Apr 9: Field extensions

Announcements

- HW2 due today
- Quiz 1 on Monday

§1. Recap Lagrange's soln

- Can assume
$$f(x) = x^4 + a_2x^2 + a_1x + a_0$$

Assume $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$

$0 = a_3 = -S_1 = -(\alpha_1 + \cdots + \alpha_4)$

$\boxed{\alpha_1+\alpha_2 = -(\alpha_3+\alpha_4)}$

$a_2 = S_2(\alpha_1,\cdots,\alpha_4) = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \cdots$

$a_1 = -S_3$

$a_0 = S_4$

Let $f_1 = (\alpha_1+\alpha_2)(\alpha_3+\alpha_4)$ — orbit of $S_4 \cdot f_1$

$f_2 = (\alpha_1+\alpha_3)(\alpha_2+\alpha_4)$

$f_3 = (\alpha_1+\alpha_4)(\alpha_2+\alpha_3)$

Idea: Solve for f_i's.

$(x-f_1)(x-f_2)(x-f_3) \in \mathbb{Q}[x]$ cubic

coeff. are in $\mathbb{Q}$ as they are polynomials in a_i's.

Then solve for α_i's.

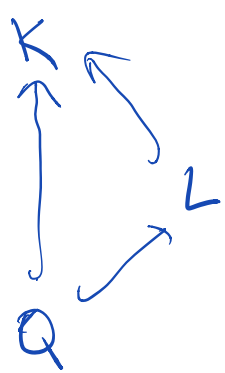
$$\alpha_1 = \frac{\sqrt{-f_1} + \sqrt{-f_2} + \sqrt{-f_3}}{2}$$

High level explanation explaining using Galois theory.

Let $H < S_4$ stabilizer of $f_1 = (\alpha_1+\alpha_2)(\alpha_3+\alpha_4)$

- $H \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ generated by (12) and (34)
- $H \subset S_4$ normal & $S_4/H \cong S_3$ (have surjection $S_4 \twoheadrightarrow S_3$)

Galois theory



K = splitting field of f $= \mathbb{Q}(\alpha_1,\cdots,\alpha_4)$

L = splitting field of cubic $(x-f_1)(x-f_2)(x-f_3)$ $= \mathbb{Q}(f_1,f_2,f_3)$

High level explanation explainly using Galois theory.

Let $H < S_4$ stabilizer of

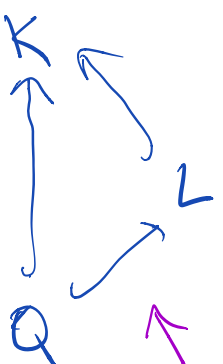
$f_1 = (\alpha_1+\alpha_2)(\alpha_3+\alpha_4)$

- $H \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ generated by (12) and (34)

$H \subset S_4$ normal & $S_4/H \cong S_3$

(have surjection $S_4 \twoheadrightarrow S_3$)

Galois theory



K = splitting field of f
$= \mathbb{Q}(\alpha_1, \dots, \alpha_4)$

L = splitting field of cubic $(x-f_1)(x-f_2)(x-f_3)$
$= \mathbb{Q}(f_1, f_2, f_3)$

Is there a surjection

$S_3 \twoheadrightarrow S_2$?

6 2

kernel $\langle (123) \rangle = \mathbb{Z}/3 \subset S_3$ normal.

- What about $S_5 \twoheadrightarrow S_4$?

No! We will see that this the reason that general quintic won't have soln.

$\rightsquigarrow$ Change direction

§2. Rings, groups & fields

- a ring R has a mult $\times$ and add $+$ satisfying axioms

Note: addition is commutative, mult. may not be

- Say R commutative if mult. is commutative.

- a group G has a mult $\times$

Again, not assume to be commutative.

Say G abelian if it's commutative.

We care about non-abelian gps.

- A field is a comm ring F such that every $x \neq 0 \in F$ has a mult. inverse.

Rmk: F field, then $(F, +)$ group

$(F \setminus 0, \times)$ group

§3. Quotients

① Let G be a group acting on a set X.

Define the quotient

$X/G :=$ set of orbits

An element of X/G is an orbit Gx

$Gx = Gy \in X/G$ iff $y \in Gx$

Have $X \xrightarrow{\pi} X/G$

where $\pi(x) = \pi(y) \in \exists\, Gx = Gy$

$\rightsquigarrow$ We can think X/G as the set X where we identify x and y iff $Gx = Gy$

Abuse notation: Let $x, y \in X$

Say $x = y \in X/G$ iff $Gx = Gy$

Or can be more precise and write $\bar{x} \in X/G$ as image of x.

§3. Quotients

① Let G be a group acting on a set X.

Define the quotient

$X/G :=$ set of orbits

② Consider $H \subset G$ subgroup

Let H act on G via mult.

The quotient of G by H is

$G/H =$ orbits of H acting on G

Here: because H is a subgp, all orbits have the same size.

They look like

$gH = \{gh \mid h \in H\}$ for $g \in G$

$gH = g'H \iff g(g')^{-1} \in H$

Defn $H \subset G$ is normal if

$\forall g \in G$ and $h \in H$ $ghg^{-1} \in H$.

Fact If $H \trianglelefteq G$ is normal, then G/H is a group and $G \to G/H$ is a group hom with kernel H.

Def Say G is solvable if

$\exists \{e\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_k = G$

chain of normal subgps such that

H_{i+1}/H_i abelian.

③ R comm. ring

Say a subset $I \subset R$ is an ideal if

(1) subgp with respect to add

(2) $\forall x \in R, a \in I \quad xa \in I$

The quotient of R by I is

R/I as quotient of abelian group $(R,+)$ by additive subgp $I \subset R$.

FACT R/I is comm ring and $R \to R/I$ is a ring hom

Defn

(1) A field extension $K \to L$ is a hom of fields

(2) $K \hookrightarrow \overline{K}$ (ex: $\mathbb{Q} \subset \mathbb{C}$)

If $\alpha \in \overline{K}$, then

$K(\alpha) :=$ ~~smallest~~ subfield of $\overline{K}$ containing α.

$K \to K(\alpha)$ simple field ext.