Lecture 1 :- (Introduction to Galois theory).

Given a polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $a_i \in \mathbb{Q}$,

how do we understand the roots of this polynomial.

Quadratic case :-

- $f(x) = x^2 + bx + c$, $b, c \in \mathbb{Q}$, the roots are $\boxed{\dfrac{-b \pm \sqrt{b^2 - 4c}}{2}}$.

Given Cubic (deg 3) or quartic (deg 4) polynomial, we can obtain formulas for roots of this polynomial (by allowing operations like $\boxed{+, -, \times, \div, n\text{th roots}}$)

(This requires more work, some clever tricks, but can be ~~done~~ done).

However, for deg ≥ 5, a general nth deg polynomial cannot be solved by radicals (Abel Ruffini)

Galois introduced groups to study symmetries in roots of polynomials and gave a impossibility statement.

proof of this

th deg poly

Given an

$f(x) = x^{\boxed{n}} + a_{n-1}x^{n-1} + \cdots + a_0$, with $a_i \in \mathbb{Q}$.

Say roots of f are $\alpha_1, \ldots \alpha_n$.

Associated to this is a gp

G_f - Galois gp of f which is a subgp of $S_{\boxed{n}}$

sym. gp on n letters

Elements of G_f acts as permutations of $\{\alpha_1, \ldots \alpha_n\}$.

<u>Thm</u>:- f is solvable by radicals $\iff$ G_f is a solvable gp.

(It has a subnormal series with successive quotients abelian)

$\left(1 \leq \boxed{A_5} \trianglelefteq S_5 \right.$ simple gp$\left.\right)$.

<u>Field extns</u>:-

<u>Recall</u>:- A field $\mathbb{F}$ is a comm ring with identity in which every non-zero element has an inverse.

- $\operatorname{char}(\mathbb{F})$ = smallest +ve int $\ni \boxed{p} \, 1_{\mathbb{F}} = 0$ if such a p exists and is 0 otherwise

(Char = 0 or a prime)
($\mathbb{R}$ $\mathbb{Z}/p\mathbb{Z}$

<u>Field extns:-</u>
A field extn K of F is a field K containing F. The field F is called the base field and this extn is written K/F.

(~~Any~~ Exercise) non-zero hom $\varphi : F_1 \to F_2$ is injective).

If K/F is a field extn then K is infact a vector space over F and the deg of K/F, written $[K:F]$ is the dim of K as a vector space over F. If this is finite, then the extn is a finite extn.

Field extns arise naturally when trying to understand roots of poly. equations.

More generally, given a field polynomial $p(x) \in F[x]$

$\mathbb{F}$ and irr. poly ... does there exist a field K containing $\mathbb{F}$, such that $p(x)$ has a root in K?

<u>Yes!</u> Let $K = \dfrac{\mathbb{F}[x]}{(p(x))}$.

$p(x)$ ↳ is irr and hence generates a max ideal in $\mathbb{F}[x]$ (Exercise: Check this)

So K is a field.

We have a natural map

$$\mathbb{F}[x] \xrightarrow{\boxed{\varphi}} \boxed{\frac{\mathbb{F}[x]}{(p(x))}} = K$$

$\varphi|_{\mathbb{F}} : \mathbb{F} \to K$ is non-zero

So this is injective

$\Rightarrow \mathbb{F} \subseteq K$.

$$\left(\begin{aligned} p(\bar{x}) &= \overline{p(x)} \\ &= p(x) \bmod (p(x)) = 0 \end{aligned} \right)$$

Further the element $\bar{x} = x \bmod (p(x))$ is a root of $p(x)$ in K.

Later we will construct extns of $\mathbb{F}$ that contain all the roots of the poly $p(x)$ leading to the notion of <u>splitting fields</u>, a central object of study in

Galois theory.

- Fields generated by subsets:-

Let $K/\mathbb{F}$ be a field extn and

let $\alpha \in K$.

Can consider $\mathbb{F}(\alpha) \subseteq K$

$\downarrow$

field generated by $\mathbb{F}$ and α

($\cap$ of all subfields of K that contain $\mathbb{F}$ & α)

Similarly for $S \subseteq K$ we have

$\mathbb{F}(S) = \{ b \in K \mid$ b can be exp. in terms of field operation $+, -, \times, \div$ applied to $S \cup \mathbb{F} \}$

- The extn $K/\mathbb{F}$ is f.g (finitely generated) if $\exists$ a finite subset $\boxed{\{\alpha_1, \ldots \alpha_n\} \subseteq K}$ such that

$K = \mathbb{F}(\alpha_1, \ldots \alpha_n)$.

- It is primitive if $K = \mathbb{F}(\alpha)$ for some $\alpha \in K$.

Note:- If $p(x) \in \mathbb{F}[x]$ is irr. and $K/\mathbb{F}$ is an extn with an element $\alpha \in K$ such that $p(\alpha) = 0$

K

$\cup\!|$

$\mathbb{F}(\alpha) \cong \mathbb{F}[x]$

Then $\boxed{F(\alpha) \cong \dfrac{\quad}{(p(x))}}$

(To see this consider the F-hom

$$F[x] \xrightarrow{\varphi} F(\alpha)$$
$$x \longrightarrow \alpha.$$

$\mathrm{Ker} = \{ f \in F[x] \mid f(\alpha) = 0 \}.$

and $p \in \mathrm{Ker}(\varphi)$

$$\left(F[x]/(p(x))\right) \xrightarrow{\varphi} F(\alpha)$$

(This is injective, and surjective).

Algebraic elements:-

Let K/F be an extn and let $\alpha \in K$.

Consider $F[x] \xrightarrow{\boxed{\varphi}} K$ (φ is an F-hom sending $x \to \alpha$)
$$x \longrightarrow \alpha$$

Can look at $\mathrm{Ker}(\varphi)$.

If $\mathrm{Ker}(\varphi) \neq 0$, this means $\exists$ $p(x) \in F[x]$ $\ni$ $p(\alpha) = 0$

Such an element is called algebraic over F.

If $\mathrm{Ker}(\varphi) = 0$, this means $\nexists$ poly $p(x) \in F[x]$ $\ni$ $p(\alpha) = 0$

element is called transcendental.

Such an ... transcen...

(Eg: $\sqrt[3]{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$
a solution to $x^3 - 2$).

If $\alpha \in K$ is alg. over F,

<u>Note</u>: there there is a <u>unique</u> monic
irr polynomial $p(x) \in F[x]$ that
has α as root and $\ni$ if
$f(x) \in F[x]$ ~~has~~ has α as a root
then $p \mid f$.

<u>To see this</u>: Take p to be
of min deg having α as a
root and make ~~it~~ it monic.
It is irr, because its deg
is minimal. (Show that if
$f(x) \in F[x]$ has α
as a root then
$p \mid f$)

This poly is called the
min. polynomial of α.

<u>Note</u>: $\boxed{[F(\alpha) : F] = \deg p}$ (where p is the min poly of α).

$\cong$

$\frac{F[x]}{(p(x))}$. $\{1, \bar{x}, \ldots, \bar{x}^{\deg p - 1}\}$

Min poly of $\sqrt[3]{2}$ is (x^3-2).

Eg: Min poly of ... over $\mathbb{Q}$.
$x^5 - 2$ is irr. over $\mathbb{Q}$.
(Reading: Review irreducibility criteria)

An extn K/F is alg. if every element of K is alg. over F.

$\{1, \alpha, \ldots, \alpha^{n-1}\}$

Note:- If K/F is a finite extn (of defn) then K/F is algebraic.

Let $\alpha \in K$. Consider $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$
They are linearly dep
$\Rightarrow \exists\ a_0, \ldots, a_n \in F \ni$
$a_0 + a_1 \alpha + \ldots a_n \alpha^n = 0$
$\Rightarrow p(x) = a_0 + a_1 x + \ldots a_n x^n$ is a poly. satisfied by α.

Fact:- Let K/F be a field extn. Then K/F is finite $\Leftrightarrow$ it is alg. & f.g.

$\Rightarrow$) is already done.

On the other hand if $K = F(\alpha_1, \ldots \alpha_n)$ where α_i are alg. over F,

$F(\alpha_1) \quad F(\alpha_1, \alpha_2) \ldots$

Let $\mathcal{F} = \underbrace{K_0 \subseteq K_1}_{<\infty} \underbrace{\subseteq K_2}_{<\infty} \subseteq \cdots \underbrace{\cdots}_{<\infty} K$

$K_{i+1} = K_i(\alpha_{i+1})$

Note: α_{i+1} is alg over $\mathcal{F}$

$\Rightarrow$ α_{i+1} is also alg over K_i

$\Rightarrow$ $[K_{i+1} : K_i] =$ deg min poly of α_{i+1} over K_i

$< \infty$

Tower law:- If $\mathcal{F} \subseteq K \subseteq L$ are field extns then

$$[L : \mathcal{F}] = [L : K][K : \mathcal{F}]$$

(Exercise: prove this
Let $\{\alpha_i\}$ be a basis for L/K
$\{\beta_j\}$ be a basis for $K/\mathcal{F}$.
Then $\{\alpha_i \cdot \beta_j\}$ is a basis for $L/\mathcal{F}$).

Then $[K : \mathcal{F}] < \infty$.

Corollary:- If $\alpha, \beta \in \Omega$ are alg over $\mathcal{F}$
then $\alpha + \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ are all alg $\mathcal{F}$.

Hint:- Consider $\mathcal{F}(\alpha, \beta) \subseteq \Omega$.