It appears with coefficient 1, since every $X_i - X_j$ contributing to M gives $\pm$ to the coefficient. In d, M comes from the product of the diagonal entries, so with coefficient 1.
So $N = 1$.

(ii) Let $s \in S_n$. $s(X_i - X_j) = X_{s(i)} - X_{s(j)}$. So s permutes the factors of δ, up to sign. So $s(\delta) = \pm\delta$

(iii) $s(\delta) = \pm\delta$, so $s(\delta^2) = \delta^2$, so $s(\Delta) = \Delta$, ie Δ is symmetric.

(iv) Δ is a polynomial function of the coefficients of a degree n polynomial $f(T)$. $\Delta = 0 \iff X_i = X_j$, some $i, j \iff f$ has a repeated root.

Remark: Any $s \in S_n$ can be written as a product of transpositions (in many ways). From $s(\delta) = \pm\delta$, we get a homomorphism, $\text{sign}: S_n \to \{\pm 1\} \cong C_2$.

By definition, $s(\delta) = \text{sign}(s).\delta$. Check this is a homomorphism:

$\text{sign}(st)\,\delta = (st)(\delta) = s(t(\delta)) = s(\text{sign}(t).\delta) = \text{sign}(t).(s(\delta)) = \text{sign}(t)\text{sign}(s).\delta$.

Claim: $\text{sign}(\tau) = -1 \quad \forall$ transpositions τ.

Proof: Check for $\tau = (12)$. (i) $(X_2 - X_1) \mapsto (X_1 - X_2)$, (ii) $(X_k - X_1) \mapsto (X_k - X_2)$, $k \geq 3$.
(iii) $(X_k - X_2) \mapsto (X_k - X_1)$, $k \geq 3$, (iv) $(X_k - X_l) \mapsto (X_k - X_l)$ $k > l \geq 3$,
τ changes sign in (i), swaps (ii) and (iii), and fixes everything else. So $\text{sign}(\tau) = -1$.

So sign is a homomorphism, surjective, onto $\{\pm 1\}$.

So, $\ker(\text{sign})$ is a subgroup of S_n of index 2. Notice that if $s \in S_n$ and $s = \tau_1 \ldots \tau_r = \tilde{\tau}_1 \cdots \tilde{\tau}_q$ with $\{\tau_i, \tilde{\tau}_j\}$ transpositions, then $\text{sign}(s) = (\text{sign}(\tau_1)) \cdots (\text{sign}(\tau_r)) = (-1)^r$.
And, $\text{sign}(s) = (\text{sign}(\tilde{\tau}_1)) \cdots (\text{sign}(\tilde{\tau}_q)) = (-1)^q$. So $q \equiv r \pmod 2$.
So, $\ker(\text{sign})$ consists of those $s \in S_n$ that can be written as a product of an even number of transpositions.

Definition: $A_n = \{s \in S_n : s \text{ is a product of an even number of transpositions}\}$.
So, $A_n = \ker(\text{sign})$, a subgroup of S_n of index 2 - a well-defined subset.

Computing Δ.

Lemma 8.4: Suppose $f, g \in K[X]$, $\deg f = n$. Then they have a common factor (over some splitting field) iff $\exists$ an equation $pf = qg$, where $p, q \in K[X]$, non-zero, with $\deg p < \deg g$, $\deg q < n$.

Proof: $(\Leftarrow)$ Extend to a splitting field of $pqfg$, then factorise both sides completely. f has n linear factors and $\deg q < n$, so ≥ 1 of the factors divides g.

$(\Rightarrow)$ If $\varphi | f$ and $\varphi | g$, take $p = g/\varphi$, $q = f/\varphi$.

Definition: Suppose $f = a_n X^n + \cdots + a_0$, $g = b_m X^m + \cdots + b_0$. Then, the resultant of f, g, $\text{Res}(f, g)$, is the $(n+m) \times (n+m)$ determinant:

$$\begin{vmatrix} a_n & \cdots & a_0 & & & 0 \\ & a_n & \cdots & a_0 & & \\ 0 & & \ddots & & \ddots & \\ & & & a_n & \cdots & a_0 \\ b_m & \cdots & b_0 & & & 0 \\ & \ddots & & \ddots & & \\ 0 & & b_m & & \cdots & b_0 \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} n \text{ rows.} \end{matrix}$$

Example: $n = 3$, $m = 2$:

$$\begin{vmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 & 0 \\ 0 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & b_2 & b_1 & b_0 \end{vmatrix}$$

Proposition 8.5: If f, g have a common factor, then $\mathrm{Res}(f,g) = 0$.

Proof: By Lemma 8.4, have $pf = qg$. Write $p = c_{m-1}X^{m-1} + \dots + c_0$, $q = d_{n-1}X^{n-1} + \dots + d_0$

Expand pf, qg, and compare coefficients of $X^{m+n-1}, \dots, 1$.

Get:
$$\begin{aligned} c_{m-1}a_n &= d_{n-1}b_m \\ c_{m-1}a_{n-1} + c_{m-2}a_n &= d_{n-1}b_{m-1} + d_{n-2}b_m \\ &\vdots \\ c_1a_0 + c_0a_1 &= d_1b_0 + d_0b_1 \\ c_0a_0 &= d_0b_0 \end{aligned}$$

Write as: $\begin{pmatrix} c_{m-1} \\ \vdots \\ c_0 \\ -d_{n-1} \\ \vdots \\ -d_0 \end{pmatrix}^T \begin{pmatrix} \text{Matrix} \\ M \end{pmatrix} = \underline{0}$

By inspection, M is the matrix above. By assumption, vector $\neq \underline{0}$, so $\det M = 0$.

Notation: Suppose $f(T) = a_n(T-x_1)\cdots(T-x_n)$, $g(T) = b_m(T-y_1)\cdots(T-y_m)$.

Write $S = a_n^m b_m^n \prod_{i,k}(x_i - y_k)$.

Lemma 8.6: $S = a_n^m \prod_{i=1}^n g(x_i) = (-1)^{mn} b_m^n \prod_{k=1}^m f(y_k)$

Proof: $g(x_i) = b_m \prod_k (x_i - y_k)$, so $\prod_i g(x_i) = b_m^n \prod_{i,k}(x_i - y_k)$. Multiply by $a_n^m \Rightarrow a_n^m \prod_i g(x_i) = S$.

Similarly, $f(y_k) = a_n \prod_i (y_k - x_i) = (-1)^n a_n \prod_i (x_i - y_k)$

So, $\prod_k f(y_k) = (-1)^{mn} a_n^m \prod_{i,k}(x_i - y_k)$. Multiply by $(-1)^{mn} b_m^n \Rightarrow (-1)^{mn} b_m^n \prod_k f(y_k) = S$.

Proposition 8.7: Let $R = \mathrm{Res}(f,g)$. Then, $S = R$.

Proof: Enough to prove this when a_n, b_m, T, x_i, y_k are independent indeterminates over field K. By Proposition 8.5, $R = 0$ when $x_i - y_k = 0$, so $(x_i - y_k) \mid R$.

So, $S \mid R$, up to "a's and b's". So, to prove $S = R$, enough to show that $a_n^m b_0^n$ has coefficient 1 in each.

In R: $a_n^m b_0^n$ comes just from the leading diagonal $\Rightarrow$ coefficient 1.

In S: b_0 = constant term of $g = b_m(-1)^m y_1 \cdots y_m$. $S = a_n^m b_m^n \prod_{i=1}^n \left(\prod_{k=1}^m (x_i - y_k) \right)$. So, in S, get term $a_n^m b_m^n ((-1)^m y_1 \cdots y_m)^n = a_n^m (b_m (-1)^m y_1 \cdots y_m)^n$, with term $a_n^m b_0^n$, coefficient 1.

So $S = R$.

Corollary 8.8: If $R = 0$, then f, g have a common factor.

Proof: $S = 0$ by Proposition 8.7, and then, by definition of S, some x_i = some y_k.

Proposition 8.9: $\mathrm{Res}(f, f') = (-1)^{\binom{n}{2}} . a_n^{2n-1} . \Delta(f)$.

Proof: $f(T) = a_n T^n + \dots + a_0 = a_n \prod_i (T - x_i)$. Let $R = \mathrm{Res}(f, f')$, $g = f'$. So, $m = n-1$.

Then, $R = S = a_n^{n-1} \prod_k f'(x_k)$. By product rule, $f'(T) = a_n \sum_j \prod_{i \neq j} (T - x_i)$

So, $f'(x_k) = a_n \prod_{i \neq k} (x_k - x_i)$. So, $R = a_n^{2n-1} \prod_k \prod_{i \neq k} (x_k - x_i) = a_n^{2n-1} \left(\prod_{k > i} (x_k - x_i) \right)^2 . (-1)^m$

where m = number of entries in $n \times n$ strictly above diagonal $= \binom{n}{2}$. So, $R = (-1)^{\binom{n}{2}} a_n^{2n-1} \Delta$.

Corollary 8.10: Discriminant $(X^3 + pX + q) = -4p^3 - 27q^2$

Proof: $\mathrm{Res}(f, f') = \begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix} = \begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 0 & 0 & -2p & -3q & 0 \\ 0 & 0 & 0 & -2p & -3q \\ 0 & 0 & 3 & 0 & p \end{vmatrix}$ $= -2p(-2p^2) + 3q(9q)$

$= 4p^3 + 27q^2 = (-1)\Delta$.

Compute disc.$(X^n + pX + q)$ similarly. (Inferior method of computation on example sheet 1).

9. Galois Groups Of Equations.

K a field. $f = f_1 \cdots f_r \in K[x]$, f_i irreducible and distinct, so no repeated roots.
Let L = splitting field for f over K. L/K is Galois.

Definition: Galois Group of f, $\mathrm{Gal}(f) = \mathrm{Aut}(L/K)$.

Write $G = \mathrm{Gal}(f)$. What is G? Say $\deg f_i = n_i$, $\deg f = n = \Sigma n_i$.

Proposition 9.1: $G \hookrightarrow S_{n_1} \times \cdots \times S_{n_r}$, and G projects on to a transitive group of each S_{n_i}.
In particular, if f is irreducible then $G \hookrightarrow S_n$ and is a transitive subgroup. G permutes the roots of f.

Proof: Follows from last part. Assume f irreducible. Suppose $\alpha, \beta \in L$ are roots of f.
G transitive $\Rightarrow \exists\, s \in G$ with $s(\alpha) = \beta$. Proof: $\exists$ isomorphism $\varphi: K(\alpha) \to K(\beta)$ where $\varphi(\alpha) = \beta$, because L is a splitting field for f over $K(\alpha)$ and $K(\beta)$.
Uniqueness of splitting fields $\Rightarrow \exists$ isomorphism $\Psi: L \to L$, extending φ.
Then $\Psi \in \mathrm{Aut}(L/K)$ and $\Psi(\alpha) = \beta$. Take $s = \Psi$. So done for f irreducible.
General case: Let L_i = splitting field for f_i over K. Then, L = composite of all L_i.
So, $\mathrm{Aut}(L/K) \hookrightarrow \mathrm{Aut}(L_1/K) \times \cdots \times \mathrm{Aut}(L_r/K)$, and maps surjectively onto each factor. Each $\mathrm{Aut}(L_i/K)$ permutes roots of f transitively.
Conversely, if G is transitive in S_n, then f is irreducible.

What is G as a subgroup of S_n? In fact $G \hookrightarrow S_n$ is defined up to conjugacy.
Given $\sigma \in S_n$, cannot distinguish between G and $\sigma^{-1} G \sigma$. So, what is G, up to conjugacy?

$n = 2$: Only transitive subgroup of S_2 is S_2, ie, given quadratic $f \in K[x]$ (with char $K \neq 2$) then either f factor (then $G = 1$) or it doesn't, then L/K is quadratic and $G = S_2 \cong C_2$.

$n = 3$: The transitive subgroups of S_3 are S_3 and $A_3 \cong C_3$.
(Blanket assumption - all finite extensions of K are separable).
Given irreducible cubic $f \in K[x]$, $G = A_3$ or S_3.
$G = A_3 \Leftrightarrow \mathrm{disc}(f)$ is a square in K. $\mathrm{disc}(f) = (-1)^{\binom{n}{2}} \mathrm{Res}(f, f') = -\mathrm{Res}(f, f')$, $n = 3$.

Proposition 9.2: Given separable $f \in K[x]$, $\deg f = n$, $\mathrm{Gal}(f) \leq A_n$ iff $\mathrm{disc}(f)$ is a square in K. (Assume char $K = 0$)

Proof: $\mathrm{disc}(f) = \Delta(f) = \delta^2$, where $\delta = \prod_{i>j}(x_i - x_j) \in L$, where $x_1, \ldots, x_n$ are roots of f.
Let $s \in G = \mathrm{Gal}(f) \leq S_n$. We know $s(\delta) = \mathrm{sign}(s).\delta$.
So, $G \leq A_n \Leftrightarrow s(\delta) = \delta\ \forall s \in G$, $\Leftrightarrow \delta \in L^G = K \Leftrightarrow \Delta$ is a square in K.

Example: $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$. $\Delta = -27q^2 - 4p^3 = -27 - 4(-3)^3 = -27 + 4.27 = 81 = 9^2$.
So $Gal(f) \subseteq A_3 \Rightarrow Gal(f) = A_3$ or $\{1\}$
$Gal(f) = 1$ iff f factors completely $\Rightarrow f$ has $\mathbb{Q}$-root $\Rightarrow f$ has $\mathbb{Z}$-root (by Gauss).
Check $X = 0, \pm 1, \pm 2$ - no. $f' = 3X^2 - 3 > 0$ if $|X| > 1 \Rightarrow$ no $\mathbb{Z}$-root. So $Gal(f) = A_3$.

$n=4$: Transitive subgroups of S_4 are: $S_4, A_4, C_2 \times C_2$ (normal), and C_4, D_8 (3 conjugate copies).
Let $V = \{1, (12)(34), (13)(24), (14)(23)\}$. S_4 acts on $V - \{1\}$ by conjugation. So have
$\pi: S_4 \to S_3$ given by this permutation action. $S_4 \to S_3$; $A_4 \to A_3$; $D_8, C_4 \to C_2$; $V \to 1$.
Given $f \in K[X]$, deg 4, say roots are x_1, x_2, x_3, x_4.
Define $t_1 = (x_1 + x_2)(x_3 + x_4)$, $t_2 = (x_1 + x_3)(x_2 + x_4)$, $t_3 = (x_1 + x_4)(x_2 + x_3)$
Key point - the t_i are invariant under $G \cap V$.
The resolvent cubic of f is $g(X) = \prod_{i=1}^{3}(X - t_i) = X^3 - e_1 X^2 + e_2 X - e_3$, $e_i = e_i(\underline{t})$.
So e_i is invariant under S_4.
The point is that S_4 permutes $x_1, .., x_4$ and so permutes $t_1, .., t_3$.
In fact, given $\sigma \in S_4$, $\pi(\sigma)$ permutes $t_1, .., t_3$. That is, S_4 permutes $t_1, .., t_3$ via homomorphism π.
So, $e_i \in L^{Gal(f)} = K$, so $g \in K[X]$. By construction, $Gal(g) = \pi(Gal(f)) \hookrightarrow S_3$.
Assume f irreducible. So $Gal(g)$ determines $Gal(f)$ up to ambiguity between D_8 and C_4 if $Gal(g) = C_2$.

Proposition 9.3: (i) $\Delta(g) = \Delta(f)$
(ii) If $f = X^4 + pX^2 + qX + r$ (replace X by $X + \alpha$, some α, to obtain this), then
$g = X^3 - 2pX^2 + (p^2 - 4r)X + q^2$.
Proof: Direct calculation in both cases.

10. Finite Fields.

Lemma 10.1: If K is a finite field, then char $K = p > 0$. That is, $\mathbb{F}_p \hookrightarrow K$. Also, $[K:\mathbb{F}_p] = r$, say, is finite and $\# K = p^r$.
Proof: If char $K \neq p$, then char $K = 0 \Rightarrow \mathbb{Q} \hookrightarrow K$ - #.
$[K:\mathbb{F}_p]$ finite is obvious. Pick basis with elements of K as column vectors, entries $\in \mathbb{F}_p$. Then, #(possible vectors) $= p^r$.

We shall see that $\forall p^r$, $\exists$ a unique field with p^r elements.

Proposition 10.2: If K is any field and if $A \subset K^*$ is a finite subgroup, then A is cyclic.
Proof: A is a finite abelian group, so (from structure theorem) $\exists$ n such that $x^n = 1$ $\forall x \in A$, and $\exists z \in A$ of order exactly n. Then every $x \in A$ is a root of $X^n - 1$.
This has degree n, so has $\leq$ roots in K. So $\# A \leq n$ and $n \mid \# A$.

Corollary 10.3: If K is finite, say $\# K = p^r = q$, then K^* is cyclic of order $q-1$.
Proof: Obvious from above.

Proposition 10.4: If K is finite with $\#K = q = p^r$, then the map $\mathrm{Frob}_p : K \to K;\ x \mapsto x^p$ is an automorphism of K. Moreover, the field of invariants $= \{x \in K : x^p = x\}$ is $\mathbb{F}_p$.

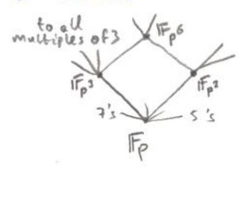
Proof: $(xy)^p = x^p y^p$. $(x+y)^p = \sum_{r=0}^{p} x^r y^{p-r} \binom{p}{r}$. If $1 \le r \le p-1$, then $\binom{p}{r} = \frac{p!}{r!(p-r)!}$.
Now, $p \mid p!$, but $p \nmid r!$, $p \nmid (p-r)!$, so $\binom{p}{r} \equiv 0 \pmod p$. $\therefore (x+y)^p = x^p + y^p$.
So, $\mathrm{Frob}_p : K \to K$ is a homomorphism of fields. $1 \mapsto 1$, so $\ker(\mathrm{Frob}_p)$ is an ideal in K, $\neq K$, so $=0$. Ie, Frob_p is injective. K is finite, so Frob_p is an isomorphism. (Ie, every $x \in K$ has a unique p^{th} root in K). Now, $x^p = x \iff x$ is a root of $X^p - X$. This is a polynomial of degree p, so has $\le p$ roots in K. All elements of $\mathbb{F}_p$ are roots, so $x \in \mathbb{F}_p$.

Corollary 10.5: If $\#K = q$, then $K/\mathbb{F}_p$ is Galois. $\mathrm{Aut}(K/\mathbb{F}_p)$ is cyclic and generated by Frob_p.
Proof: Let $s = \mathrm{Frob}_p$. Then $\langle s \rangle \subseteq \mathrm{Aut}$, so $\mathbb{F}_p \overset{=}{\hookrightarrow} K^{\langle s \rangle} \hookrightarrow K$. So, by FTGT, $\mathrm{Aut}(K/\mathbb{F}_p) = \langle s \rangle$.

Theorem 10.6: If $q = p^r$, $\exists$ field K with $\#K = q$, and K is unique up to isomorphism.
Proof: Let $K =$ splitting field for $X^q - X$ over $\mathbb{F}_p$. So, $K = \mathbb{F}_p(\alpha_1, \dots, \alpha_r)$, α_i roots of $X^q - X = f$.
So $\alpha_i^q = \alpha_i$. Let $x \in K$. Then $x = \sum \lambda_{n_1,\dots,n_r} \alpha_1^{n_1} \cdots \alpha_r^{n_r}$ ($\lambda_{\underline{n}} \in \mathbb{F}_p$). So, $x^q = \sum \lambda_{\underline{n}}^q (\alpha_1^{n_1})^q \cdots (\alpha_r^{n_r})^q$.
Now $\lambda_{\underline{n}}^q = \lambda_{\underline{n}}$, since $\lambda_{\underline{n}} \in \mathbb{F}_p$. And $\alpha_i^q = \alpha_i$, so $x^q = x$. So every $x \in K$ is a root of f.
So $\#K = \#(\text{roots of } f)$. Now, f is a product of q linear terms in $K[X]$. Notice $f' = -1$.
So, $(f, f') = 1$, so f has no repeated roots. So $\#K = \deg f = q$.
Uniqueness: If $\#L = q$, L^* is of order $q-1$, so $x^{q-1} = 1\ \forall x \in L^*$. So $x^q - x = 0\ \forall x \in L$, ie, every $x \in L$ is a root of f. So, $L \subseteq \mathbb{F}_p(\text{all roots of } f) =$ splitting field for $f = K$.
But $\#L = q = \#K$, so $L = K$.

Theorem 10.7: Say $K = \mathbb{F}_q$, $L = \mathbb{F}_Q$, $q = p^r$, $Q = p^s$. Then, $K \hookrightarrow L \iff r \mid s$.
Proof: Suppose $K \hookrightarrow L$. Then $\#L = (\#K)^{[L:K]}$. So $s = rm$, where $m = [L:K]$.
Conversely, suppose $r \mid s$. Need $K \hookrightarrow L$. If $x \in K^*$, then $x^{q-1} = 1$, ie $x^{p^r - 1} = 1$.
Say $s = r.m$. Then $p^s - 1 = p^{rm} - 1 = (p^r - 1)\left((p^r)^{m-1} + \dots + p^r + 1\right)$. So $p^r - 1 \mid p^s - 1$.
So $x^{p^s - 1} = 1$. So every $x \in K$ is a root of $g := X^{p^s} - X$.
L was constructed as the splitting field of g. So $x \in L\ \forall x \in K$, ie, $K \subseteq L$.

Theorem 10.8: Suppose $r \mid s$, so that $K = \mathbb{F}_{p^r} \hookrightarrow L = \mathbb{F}_{p^s}$, say $s = rm$. Then, L/K is Galois. $\mathrm{Aut}(L/K)$ is cyclic and generated by $\mathrm{Frob}_q := (\mathrm{Frob}_p)^r$.
Proof: Let $s = \mathrm{Frob}_q$. Easy to see that $s \in \mathrm{Aut}(L/K)$ and $L^{\langle s \rangle} = K$.
Let $x, y \in L$. $s(x) = x^q$. So, $s(x) + s(y) = s(x+y)$, $s(xy) = s(x)s(y)$, as already seen.
If $x \in K^*$, then $x^{q-1} = 1$, so $x^q = x\ \forall x \in K$. So $K \subseteq L^{\langle s \rangle}$
Suppose $z \in L$ and $s(z) = z$, ie, $z^q = z$. Then z is a root of $f = X^q - X$, a polynomial whose splitting field is K. So $z \in K$, so $K = L^{\langle s \rangle}$, as required.
Fix p. Then the finite fields $\mathbb{F}_q$ of characteristic p form a lattice:
$\mathbb{F}_q \subset \mathbb{F}_Q \iff Q = q^m$.



11. Cyclotomic Fields and Polynomials over $\mathbb{Q}$.

The nth cyclotomic field is $\mathbb{Q}(\zeta_n)$, where $\zeta_n = \exp(2\pi i/n)$

Lemma 11.0: Inside $\mathbb{C}$, the nth roots of 1 form a cyclic group of order n, called μ_n.
Proof: The nth roots of 1 are just the ζ^r, where $0 \leq r < n$.

Definition: A primitive nth root of unity is a generator of μ_n (Eg: ζ_n is primitive)

The primitive roots are the ζ_n^r with $(r,n) = 1$. There are $\varphi(n)$ primitive nth roots.
So, if $n = p$, prime, $\varphi(n) = p-1$, so every $\zeta \neq 1$ is primitive.

We shall examine the Galois nature of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. This is a Galois extension of degree $\varphi(n)$, and $Aut(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\psi, \cong} (\mathbb{Z}/n\mathbb{Z})^*$, $\psi(s) = s(\zeta_n)$.

Definition: The nth cyclotomic polynomial is $\Phi_n(X) = \prod_{\zeta \text{ primitive}} (X - \zeta)$. Ie, over $\zeta = \exp(\frac{2\pi i r}{n})$, $(r,n) = 1$.

Note: $\forall \zeta \in \mu_n$, $\exists$ unique $d | n$ such that ζ is a primitive dth root of 1. Take d = order of ζ.
So, $\prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{d|n} \Phi_d(X) = X^n - 1$.

Proposition 11.1: $\Phi_n(X) \in \mathbb{Z}[X]$.
Proof: Induction on n. $\Phi_1 = X - 1$. Assume $n > 1$, then $X^n - 1 = \Phi_n(X) . \underbrace{\prod_{d|n, d<n} \Phi_d(X)}_{=: g(x)}$.
So, $g(x) \in \mathbb{Z}[X]$, by induction hypothesis.
All polynomials appearing lie in $\mathbb{Q}(\zeta_n)[X]$. By construction, $hcf(g, X^n - 1) = g$ in $\mathbb{Q}(\zeta_n)[X]$.
We know that extending fields does not change hcfs, so $hcf(g, X^n - 1) = g$ in $\mathbb{Q}[X]$.
So, $g | X^n - 1$ in $\mathbb{Q}[X]$ and so (by Gauss) in $\mathbb{Z}[X]$. Ie, $\frac{X^n - 1}{g} \in \mathbb{Z}[X]$. But $\frac{X^n - 1}{g} = \Phi_n(X)$.

Theorem 11.2: $\Phi_n(X)$ is irreducible in $\mathbb{Q}[X]$ and so in $\mathbb{Z}[X]$, by Gauss.
Proof: Pick $\zeta \in \mu_n$, primitive. Say its minimal polynomial in $\mathbb{Z}[X]$ is f. $\Phi_n(\zeta) = 0$, so $f | \Phi_n$ in $\mathbb{Z}[X]$. Pick some prime $p \nmid n$. Then $\zeta^p \in \mu_n$ is primitive, with minimal polynomial g, say.
Assume $f \neq g$. So f, g are coprime, and divide $X^n - 1$, so $X^n - 1 = f(x) g(x) h(x)$, some h — $\circledast$
Note $g(X^p)$ has root $X = \zeta$, so $f(x) | g(X^p)$, say $g(X^p) = f(x) k(x)$, some k.
Let bars denote reduction mod p. Recall $\alpha^p = \alpha$ $\forall \alpha \in \mathbb{F}_p$. So $\bar{g}(X^p) = \bar{g}(X^p)$.
So, $\bar{g}(X)^p = \bar{f}(X) \bar{k}(X)$. Suppose $\bar{\varphi}$ is a prime factor in $\mathbb{F}_p[X]$ of $\bar{f}$, so $\bar{\varphi}$ is a factor of $\bar{g}$ as well.
From $\circledast$, $\bar{\varphi}^2$ divides $X^n - 1$ in $\mathbb{F}_p[X]$. But $\frac{d}{dx}(X^n - 1) = nX^{n-1} \neq 0$ as $p \nmid n$.
So, $(X^n - 1, \frac{d}{dx}(X^n - 1)) = 1$, so $X^n - 1$ has no repeated root, in any extension of $\mathbb{F}_p$.
$\#$ to $\bar{\varphi}^2 | X^n - 1$, so $f = g$. So ζ primitive $\Rightarrow \zeta^p$ also a root of f.
Now, every primitive element of μ_n is of the form ζ^m, where $(m,n) = 1$.
Write $m = p_1 \cdots p_r$, p_i prime, $p_i \nmid n$. ζ is a root of f, so ζ^{p_1} is a root of f, so $(\zeta^{p_1})^{p_2}$ is a root of f, .., so ζ^m is a root of f.
So every root of Φ_n is a root of f. f is irreducible in $\mathbb{Z}[X]$, as it is a minimal polynomial, so $\Phi_n = f$.

Corollary 11.3: $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois, and $G = \mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\psi, \cong} (\mathbb{Z}/n\mathbb{Z})^*$, $s(\zeta_n) \to \zeta_n^{\psi(s)}$.

Proof: $\mathbb{Q}(\zeta_n)$ contains all ζ_n^r. The conjugates of ζ_n are the roots of its minimal polynomial Φ_n, and so are the ζ_n^r, $(r,n)=1$. So $\mathbb{Q}(\zeta_n)$ contains every conjugate of ζ_n, and is separable, so is Galois.

$\forall s \in G$, $s(\zeta_n) = \zeta$, say, satisfies $\zeta^n = 1$. If $\zeta^m = 1$, some $m < n$, then $\zeta_n = s^{-1}(\zeta)$ would satisfy $\zeta_n^m = 1$ - #. So ζ is primitive. So $\zeta = \zeta_n^r$, $(r,n)=1$, and r is unique, subject to $1 \le r < n$. So we have a well-defined map $\psi: G \to (\mathbb{Z}/n\mathbb{Z})^*$, $s(\zeta_n) \to \zeta_n^{\psi(s)}$.

Suppose $s, t \in G$, say $s(\zeta_n) = \zeta_n^p$, $t(\zeta_n) = \zeta_n^q$. Then, $(st)(\zeta_n) = s(t(\zeta_n)) = s(\zeta_n^q) = (s(\zeta_n))^q = (\zeta_n^p)^q = \zeta_n^{pq}$.

So, $\psi(st) = pq = \psi(s)\psi(t)$, so ψ is a group homomorphism.

Suppose $s \in \ker \psi$. Then $\psi(s) = 1$, so $s(\zeta_n) = \zeta_n$. But ζ_n generates $\mathbb{Q}(\zeta_n)$, so $s = 1$ on all of $\mathbb{Q}(\zeta_n)$, ie, $s = 1$. So $\ker \psi = 1$, so ψ is injective.

Finally, $\# G = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$, so ψ is an isomorphism

Remark: If $n = p$, prime, then $\Phi_n = \Phi_p = \dfrac{X^p - 1}{X - 1} = X^{p-1} + \dots + X + 1$.

Easy exercise to prove this is irreducible, via Eisenstein.

Corollary 11.4: If K is any field of characteristic 0, then $K(\zeta_n)/K$ is Galois, and $\mathrm{Aut}(K(\zeta_n)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ is surjective. (So $\mathrm{Aut}(K(\zeta_n)/K)$ is abelian).

Proof: $K(\zeta_n)$ contains all powers of ζ_n, so all conjugates of ζ_n, so $K(\zeta_n)/K$ is Galois, say group H. Get $\psi: H \to (\mathbb{Z}/n\mathbb{Z})^*$ exactly as before. Same proof shows that ψ is an injective homomorphism. (But we cannot deduce that ψ is an isomorphism).

12. Kummer Theory.

By definition, this concerns extensions L/K that are Galois with abelian Galois group, say G, (ie, L/K is abelian), such that G is of exponent n (ie, $s^n = 1$ $\forall s \in G$), and K contains a primitive nth root of unity, and char $K \nmid n$.

We shall assume char $K = 0$, so $\mathbb{Q} \hookrightarrow K$, so that the hypothesis on nth roots means $\mathbb{Q}(\zeta_n) \hookrightarrow K$.

Theorem 12.1: Assume L/K satisfies all the above (ie, a Kummer extension, char $= 0$), and that G is cyclic of order m dividing n. Then, $\exists a \in K$ such that $L = K(a^{1/n})$.

Proof: Put $\zeta = \zeta_n^{n/m} = \exp(\frac{2\pi i}{n} \cdot \frac{n}{m})$, then $\zeta = \zeta_m$, a primitive mth root of 1.

Pick $\theta \in L$ with $L = K(\theta)$. Say $G = \langle s \rangle$. Put $\theta_i = s^i(\theta)$, so $\{\theta = \theta_0, \dots, \theta_{m-1}\}$ are the conjugates of θ. Put $\alpha = \theta_0 + \zeta\theta_1 + \dots + \zeta^{m-1}\theta_{m-1}$. Then, $s(\alpha) = s(\theta_0) + \zeta s(\theta_1) + \dots + \zeta^{m-1} s(\theta_{m-1})$ $= \theta_1 + \dots + \zeta^{m-1}\theta_0 = \zeta^{-1}\alpha$. So, $s(\alpha^m) = (\zeta^{-1}\alpha)^m = \alpha^m$, So $\alpha^m \in K$.

We have $K \hookrightarrow K(\alpha) \hookrightarrow L$. By FTGT, $K(\alpha) = L^H$, $H \le G$. Say $H = \langle s^r \rangle$.

Then $s^r(\alpha) = \alpha$, so $\alpha = \zeta^{-r}\alpha$, so $m | r$. $\therefore s^r = 1$, so H trivial, so $K(\alpha) = L$.

Blanket assumption: All finite extensions of K are separable.

Proposition 12.3: If $\mu_n \hookrightarrow K$ and $L = K(a^{1/n})$, then L/K is cyclic, with cyclic Galois group

Proof: Put $\alpha = a^{1/n}$, so $L = K(\alpha)$. If $\mu_n = \langle \zeta \rangle$, then the conjugates of α are a subset of $\{\alpha, \zeta\alpha, .., \zeta^{n-1}\alpha\}$. (This is a list of all roots of $X^n - a$. Minimal polynomial f of α divides this, so roots of f form a subset). So L contains all conjugates of α. L/K is separable, so Galois. Let $G = \mathrm{Aut}(L/K)$. Get $G \xrightarrow{\psi} (\mathbb{Z}/n\mathbb{Z})^\times$ by $s(\alpha) \to \psi(s)\alpha$. ($s(\alpha)$ is some conjugate of α, so is $\zeta^?\alpha$). Exactly as before, ψ is an injective homomorphism, so $G \hookrightarrow \mu_n$.

Examples: (i) $G = S_4$: $1 \overset{2}{\hookrightarrow} \overset{\cong C_2}{\langle(12)\rangle} \overset{2}{\hookrightarrow} \overset{\cong C_2 \times C_2}{V} \overset{3}{\hookrightarrow} A_4 \overset{2}{\hookrightarrow} S_4$. (Note: $\langle(12)\rangle \triangleleft V$, not of S_4)

(ii) abelian (and finite) $\Rightarrow$ soluble.

(iii) If G is soluble and $H \leq G$, then H is soluble. Let $H_i = H \cap G_i$.

$$\begin{array}{ccccccccc} 1 & \subset & G_0 & \subset & G_1 & \subset \cdots \subset & G_s & = & G \\ & & \uparrow & & \uparrow & & & & \\ \text{So, } 1 & \subset & H_0 & \subset & H_1 & \subset \cdots \subset & H_s & = & H. \end{array}$$

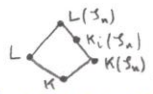
Then, $\frac{\#H_{i+1}}{\#H_i} \,\Big|\, \frac{\#G_{i+1}}{\#G_i}$, but RHS is prime.

(iv) If $H \triangleleft G$ and if H and G/H are both soluble, then so is G. (Recall that if G and H acts trivially, then G/H acts on X) $\#(G/H) = \#G/\#H$.

(v) Any dihedral group is soluble: the rotation group is cyclic and normal of index 2.

(vi) $\exists$ non-soluble groups, for example, any non-abelian simple groups.

Example: $G = A_n$ ($n \geq 5$). (A_4 is soluble, $A_3 \cong C_3$, $A_2 = 1$). See handout, or Van der Waerden.

Proof of Theorem 12.4: Assume $L \subseteq \mathbb{C}$, $\zeta_n = \exp(2\pi i/n)$. First, construct: 

where n is divisible by all n_i, say, $n =$ hcf. Take Galois closure $\tilde{L}$ of $L(\zeta_n)/K(\zeta_n)$.
To get $\tilde{L}$, adjoin all conjugates of all generators of $L(\zeta_n)/K(\zeta_n)$. Do this in stages. Let $K_1(\zeta_n) = K(\zeta_n)(\alpha_1)$, $\alpha_1^n \in K$. Then the conjugates of α_1 lie in the subset $\{\zeta_n^j \alpha_1\}$. Since $\zeta_n \in K(\zeta_n)$, these conjugates all lie in $K_1(\zeta_n)$. So $K_1(\zeta_n)/K(\zeta_n)$ is Galois and has cyclic Galois group ($\hookrightarrow \mu_n$). Similarly, $K_{i+1}(\zeta_n)/K_i(\zeta_n)$ is Galois with cyclic Galois group $G_i \hookrightarrow \mu_n$. Get $L(\zeta_n) = K_s(\zeta_n)$, $K_{i+1}(\zeta_n) = K_i(\zeta_n)(\alpha_{i+1})$.
Adjoin conjugate $\tilde{\alpha_2}$ of α_2 wrt $K(\zeta_n)$. $\alpha_2^n \in K_1(\zeta_n)$, Galois over $K(\zeta_n)$.
So $\tilde{\alpha_2} \in K_1(\zeta_n)$. So, $K_1(\zeta_n)/(\{\tilde{\alpha_2}\})$ is obtained by adjoining a collection of nth roots. Each $\widetilde{K_{i+1}}$ is obtained from $\widetilde{K_i}$ similarly.
$\tilde{L}$ is Galois over $K(\zeta_n)$, say with group G. FTGT $\Rightarrow$ $\widetilde{K_i} = \tilde{L}^{H_i}$, $H_i \leq G$.
$1 = H_s \subset H_{s-1} \subset \cdots \subset H_i \subset \cdots \subset H_0 = G$. $\widetilde{K_{i+1}} = \widetilde{K_i}(\beta_1, .., \beta_t)$, $\beta_j^n \in \widetilde{K_i}$.
This is a Galois extension, with Galois group a subgroup of $\mu_n \times \cdots \times \mu_n = (\mu_n)^t$.
$\Gamma \overset{\psi}{\hookrightarrow} (\mu_n)^t$ by $\psi(\gamma) = (w_1, .., w_n)$ if $\gamma(\beta_i) = w_i\beta_i$, $w_i \in \mu_n$.
So, (FTGT), H_{i+1} is a normal subgroup of H_i, and $H_{i+1}/H_i \cong \Gamma$.
To get a chain exhibiting G as soluble, insert more subgroups between H_{i+1} and H_i, or use lemma quoted to the effect that H normal in G and H, G/H both soluble $\Rightarrow$ G soluble. So again G is soluble.
Write $N/K =$ Galois closure of L/K.
We have proved that given L/K obtained by adjoining a succession of roots, then after adjoining ζ_n, get soluble Galois closure. Need to deduce that L/K has Galois closure N/K with $\mathrm{Aut}(N/K)$ soluble.

Theorem 12.4 (Take 2): Given $K \hookrightarrow L$ such that L is obtained by successively adjoining roots. (Assume char $K=0$, or $=p>0$ with $p \nmid n_i$, and all finite extensions of K are separable). So, $K = K_0 \hookrightarrow K_1 \hookrightarrow \cdots \hookrightarrow K_r = L$, $K_i = K_{i-1}(\alpha_i)$, $\alpha_i^{n_i} = a_i \in K_{i-1}$.
Then $\exists$ Galois M/K, with $K \hookrightarrow L \hookrightarrow M$ such that $Aut(M/K)$ is soluble.

Proof: Put $N = \prod n_i$, $\zeta = \zeta_N$. Let $\{\alpha_{ij}\}$ be the set of K-conjugates of α_i, $\{a_{ij}\}$ those of a_i.
$L_s = K(\{\alpha_{ij} : i \leq s\}, \zeta)$. Each L_s is generated over K by K-conjugates, so is Galois over K. Also, $K_s \hookrightarrow L_s$ $\forall s$. $L_{s+1} = L_s(\alpha_{s1}, \dots, \alpha_{st})$. $\forall j$, $\alpha_{sj}^{n_s} \in L_s$. All n_s^{th} roots of 1 lie in L_s.
So L_{s+1}/L_s is Galois, say with group H_s. H_s is abelian (For: $H_s \hookrightarrow (\mu_N)^t$. This embedding is given by $\sigma \mapsto (\omega_1, \dots, \omega_t)$, where $\sigma(\alpha_{sj}) = \omega_j \alpha_{sj}$ ($\mu_{n_s} \subset \mu_N$ as $n_s | N$). Since $\sigma(\alpha_{sj}^{n_s}) = \alpha_{sj}^{n_s} \in L_s$. So H_s is abelian). So we have $K \hookrightarrow L_0 \hookrightarrow L_1 \hookrightarrow \cdots \hookrightarrow L_r$.
Let $G = Aut(L_r/K)$. FTGT $\Rightarrow L_i = L_r^{G_i}$, some $G_i \leq G$. Moreover, since L_i is Galois over K, we have (FTGT) $G_i \trianglelefteq G$ and $Aut(L_i/K) \cong G/G_i$.
Also, $H_i = Aut(L_{i+1}/L_i) \cong G_i/G_{i+1}$. At group level, $G \hookleftarrow G_0 \hookleftarrow G_1 \hookleftarrow \cdots \hookleftarrow G_r = 1$ — ⊛.
$G/G_0 = Aut(L_0/K) = Aut(K(\zeta)/K)$, which we known is abelian [$\leq (\mathbb{Z}/n\mathbb{Z})^*$)
So we have $L \hookrightarrow L_r$, L_r/K - Galois group G, containing chain of subgroups ⊛ all normal in G, such that each successive quotient is abelian. So G is soluble.

Converse: Suppose L/K Galois, and $G = Aut(L/K)$ is soluble, say $N = \# G$, $\zeta = \zeta_N$. Then $L(\zeta)/K$ is obtained from K by adjoining first ζ and then successively adjoining roots.

Proof: Say $L = K(\alpha)$: L contains all K-conjugates of α. Then $L(\zeta) = K(\alpha, \zeta)$ contains all K-conjugates of α and ζ. So $L(\zeta)/K$ is Galois, say group Γ, $K(\zeta) = L(\zeta)^{\Delta}$, by FTGT.
Now, L/K is Galois, so $L = L(\zeta)^H$, where $H \trianglelefteq \Gamma$. In fact, Γ preserves L, so Δ does too.
So get $\Delta \to Aut(L/K)$. If $\delta \in \Delta$, $\delta(\lambda) = \lambda$ $\forall \lambda \in L$. Now, $\delta(\zeta) = \zeta$, by definition of Δ, so $\delta(x) = x$ $\forall x \in L(\zeta)$, so $\delta = 1$, i.e, $\Delta \hookrightarrow Aut(L/K) = G$, so Δ is soluble. Get:
$1 = \Delta_0 \hookrightarrow \Delta_1 \hookrightarrow \cdots \hookrightarrow \Delta_r = \Delta$, $\Delta_i \trianglelefteq \Delta_{i+1}$, Δ_{i+1}/Δ_i cyclic of ordering dividing $\# \Delta$, which divides $\# G = N$. The Δ_i correspond to $L(\zeta) = L_0 \hookleftarrow \cdots \hookleftarrow L_r = K(\zeta)$, each L_i Galois and cyclic over L_{i+1} of degree n_i dividing N. So $L_i = L_{i+1}(a_i^{1/n_i})$ by Kummer.

Corollary: Given polynomial $f \in K[X]$, let L = splitting field of f over K. $Gal(f) = Aut(L/K)$.
Then, f can be solved by successively adding radicals iff $Gal(f)$ is soluble.

Example: $K = \mathbb{Q}$, $f = X^5 - 20X + 5$, $G = Gal(f)$. Eisenstein at 5 $\Rightarrow$ f irreducible. Degree $f = 5$, so $G \hookrightarrow S_5$ is transitive, as f irreducible. Now, complex conjugation is a transposition in G, so f has just 3 real roots. $f' = 5x^4 - 20 = 0$ only at $x = \pm\sqrt{2}$.
$f(-\sqrt{2}) = -4\sqrt{2} + 20\sqrt{2} + 5 > 0$, $f(\sqrt{2}) = 4\sqrt{2} - 20\sqrt{2} + 5 < 0$. So graph is: 
$G = S_5$, which is not soluble, so cannot find roots by adjoining radicals.

Example: $f = X^n - e_1 X^{n-1} + \cdots + (-1)^n e_n \in \mathbb{Q}(e_1, \dots, e_n)[X]$, e_i independent indeterminates, has $Gal(f) = S_n$. If roots of f are $\alpha_1, \dots, \alpha_n$ then e_i = ith elementary symmetric function of the α's. S_n permutes the α_i, which are also independent indeterminates, and $\mathbb{Q}(\underline{e}) = \mathbb{Q}(\underline{\alpha})^{S_n}$

$\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is abelian. ζ_N is the value of $z \mapsto \exp(2\pi i z)$, evaluated at the special point $z = 1/N$. Also, comparably, extensions of $\mathbb{Q}$ with Galois group A_5, for example, can be obtained by evaluating more complicated holomorphic functions at special points. So, in fact, having non-soluble Galois group is not the end of the story, but the start of something more interesting.