4.1.16 $\mathrm{ch}\,\mathbb{Q}=0$ より　$f(x)$ は分離多項式

よって　$f(x)$ の相異なる　p 個の解を $\{\alpha_1, \alpha_2, \cdots, \alpha_p\}$ とおく。

このとき、条件から　α_1, α_2 以外はすべて実数解としてよい。

$f(x)$ の $\mathbb{Q}$ 上の最小分解体を L とすると　$L \supset \mathbb{Q}(\alpha_1) \supset \mathbb{Q}$ より

$$[L:\mathbb{Q}] = [L:\mathbb{Q}(\alpha_1)][\mathbb{Q}(\alpha_1):\mathbb{Q}]$$
$$= [L:\mathbb{Q}(\alpha_1)]\,p$$

よって　$[L:\mathbb{Q}] = |\mathrm{Gal}(L/\mathbb{Q})|$ は p の倍数となる。

ここで、$\mathrm{Gal}(L/\mathbb{Q})$ の $\{\alpha_1, \cdots, \alpha_p\}$ への作用によって、置換表現 ρ を定める。

$$\rho : \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow \mathfrak{S}_p$$

L は $\mathbb{Q}$ 上 $\{\alpha_1, \cdots, \alpha_p\}$ で生成されるので、$\ker\rho = \{1\}$ で　単射である。工藤

$|\mathrm{Gal}(L/\mathbb{Q})|$ は p の倍数より　~~コーシーの定理より~~ シロー p 部分群の定理の系に書いてある。

位数 p の元 $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ が存在する。　$\rho(\sigma)$ の位数は　ρ が単射より

p であるがこれは長さ p の巡回置換となる

故に　$\rho(\sigma) = (1\ \beta_2\ \beta_3\ \cdots\ \beta_p)$　とおける。（$\beta_2, \cdots, \beta_p$ は $2 \sim p$ の相異なる整数）

複素共役　$\tau \in \mathrm{Gal}(L/\mathbb{Q})$ については明らかに　$\rho(\tau) = (1\,2)$

ここで　$\rho(\sigma)^i$ の $1, 2$ の行き先は i によって互いに異なるので、$(i = 1, \cdots, p-1)$

$\rho(\sigma)^i (1\,2)\, \rho(\sigma)^{-i}$ を各 i について考えることで、

$(1\,2), (2\,r_2), (3\,r_3), \cdots, (p\,r_p) \in \mathrm{Im}\,\rho$

ただし、$(r_2, r_3, \cdots, r_p$ は 2 ではない、1 から p の相異なる整数）

このとき　$r_2 \neq 1$ であることを示す。

$\rho(\sigma)^i = (1\ \beta_2\ \cdots\ \beta_p)^i$　となっているが、

$r_2 = 1$ ならば、ある i に対して　$\rho(\sigma) = (\underbrace{1 \cdots}_{i\text{個}} \underbrace{2 \cdots}_{i\text{個}}\ \beta_{?})$　（p 個）

すなわち　$i + i \equiv 2i \equiv 0 \pmod p$　となる。

p は奇素数より　$i \equiv 0 \pmod p$　となるが

$i < p$ で p は素数なり矛盾　よって　$r_2 \neq 1$

$p = 2$ のときは実際に $(2\,1)$ のこと。$((1\,2)(1\,2)(1\,2)^{-1} = (1\,2)$ となり $r_2 \neq 1$ とは言えない

よって　$(2\,r_2)(1\,2)(2\,r_2)^{-1} = (1\,r_2)$

さらに　$(3\,r_3), \cdots, (p\,r_p)$ の中から　$r_2 \neq 1, 2$ より

$(r_2\ r_2')$ となるものを選べる。このとき　$r_2' \neq 2, r_2$ で

先ほどと同様の議論により　$r_2' \neq 1$

よって　$(r_2\ r_2')(1\,r_2)(r_2\ r_2')^{-1} = (1\,r_2')$

これを繰り返して　互換 $(1\,2), (1\,3), \cdots, (1\,p) \in \mathrm{Im}\,\rho$ である

さらに $(n\,m)$　[n, m は相異なる $2 \sim p$ の整数] について

$(1\,m)(1\,n)(1\,m)^{-1} = (m\,n)$　となる。

よって　$\mathrm{Im}\rho$ は $\mathfrak{S}_p$ のすべての互換を含むので

$\mathrm{Im}\rho \supset \mathfrak{S}_p$ となり　$\mathrm{Im}\rho = \mathfrak{S}_p$

したがって　$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathfrak{S}_p$ である

$p=2$ のときも別個に証明すれば成り立つことが分かる。

どれも位数2の部分群は $H \cong \mathfrak{S}_2$ である。

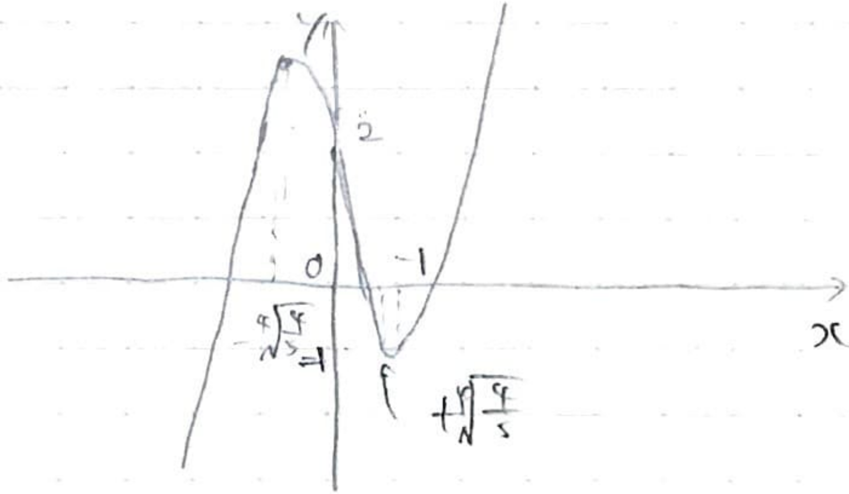
(2)　x^5-4x+2 は アイゼンシュタインの判定法より既約

$f(x)=x^5-4x+2$ であるとき　$f'(x)=5x^4-4$

よって　増減表は

x	$-\infty$	$\cdots$	$-\sqrt[4]{\frac{4}{5}}$	$\cdots$	0	$\cdots$	$+\sqrt[4]{\frac{4}{5}}$	$\cdots$	$+\infty$
$f'(x)$	$+$	$+$	0	$-$	$-$	$-$	0	$+$	$+$
$f(x)$	$-\infty$	↗		↘	2	↘		↗	$+\infty$

グラフは



よって　$f(x)=0$ の実数解は3つ

(1)より　題意は示された。