Review

FTOGT K/F Galois with $G = Gal(K/F)$. Then $\exists$
$\cong$ between lattice of subgroups and intermediate fields $H \leftrightarrow E$
such that

- $Gal(K/E) \cong H$
- E/F is Galois $\leftrightarrow H \trianglelefteq G$ in which case $Gal(E/F) \cong G/H$

Highlights of Proof

Def G group, L a field, a linear character is a group homo $\chi : G \to L^*$
Ex $\det : Gl_n(F) \to F$

Thm Let χ_1, χ_2, χ_n be distinct characters, then they are lin ind $/L$.

Proof Choose m minimal and reorder so $a_1\chi_1 + \cdots + a_m\chi_m = 0$, $a_i \neq 0$.
Thus
$$(*)\ a_1\chi_1(g) + \cdots + a_m\chi_m(g) = 0 \quad \forall g.$$

Choose g_0 with $\chi_1(g_0) \neq \chi_m(g_0)$.
$$a_1\chi_1(g_0 g) + \cdots + a_m\chi_m(g_0 g) = 0. \quad \text{So}$$
$$(**)\ a_1\chi_1(g_0)\chi_1(g) + \cdots + a_m\chi_m(g_0)\chi_m(g) = 0.$$

Take $\chi_m(g_0)\cdot(*) - **$ and get relation with fewer $\neq 0$. //

COR R.C.F. problem on HW

COR Distinct field auts of K are linearly independent.

Thm Let $G \overset{\text{finite}}{\leq} \operatorname{Aut} K$. Then $[K : \operatorname{Fix}(G)] = |G|$.

Proof long..

COR $|\operatorname{Aut}(K/F)| \leq [K:F]$

COR $G \leq \operatorname{Aut}(K)$ Then $K/\operatorname{Fix}(G)$ is Galois.

COR $G_1 \neq G_2 \to \operatorname{Fix}(G_1) \neq \operatorname{Fix}(G_2)$

Thm K/F is Galois $\leftrightarrow$ it is splitting field of a separable poly $/F$.
In this case every irreducible in $F[x]$ w/ a root in K is separable and splits. Thus K/F is separable.

Proof $\leftarrow$ done already

$\rightarrow$

Assume K/F Galois, $G = \operatorname{Gal}(K/F)$, $p(x)$ irred w/ root $\alpha \in K$.
Then consider

$$\alpha, g_2(\alpha), \ldots, g_n(\alpha) \qquad g_i \in G$$
$$\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r \qquad \text{distinct roots}$$

Set $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r)$, any $\sigma \in G$ permutes α_i.

Thus $\sigma f = f$ so $f \in F[x] \Rightarrow f(x) = p(x)$ separable, and all roots are in K.

Finally, let $\omega_1, \omega_2, \ldots, \omega_n$ a basis of K, $p_i(x)$ minpoly (ω_i), so $p_i(x)$ separable w/ roots in K.

Take $p_1(x)\cdots p_n(x)$, remove repeats to get sep poly. //

Def K/F Galois, $\alpha \in K$, $\{\sigma\alpha \mid \sigma \in Gal(K/F)\}$ are Galois conjugates

Ex $a+bi$, $a-bi$ $\mathbb{C}/\mathbb{R}$

Rmk TFAE for K/F

1. K/F is spl field of a separable poly $/F$
2. $F = Fix(Aut(K/F))$
3. $[K:F] = |Aut(K/F)|$ = D-F def
4. Finite normal separable extension

$\left.\begin{matrix} \\ \\ \\ \end{matrix}\right\}$ Galois

(normal = spl field)

Example SPL FIELD OF x^8-2

Let $\zeta = e^{2\pi i/8} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i$ Roots are $\{\sqrt[8]{2}\zeta^i \mid 0 \le i \le 7\}$

Thus S.F. $= \mathbb{Q}(\zeta, \sqrt[8]{2}) = \mathbb{Q}(\sqrt[8]{2}, i)$

Rmk $\zeta^4 = -1$ so minpoly $\zeta = x^4+1$ so suggests 32 possible maps,
however it is clear that

$$\begin{array}{c} \mathbb{Q}(\sqrt[8]{2}, i) \\ |\,8 \\ \mathbb{Q}(i) \\ |\,2 \\ \mathbb{Q} \end{array}$$

so degree is 16.

Thus $\sqrt[8]{2} \to \sqrt[8]{2}\zeta^i$ $0 \le i \le 7$
$i \to \pm i$ gives entire Galois group.

Notice $\zeta = \frac{1}{2}(\sqrt[8]{2}^4 + \sqrt[8]{2}^4 i)$

Def

σ: $\sqrt[8]{2} \to \sqrt[8]{2}\,\zeta$, $i \to +i$, $\zeta \to \zeta^5 = -\zeta$

τ: $\sqrt[8]{2} \to \sqrt[8]{2}$, $i \to -i$, $\zeta \to \zeta^7$

Exercise $G = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = e,\ \sigma\tau = \tau\sigma^3 \rangle$
quasi-dihedral ($3 \to 7$ gives dihedral)

Some Fixed Fields

1. $H = \langle \sigma \rangle$ index 2, $H \trianglelefteq G$. Then $E:\mathbb{Q} = 2$
But $\mathbb{Q}(i)$ is fixed, Thus $Fix(H) = \mathbb{Q}(i)$.
$Gal(\mathbb{Q}(i):\mathbb{Q}) \cong G/H$

2. $H = \langle \sigma^4 \rangle$ Now $|H| = 2$, $H = Z(G) \trianglelefteq G$, so $E:\mathbb{Q} = 8$.

σ^4: $\sqrt[8]{2} \to -\sqrt[8]{2}$, $i \to i$, $\zeta \to \zeta$

clearly $\sqrt[4]{2}$, i fixed
$\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q} = 8$ so done!
$^{\kappa}$SF of $x^4 - 2$.

3. $\langle \sigma^2, \tau \rangle \cong D_8$ Fix field $= \mathbb{Q}(\sqrt{2})$
Thus $Gal(\mathbb{Q}(\sqrt[8]{2}, \zeta)/\mathbb{Q}(\sqrt{2})) \cong D_8$

$\langle \sigma^2, \tau\sigma^3 \rangle \cong Q_8$ $Fix = \mathbb{Q}(\sqrt{-2}) = \mathbb{Q}(i\,\zeta^4)$

$Gal(\mathbb{Q}(\sqrt[8]{2}, \zeta)/\mathbb{Q}(\sqrt{-2})) \cong Q_8$

Galois Groups of Polynomials

Recall 1. $\deg f(x) = n$, $f(x)$ separable, $Gal(f(x)) \hookrightarrow S_n$
2. If $f(x)$ is irreducible, then Galois group is transitive on roots

Thm Let $F(s_1, s_2, \ldots, s_n)$ field of rational functions. Then

$$x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + \pm s_n$$ is separable w/ Galois group S_n

COR Over $\mathbb{Q}$, generic poly has Galois group S_n.

Inverse Galois Problem: Let G be finite. Is G a Galois group of some polynomial in $\mathbb{Q}[x]$?

- G is Galois group of some K/F
- ok for S_n, cyclic groups, A_n, solvable groups
- Springer book

Special Cases

1. degree 2 $G = \{e\}$ or $\mathbb{Z}_2$ based on discriminant

2. Cubics : • Reducible $\Rightarrow$ trivial or $\mathbb{Z}_2$
   - Otherwise A_3 or S_3 based on D
   - Formula for roots known

3. Quartics • S_4, A_4, V, D_8 or C_4
   - Formula for roots

FTOA: $\mathbb{C}$ is alg closed

Assume

1. odd degree in $\mathbb{R}[x]$ has real roots (IVT), thus no fin ext of odd deg
2. Quadratics have roots, so no quadratic extensions of $\mathbb{C}$ (quadratic formula)

Proof

Let $f(x) \in \mathbb{C}[x]$. Notice $f(x)\overline{f(x)} \in \mathbb{R}[x]$ so WLOG $f(x) \in \mathbb{R}[x]$

Let $K/\mathbb{R}$ a spl field. Then $K(i)/\mathbb{R}$ is Galois

$$\begin{tikzcd}[column sep=small]
 & K(i) \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & \mathbb{C} \arrow[dl, dash, "2"] \\
 & \mathbb{R} &
\end{tikzcd}$$

Let $G = Gal(K(i)/\mathbb{R})$

Let $P_2 = Syl_2(G)$, so $Fix(P_2):\mathbb{R}$ is odd degree, so trivial

~~Thus $|G| = 2^a$. Thus G has subgr~~oups of

Thus $|G| = 2^a$ so $|Gal(K(i)/\mathbb{C})| = 2^{a-1}$

Thus has subgroup of order 2^{a-2}

$\Rightarrow$ QUADR EXT OF $\mathbb{C}$

//