Let $F \subset E$ be a field extension. Then $\text{Gal}(E/F)$, the Galois group of $E$ over $F$ is the group of field automorphisms of $E$ fixing $F$.

Examples

1. $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2})$
   $\text{Gal}(E/F) \cong \mathbb{Z}/2$ with $\sqrt{2} \mapsto -\sqrt{2}$

2. $E = \mathbb{Q}(\sqrt[3]{2})$, $\text{Gal}(E/F)$
is trivial. \( \sqrt{3} \) must be sent to itself because it is the only root of \( x^2 = 3 \) present. \( E = \mathbb{Q}[x]/(x^3 - 2) \)

\( E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) \) (first day example)

\( E \) splitting for \( x^3 - 2 \)

\( \text{Gal}(E/F) \approx S_3 \)

In 0 and 3, \( [E : F] = 1 = \text{deg}(E/F) \), but not so in \( E \).
Theorem 12.1.24 Let \( F = \text{field} \), \( f(x) \in F[x] \) separable.
\[ E = \text{splitting field of } f(x) \]
\[ G = \text{Gal } (E/F) \]
Then \( |G| = [E:F] = n \).

Before proving this we need

Lemma 12.1.23 Let \( p(x) \) be an irreducible factor of \( g(x) \) with zeros \( x_1 \) and \( x_2 \). Then
\[ \exists \ y \in G \text{ with } p(y) = x_2. \]
Proof (see 10.3.20 and 10.3.21)

\( E \rightarrow F(\bar{x}_1) \rightarrow E \) \( F(\bar{x}) \) and \( F(\bar{x}_2) \) are both isomorphic to 

\( F[\bar{x}] / \langle f(\bar{x}) \rangle \).

and there is an automorphism of \( E \)

sanding \( F(\bar{x}_1) \) to \( F(\bar{x}_2) \) (QED)

Pf of Thm by induction on \( n \). Statement for \( n = 1 \) is obvious.

Let \( p(\bar{x}) \) be an irreducible factor of \( f(\bar{x}) \)
with zeros $\alpha_1, \alpha_2, \ldots, \alpha_k$ with $k \geq 1$. By the lemma, $\exists \gamma \in G$ with $\gamma(\alpha_i) = \alpha_i$. Then $[F(\alpha_i) : F] = k$ and $[E : F(\alpha_i)] = m$ with $[E : F] = m, k = n$. By induction,

$$|\text{ Aut } (E/ F(\alpha_i))| = [E : F(\alpha_i)] = m < n.$$

Because $E$ is the splitting field of $f(x)$. 
Claim 1. The elements \( y_i, \Theta_i \) are distinct.

Claim 2. Every \( \phi \in G \) is one of these.

Proof of Claim 1: Suppose \( y_i, \Theta_i = y_i, \Theta_i' \).
Then \( y_i = y_i, \Theta_i(x_i) = y_i, \Theta_i'(x_i) = y_i, \Theta_i'(x_i) \Theta_i \Theta_i^{-1} \).

But \( y_i, \Theta_i(x_i) = y_i, \Theta_i(x_i) = x_i \).

So \( i = i' \).
This means \( y_i \cdot j_y = y_i \cdot j_Y \)

so \( A_j = A_j^i \) and \( Y = f \).

QED

Proof of Claim 2:

Let \( E \rightarrow E \) be given

\[ x_i \mapsto x_i \] for some \( i \)

Let \( \theta = y_i^{-1} \phi \), so \( \theta(x_i) = x_i \). It fixes \( F(x_i) = \mathcal{O} \). Hence, \( \theta \in \text{Gal}(E/F) \)

so \( \theta = \theta_j \) for some \( j \).
\[ \theta_1 = \psi^1 \phi \quad \text{and} \quad \phi = \psi_1 \theta_1. \]

(QED)

Hence \( |G| = m \kappa^n \) as claimed (QED).

Proof 12.1.6 Let \( f(x) \in F[X] \) be a separable polynomial of degree \( d \)
and let \( E \) and \( G \) be as above.

Then \( G \) is a subgroup of \( S_d \). Hence
$161$ divides $d!$

Proof: An elt $\phi \in G$ permutes the $d$ roots of $f(x)$ and is determined by that permutation, so we have a $1:1$ hom $G \rightarrow S_d$, QED

There is an example in the book for $d = 5$ and $\Gamma = \mathbb{Q}$ in which $G$ contains $A_5$
We also know that $A_5$ is not solvable.

Recall $G$ is solvable if it satisfies

$$e G e = G_0 \triangleleft G_1 \triangleleft G_2 \ldots \triangleleft G_n = G$$

where $G_{i-1}$ is normal in $G_i$ with $G_i / G_{i-1}$ is abelian.

$G$ is simple if its only its only normal subgroups are $G$ and $e G e$.
A non-abelian simple group (e.g. $A_n$ for $n \geq 5$) is not solvable.

Let $f(x)$ etc be as above. Let $G$ be the Galois group of $f(x)$ over $\mathbb{F}_n$.

Galois' main theorem states that $f(x) = 0$ is solvable by radicals (to be defined shortly) iff its Galois group is solvable as defined.
above.

Def 12.5.5: An extension $K$ of $F$ is a simple radical extension if it has the form $K = F(p)$ where $p^n \in F$ for some $n > 0$. A radical tower over $F$ is $F = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_n = K$ where each $K_i$ is a simple radical
extension of $K_{i-1}$, $m$ in its height and $K_m$ is the top of the tower $K$. $F$ is an extension by radicals if it is the top of a radical tower over $F$. $f(x) \in F[x]$ is solvable by radicals if its splitting $E$ is contained in an extension of $F$ by radicals.
Thm 12.5.16 (Galois main thm)

Let $F$ be a field of char 0 and $f(x) \in F[x]$. Then $f(x)$ is solvable by radicals $\iff$ its Galois gp is solvable.

Goal of course is to prove this.

It implies there is no general formula for the roots of
a polynomial of degree \( \geq 5 \).

Thus 12.2.9 Let \( E \) be a finite extension of \( F \) with \( G = Gal(E/F) \). The following are equivalent (TFAE):  

1) \( F = EG_1 \), set of elt in \( E \) fixed by \( G \).  
2) Every irreducible polynomial \( p(x) \) with a root in \( E \) is separable and has all of its zeros in \( E \).
3) $E$ is the splitting field of a separable polynomial.

Def: An extension $E \supset F$ is a Galois extension if the above conditions hold.