

$$p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0, \quad a_i \in \mathbb{Q}.$$

roots of  $p$  are  $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{C}$ .

$$\text{Want: } \alpha_i = b_1 + \sqrt[3]{b_2 - \sqrt[5]{b_3 + \sqrt[6]{b_4 - \sqrt{b_5}}}}, \quad b_i \in \mathbb{Q}.$$

(express  $\alpha_i$  by radicals in terms of rationals.

$\{\omega : \omega^n = 1, n \in \mathbb{N}\}$  - roots of unity

Let  $F$  be the field generated by  $\mathbb{Q}$  and roots of unity.

$b_7 \in F$ ,  $F_1 = F(\sqrt[5]{b_7})$  - field generated by  $F$  and  $\sqrt[5]{b_7}$ ,  
extension of  $F$  by  $\sqrt[5]{b_7}$ .

$$F_2 = F(\sqrt[6]{b_2 - \sqrt{b_5}})$$

We get a tower of "radical extensions"

$$\text{s.t. } \forall i, F_{i+1} = F_i(\sqrt[n_i]{c_i})$$

where  $c_i \in F_i$ .

$$\begin{array}{c} F_n \supset K \\ | \\ \vdots \\ | \\ F_2 \\ | \\ F_1 \\ | \\ F \end{array}$$

The goal is to find such a tower that contains all  $\alpha_i$ ,

and so containing  $F(\alpha_1, \dots, \alpha_n)$  - field generated by  $\alpha_i$ .  
 $\parallel$   
 $K$

Note:  $F(\sqrt[n]{c})$  contains all  $n^{\text{th}}$  roots of  $c$ :

$$\beta^n = c \Rightarrow \{\text{all roots of } c\} = \{\omega\beta, \omega^2\beta, \dots, \omega^{n-1}\beta, \beta\}$$

$$\text{where } \omega = \sqrt[n]{1} = e^{2\pi i/n}$$

$\mathbb{Z} \mapsto \bar{\mathbb{Z}}$  permutes roots of  $-1$ .

If  $K$  is an extension of  $F$ , the group

$$\text{Aut}(K/F) = \{\varphi \in \text{Aut}(K) : \varphi|_F = \text{Id}_F\}$$

is the Galois group of the extension.  
 $\text{Gal}(K/F)$

If  $K$  is generated by roots of a poly  $f$ ,

then  $\text{Gal}(K/F)$  is a subgroup of the group of permutations of the roots of  $f$ .

Since any such auto-sm is uniquely defined by its actions on generators.

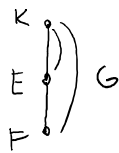
For  $K = F(\sqrt[n]{c})$ ,  $\text{Gal}(K/F)$  is cyclic.

Fundamental Galois Thm: if  $K/F$  is "good", then

Subfields of  $K$  containing  $F$  are in 1-1

Correspondence w/ subgroups of  $\text{Gal}(K/F)$ .

if  $F \subseteq E \subseteq K$ , then  $\text{Gal}(K/E) \trianglelefteq \text{Gal}(K/F)$



if  $\text{Gal}(K/E) \trianglelefteq \text{Gal}(K/F)$ , then

$$\text{Gal}(E/F) = \text{Gal}(K/F) / \text{Gal}(K/E)$$

$K$  is contained in a tower of radical extensions

iff  $\text{Gal}(K/F)$  is a quotient group of a solvable

tower of cyclic groups iff  $\text{Gal}(K/F)$  is solvable.

deg  $P = 4 \Rightarrow \text{Gal} \leq S_4$  ↓ solvable, so  $P$  is solvable in radicals

$$S_3: \quad 1 \triangleleft \mathbb{Z}_3 \triangleleft S_3 \quad S_3/\mathbb{Z}_3 = \mathbb{Z}_2$$

$$S_4: \quad 1 \triangleleft \mathbb{Z}_2 \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$$

$$\quad \quad \mathbb{Z}_2 \quad \quad \mathbb{Z}_2 \quad \quad \mathbb{Z}_3 \quad \quad \mathbb{Z}_2$$

$S_5$ : not solvable.

Field: Integral domain  $\Rightarrow R^\times = R \setminus \{0\}$ .

e.g.  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p, F(x) = \left\{ \frac{p(x)}{q(x)} : p(x), q(x) \in F(x), q(x) \neq 0 \right\}$

no nontrivial ideals, so no factor fields

$\forall$  field hom-sm is injective (Kernel is an ideal, &  $1 \mapsto 1$  so  $\text{Ker} = 0$ ).

Prime subfield: sub field generated by 1

$\hookrightarrow$  it's either  $\underbrace{\mathbb{Z}_p}_{\text{characteristic} = p}$  or  $\underbrace{\mathbb{Q}}_{\text{characteristic} = 0}$ .

If  $F$  is a sub field of  $K$ ,  $K$  is an extension of  $F$ ,

also we write  $K/F$  or  $\begin{smallmatrix} K \\ | \\ F \end{smallmatrix}$ .

Tower of extensions  $K_1/K_2/K_3/\dots/K_n$  or

$\begin{smallmatrix} K_1 \\ | \\ K_2 \\ | \\ \vdots \\ K_n \end{smallmatrix}$

Composite of two ...

extensions:  $K/F$

Sub extensions  $K_1/F, K_2/F$  s.t.  $K_1, K_2 \subseteq K$ .

Then composite  $K_1 K_2 / F$  is minimal subfield of  $K/F$  containing both  $K_1$  &  $K_2$ .  
sub extension

