MAT401 March 19th 2008

Goal: Some polynomials cannot be solved using $+, -, \times, \div, \sqrt[n]{\ }$

Galois' Theory (roughly)

$$\begin{Bmatrix}\text{field} \\ \text{extensions}\end{Bmatrix} \xleftarrow[\text{Theorem}]{\text{The Fundamental}} \{\text{groups}\}$$

$$\begin{Bmatrix}\text{extensions} \\ \text{using } \sqrt[n]{\ }\end{Bmatrix} \longrightarrow \{\text{"Solvable groups"}\}$$

splitting $3x^5 - 15x + 5$ $\longrightarrow$ The non-solvable group S_5

Def: A group is a set G with a binary operation $\cdot$ "times" s.t.

1. associative $(ab)c = a(bc)$
2. $\exists$ a "unit" $1 = e \in G$ (unique) $1 \cdot g = g \cdot 1 = g$
3. $\forall g \in G$ $\exists g^{-1} \in G$ s.t. $g^{-1}g = gg^{-1} = 1$ (unique)

Examples: $(\mathbb{Z}/18, +)$; $(\mathbb{Z}/7, \cdot)$; $(R, +)$, $(F \setminus \{0\}, \times)$ — Abelian: $a, b \in G$. $ab = ba$

Examples:

not abelian:

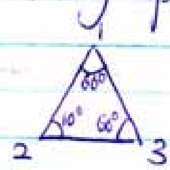
$S_n = \{\sigma : \{1, \dots, n\} \circlearrowleft : \sigma \text{ is 1-1 \& onto "bijection"}\}$

$\sigma\tau = \sigma \cdot \tau$

$|G|$ order of a group $\rightarrow$ # of elements

$|S_n| = n!$

Example: The group of "symmetries" of triangle

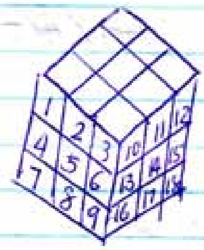


$G \cong S_3 \qquad |G| = 6.$

} not abelian

Example: Rubik's Cube Group.

The set of all "motions" from a group, is "subgroup" of S_{54}.



Def. A subset $H \subset G$ of a group G, is called a "subgroup" if it is a group using the same binary or $\Leftrightarrow$ closed under mult & inversion; we write $H < G$

Given $H < G$, define $g_1 \sim g_2 \mod H$ if $g_1 = g_2 h$ for some $h \in H$, this is an equivalent relation, $G/H = G/\sim$. For any $g \in G$, $|[g]| = |H|$ so $|G| = |G/H| \cdot |H| \rightsquigarrow |H| \mid |G|$

↳ # of elements in each equivalence class.

A product on G/H

$$[g_1][g_2] = [g_1 g_2]$$

$$g_1' \quad g_2^2 \mapsto g_1' g_2'$$

In general, G/H isn't a group, unless H is "normal" in G. $h \in H$, $g \in G$ then $g^{-1} h g \in H$ (write $H \triangleleft G$)

$\varphi : R \to S'$

$R/\ker\varphi \cong \operatorname{im}\varphi$

$\Psi : G_1 \longrightarrow G_2$ "group homomorphism"

$G_1/\ker\Psi \cong \mathrm{im}\,\Psi$ "first isomorphism thm"

Def: Given E/F

$Gal(E/F) = \{\phi : E \to E \mid$ 1. ϕ an automorphism "homomorphism of a thing to itself, which is invertible" 2. $\phi/F = I_d$ i.e., if $x \in F$, $\phi(x) = x\}$

"The Galois group of E/F"

Example:

$Gal(\mathbb{C}/\mathbb{R}) = \{\phi_1, \phi_2\}$

$\phi : \mathbb{C} \to \mathbb{C}$
$\phi_1 : (z) = z$
$\phi_2 : (z) = \bar{z}$
$\phi_2(a+bi) = a-bi$

$\overline{z_1+z_2} = \bar{z}_1 + \bar{z}_2$
$\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$
$\bar{\bar{z}} = z$ so $\phi_2 \cdot \phi_2 = I_d$

if $r \in \mathbb{R}$, $\bar{r} = r$ so $\phi_2(r) = r$

claim: If $f \in F[x]$ and $\alpha \in E$ is a root of f, and $\phi \in Gal(E/F)$ then $\phi(\alpha)$ is also a root of f.

Eg: i is a root of $x^2+1 = 0 \in \mathbb{R}[x]$
So if $\phi \in Gal(E/F)$ then $\phi(i)$ is a root of x^2+1

i.e. $\phi(i) = \pm i$ · $a, b \in \mathbb{R}$

$\phi(i) = i$ then $\phi(a+bi) = \phi(a) + \phi(b)\phi(i)$
$= a+bi$ so $\phi = \phi_1$

if

$\phi(i) = -i$ then $\phi(a+bi) = \phi(a) + \phi(b)\phi(i)$
$= a-bi$ so $\phi = \phi_2$

Example: $Gal(\mathbb{R}/\mathbb{Q})$ is a group from hell. Absolutely huge, nobody understands it.

Claim: $Gal(E/F)$ is a group under composition

Proof: $(\phi\cdot\psi)(a+b) = (\phi\cdot\psi)(a) + (b\cdot\psi)(b)$

Def: Given E/F, and $H < Gal(E/F)$

let $E_H = \{x \in E : \forall h \in H \ \ hx = x\}$
"The fixed field of H" $E - F$

Examples:
$\mathbb{C}/\mathbb{R}$, $G = \{1, \tau\}$ $\tau z = \bar{z}$
$H = \{1\}$ $G_H = \{z \in \mathbb{C} : 1z = z\} = \mathbb{C}$
$H = \{1, \tau\}$ $G_H = \{z \in \mathbb{C} : \tau z = z \ \ \bar{z} = z\} = \mathbb{R}$.

Thm let F be a field of characteristic 0 and let E be the splitting field of some polynomial in $F[x]$.

Remainder: splitting field of f over F
$S_F(f)$ is a field in which f splits (can be written as a product of linear factors) and so that f does not split in any smaller field.
$\leftrightarrow$ let $a_1, \dots, a_n$ be the roots of f. In some big field in which f splits. Then
$S_F(f) = F(a_1, \dots, a_n)$

Claim: all splitting fields of F are isomorphic. (Not yet proven).

Then there is a bijection:

$$\begin{array}{ccc} & & G \\ & & \| \\ \{K : E/K/F\} & \longrightarrow & \{H < \mathrm{Gal}(E/F)\} \\ F \subset E_H \subset E & \xleftarrow{\Psi} & H \\ K & \xmapsto{\Phi} & \mathrm{Gal}(E/K) < \mathrm{Gal}(E/F) \end{array}$$

Furthermore:

0. $H = \mathrm{Gal}(E/E_H)$ $\quad E_{\mathrm{Gal}(E/K)} = K$
1. Inclusion - reversing
   $H_1 < H_2 \Rightarrow E_{H_1} > E_{H_2}$ & $K_1 < K_2 \Rightarrow \mathrm{Gal}(E/K_1) > \mathrm{Gal}(E/K_2)$
2. degree / index / order respecting
   $\underset{?}{[E:K]} = \underset{?}{|\mathrm{Gal}(E/K)|}$

Example:

$K = E \xrightarrow{\Phi} \mathrm{Gal}(E/E) = \{1\}$

$K = F \xrightarrow{\Phi} \mathrm{Gal}(E/F) = G$

$H = \{1\} \xrightarrow{\Psi} E_{\{1\}} = E$ obvious in fact

$H = G \xrightarrow{\Psi} E_G = E_{\mathrm{Gal}(E/F)} \supset F$

$E = \mathbb{Q}(\sqrt{3}, \sqrt{5}) / \mathbb{Q} = F$

E is $S_{\mathbb{Q}} : ((x^2-3)(x^2-5))$

$(x-\sqrt{3})(x+\sqrt{3})(x-\sqrt{5})(x+\sqrt{5})$

$E = \{a_0 1 + a_1\sqrt{3} + a_2\sqrt{5} + a_3 \underset{\sqrt{3}\sqrt{5}}{\sqrt{15}} : a_{0,1,2,3} \in \mathbb{Q}\}$

$[E:F] = 4 \quad |\mathrm{Gal}(E/F)| = 4$

$(\mathbb{Z}/4, +) \qquad (\mathbb{Z}/2)^2$

$0, 1, 2, 3 \qquad 00, 01, 10, 11$

if $\phi \in Gal$, $\phi(\text{root}) = \text{root}$.

$G = Gal(E/F)$

$\phi(\sqrt{3}) = \pm\sqrt{3}$ $\quad \phi(\sqrt{5}) = \pm\sqrt{5}$ for any $\phi \in G$.
root of $x^2 - 3$

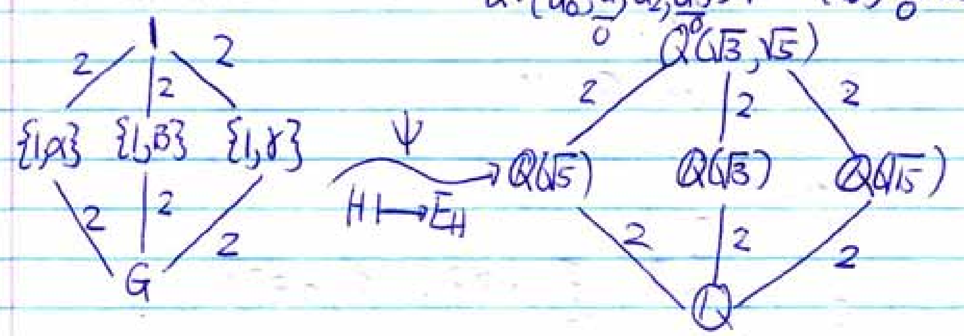
Suppose $\phi_{1,2} \in G$, & $\phi_1(\sqrt{3}) = \phi_2(\sqrt{3})$ & $\phi_1(\sqrt{5}) = \phi_2(\sqrt{5})$.
$\Rightarrow \phi_1 = \phi_2$

so $Gal(E/F) = \{1, \alpha, \beta, \gamma\}$.

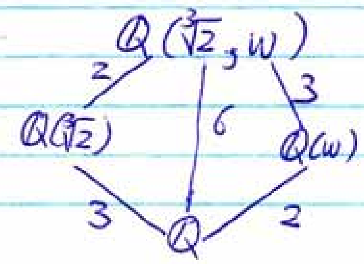
$1(\sqrt{3}) = \sqrt{3}$ $\quad \alpha(\sqrt{3}) = -\sqrt{3}$ $\quad \beta(\sqrt{3}) = \sqrt{3}$ $\quad \gamma(\sqrt{3}) = -\sqrt{3}$.
$1(\sqrt{5}) = \sqrt{5}$ $\quad \alpha(\sqrt{5}) = \sqrt{5}$ $\quad \beta(\sqrt{5}) = -\sqrt{5}$ $\quad \gamma(\sqrt{5}) = -\sqrt{5}$
$\alpha^2 = 1$ $\quad \gamma = \alpha \circ \beta$ $\quad \beta^2 = 1$ $\quad \gamma^2 = 1$

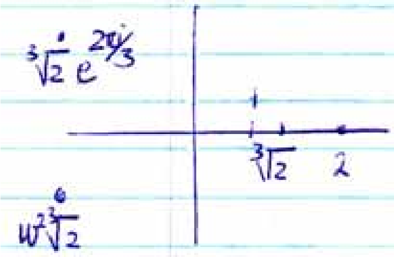
Subgroup of G. $\quad |G| = 4$
order 1 $\quad \{1\}$
2 $\quad \{1, \alpha\}$; $\{1, \gamma\}$.
4 $\quad G$.

$\alpha : (a_0, a_1, a_2, a_3) \longmapsto (a_0, -a_1, a_2, -a_3)$



$E = S_{\mathbb{Q}}(x^3 - 2) / \mathbb{Q} = F$
$\parallel \quad r_1 \quad r_2 \quad r_3$
$\mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2})$
$= \mathbb{Q}(\sqrt[3]{2}, w)$.





$$\omega = e^{2\pi i/3} = \cos 120^\circ + i\sin 120^\circ$$
$$= -\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}$$

$\omega + \omega^2 + 1$

$$\omega^3 - 1 = 0$$
$$(\omega - 1)(\omega^2 + \omega + 1) = 0$$
$$\omega^2 + \omega + 1 = 0$$

$|Gal(E/F)| = 6$
$\phi \in G$

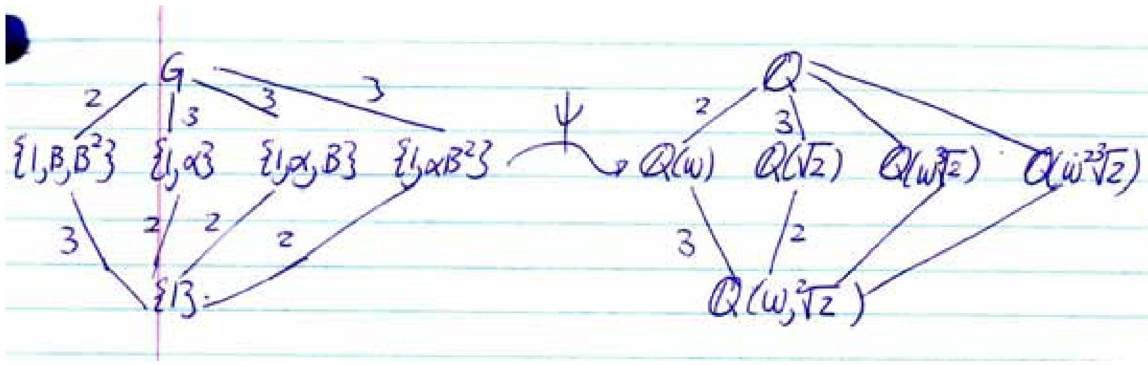
$\phi(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$
$\phi(\omega) \in \{\omega, \bar{\omega} = \omega^2\}$

$\sqrt[3]{2}$	r_1	r_1	r_1	r_2	r_3	r_3	r_2	
$\omega\sqrt[3]{2}$	r_2	r_2	r_3	r_3	r_1	r_2	r_1	
$\omega^2\sqrt[3]{2}$	r_3	r_3	r_2	r_1	r_2	r_1	r_3	
		1	α	β	β^2	$\alpha\beta$	$\alpha\beta^2$	$\beta\alpha = \alpha\beta^2$
	ω	ω	ω^2	ω	ω	ω^2	ω^2	ω^2
	$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega\sqrt[3]{2}$

The only group of order 6 non-abelian is S_3

Subgroup of G Δ

Order
1. $\{1\}$
2. $\{1, \alpha\}$, $\{1, \alpha\beta\}$, $\{1, \alpha\beta^2\}$
3. $\{1, \beta, \beta^2\}$
6. G.


G
{1, β, β²}
{1, α}
{1, αβ}
{1, αβ²}
{1}
ψ
ℚ
ℚ(ω)
ℚ(∛2)
ℚ(ω∛2)
ℚ(ω²∛2)
ℚ(ω, ∛2)