(b): Assume $\mathbb{K}$ / degree p, Galois / $\mathbb{F}$ / $\mathbb{Q}(\zeta_p)$, so $G = G(\mathbb{K}/\mathbb{F}) = \langle\sigma\rangle \cong \mathbb{Z}/p\mathbb{Z}$ for some σ (since $|G|=p$).

CLAIM: $\exists$ some $\alpha \in \mathbb{K}$ with $\beta := \alpha + \zeta_p\sigma(\alpha) + \zeta_p^2\sigma^2(\alpha) + \cdots + \zeta_p^{p-1}\sigma^{p-1}(\alpha) \neq 0$.

Assuming the CLAIM for the moment, then note

$$\sigma(\beta) = \sigma(\alpha) + \zeta_p\sigma^2(\alpha) + \zeta_p^2\sigma^3(\alpha) + \cdots + \zeta_p^{p-2}\sigma^{p-1}(\alpha) + \zeta_p^{p-1}\underbrace{\sigma^p(\alpha)}_{=\alpha} = \zeta_p^{-1}\cdot\beta$$

and hence $a := \beta^p$ has $\sigma(a) = \sigma(\beta^p) = \sigma(\beta)^p = (\zeta_p^{-1}\cdot\beta)^p = \underbrace{\zeta_p^{-p}}_{=1}\cdot\beta^p = a$

so $a \in \mathbb{K}^{\langle\sigma\rangle} = \mathbb{K}^{G(\mathbb{K}/\mathbb{F})} = \mathbb{F}$

Also $\beta = \sqrt[p]{a} \notin \mathbb{F}$, else $\sigma(\beta) = \beta$, so $\zeta_p^{-1}\cdot\beta \neq \beta$, $\deg p$ / $\mathbb{F}$, and we'd be done.

4/24/2019 >

To prove the CLAIM, we prove a well-known stronger fact

THEOREM (On linear independence of characters)

For any group H, any set of distinct homomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_n$

$$H \xrightarrow{\sigma_1, \sigma_2, \ldots, \sigma_n} \mathbb{K}^\times$$ into any field $\mathbb{K}$

are $\mathbb{K}$-linearly independent, i.e. $c_1\sigma_1(h) + c_2\sigma_2(h) + \cdots + c_n\sigma_n(h) = 0$ with $c_1, \ldots, c_n \in \mathbb{K}$ $\forall h \in H$

$$\Longrightarrow c_1 = \cdots = c_n = 0.$$

REMARKS: ① This proves the CLAIM taking $H = \mathbb{K}^\times$ and $\sigma_1, \sigma_2, \ldots, \sigma_n$ to be $1, \sigma, \sigma^2, \ldots, \sigma^{p-1}$

② It also proves for any finite extension $[\mathbb{K}:\mathbb{F}] < \infty$ that $|G(\mathbb{K}/\mathbb{F})| \leq [\mathbb{K}:\mathbb{F}]$ without assuming $\mathrm{char}(\mathbb{F}) = 0$, ($|\{\sigma_1, \ldots, \sigma_n\}|$) using a little work/thought.

proof of THM: Pick a nontrivial dependence $c_1\sigma_1(h) + \cdots + c_{m-1}\sigma_{m-1}(h) + c_m\sigma_m(h) \overset{(*)}{=} 0$ $\forall h \in H$ with $c_1, \ldots, c_m$ all nonzero and m smallest.

We'll produce a nontrivial dependence with smaller m, giving a contradiction.

(104) Since $\sigma_1 \neq \sigma_m$, pick $h_0 \in H$ with $\sigma_1(h_0) \neq \sigma_m(h_0)$ in K.

Then $c_1\sigma_1(h_0h) + \cdots + c_{m-1}\sigma_{m-1}(h_0h) + c_m\sigma_m(h_0h) = 0 \quad \forall h \in H$

so $c_1\sigma_1(h_0)\sigma_1(h) + \cdots + c_{m-1}\sigma_{m-1}(h_0)\sigma_{m-1}(h) + c_m\sigma_m(h_0)\sigma_m(h) = 0 \quad \forall h \in H$

and multiply (*) by $\sigma_m(h_0)$ gives

$c_1\sigma_m(h_0)\sigma_1(h) + \cdots + c_{m-1}\sigma_m(h_0)\sigma_{m-1}(h) + c_m\sigma_m(h_0)\sigma_m(h) = 0 \quad \forall h \in H$

which subtracting gives

$$\underbrace{c_1}_{\neq 0}\underbrace{(\sigma_1(h_0) - \sigma_m(h_0))}_{\neq 0}\sigma_1(h) + \cdots + c_{m-1}(\sigma_{m-1}(h_0) - \sigma_m(h_0))\sigma_{m-1}(h) + 0 = 0 \quad \forall h \in H$$

at most $m-1$ terms ∎

§16.12 Solvability by radicals

We know how to solve $x^2 + bx + c = 0$ via $x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$

and a cubic $x^3 + ax^2 + bx + c = 0$

can be reduced using $\left(x + \frac{a}{3}\right)^3 = x^3 + 3\left(\frac{a}{3}\right)\cdot x^2 + 3\left(\frac{a}{3}\right)^2 \cdot x + \left(\frac{a}{3}\right)^3$
$= x^3 + ax^2 + \cdots$

to $\left(x + \frac{a}{3}\right)^3 + b'x + c' = 0$ for some b', c'

i.e. $f(x) = x^3 + bx + c = 0$ is good enough, where

Cardano's formula works: (see end of §16.11)

$$x = \sqrt[3]{-\frac{c}{2} + \sqrt{\frac{D}{108}}} + \sqrt[3]{-\frac{c}{2} - \sqrt{\frac{D}{108}}}$$

where $D = D(f) = 4c^2 + 27b^3$

(choices of $\sqrt[3]{(-)}$ yoked together in a certain way...)

Q: Are there such iterated radical formulas for roots of $f(x) = 0$ when $\deg(f) = 4, 5, 6, \ldots$?

YES | NO

← | →

DEFIN: (16.12.2(a)) Given $\mathbb{F} \subset \mathbb{C}$ and $\alpha \in \mathbb{C}$, say α is solvable (by radicals) over $\mathbb{F}$ if $\exists$ a tower $\mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_r \ni \alpha$ with $\mathbb{F}_i = \mathbb{F}_{i-1}(\sqrt[n_i]{a_i})$ for some n_i and $a_i \in \mathbb{F}_{i-1}$, where $\mathbb{F}_0 = \mathbb{F}$.

Note that one can always assume each n_i is a prime p_i since if $n = p_1 p_2 \cdots p_m$ then $\sqrt[n]{a} = \sqrt[p_m]{\cdots \sqrt[p_2]{\sqrt[p_1]{a}}}$

e.g. $\sqrt[12]{a} = \sqrt[3]{\sqrt[2]{\sqrt[2]{a}}}$

We'll show the forward implication in the following:

THEOREM (Galois) For $\mathbb{F} \subset \mathbb{C}$ and $f(x) \in \mathbb{F}[x]$,

all roots of $f(x)$ are solvable $\iff$ $G := G(\mathbb{K}/\mathbb{F})$ where $\mathbb{K} = \text{split}_{\mathbb{K}}(f(x))$ is a solvable group:

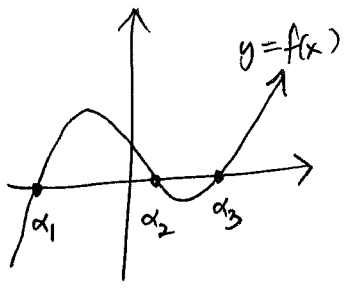
DEFN: $\exists$ subgroups $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G$ with G_i/G_{i-1} cyclic

We'll also show that when $\deg(f(x)) = 5$, so $G \leq S_5$,

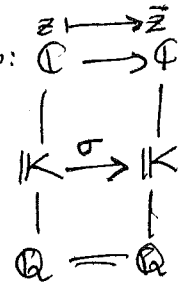
THEOREM: $G = S_5$ and A_5 are both not solvable.

But there are definitely $f(x)$ achieving $G = S_5$ (in fact most do!)

EXAMPLE: $f(x) = x^5 - 16x + 2 \in \mathbb{Q}[x]$ has 3 real roots $\alpha_1, \alpha_2, \alpha_3$
2 complex conjugate roots $\alpha_4 = \overline{\alpha_5} \in \mathbb{C} - \mathbb{R}$



This implies $G = G(\mathbb{K}/\mathbb{F})$ contains the transposition $(\alpha_4\ \alpha_5)$ by restricting conjugation:



It also contains elements $\sigma \in G$ of order 5 since $|G| = [\mathbb{K}:\mathbb{Q}] = [\mathbb{K}:\mathbb{Q}(\alpha_1)][\mathbb{Q}(\alpha_1):\mathbb{Q}]$, with $[\mathbb{Q}(\alpha_1):\mathbb{Q}] = 5$, by Cauchy or Sylow's Theorems.

But $\sigma \in G \leq S_5$ of order 5 $\Rightarrow$ σ is a 5-cycle $(a\ b\ c\ d\ e)$, which together with the transposition $(\alpha_4\ \alpha_5)$ will generate S_5. So $G = S_5$ (EXER. 16.12.8)