(521) Supplement: S_p as Gal gr / $\mathbb{Q}$

(P) Let $f \in \mathbb{Q}[x]$ be irred, $\deg f = p$ prime, f w/ 3 real roots & 2 non-real. Then Gal gr of f is S_p

Pf. $p \mid |\text{Gal}| \Rightarrow G = \text{Gal} \ni$ elt of ord p by Sylow $\Rightarrow G \ni (123\ldots p)$ (blc any perm in S_p has ord the lcm of the lengths of its cycles. But complex conj $\in G$ so a transp $\tau \in G$. But $S_p = \langle \sigma, \tau \rangle$.

(EG) $f(x) = x^5 - 4x - 2$ has Gal gr S_5 so not sol by rads

(T) Let $f \in \mathbb{Z}[x]$ monic & p prime, $\bar{f}_p \in \mathbb{F}_p[x]$. Ass $\bar{f}$ has no mult roots in $\overline{\mathbb{F}_p}$. Then $\exists$ bij $S = \{\alpha \in \mathbb{C} \mid f(\alpha) = 0\} \xrightarrow{\sim} \{\bar{\alpha} \in \overline{\mathbb{F}_p} \mid \bar{f}_p(\bar{\alpha}) = 0\} = \bar{S}$ & an emb $G_{\bar{f}_p} \hookrightarrow G_f$ of Gal grs / $\mathbb{Q}$ & $\mathbb{F}_p$ resp s.t. the actions of $G_{\bar{f}_p}$ & G_f on S & $\bar{S}$ corr to each other. [Pf: via rings of ints]

(EG) $f(x) = x^5 - x + 1$ irr in $\mathbb{Q}[x]$ blc $\bar{f}_5$ irr in $\mathbb{F}_5[x]$ (+ Gauss).

Now mod 2, $\bar{f}_2 = (x^2 + x + 1)(x^3 + x^2 + 1) \in \mathbb{F}_2[x]$.

$\Downarrow$

$G_f \ni (12345)$

Since $(2,3) = 1$, $G_{\bar{f}_2} \ni \text{Frob} = (ij)(klm)$. Now cube of $\Rightarrow$ is a transp.

So $G_f = S_5$.

Frob permutes roots of $x^2 + x + 1$ & permutes cyclically roots of $x^3 + x^2 + 1$. (blc it cannot fix any of the roots, blc $\bar{f}$ irr).

(D) If $f \in K[x]$, $f = \prod (x - x_i)$, $D(f) = \prod_{i<j} (x_i - x_j)^2$, $x_i \in \bar{K}$. (P) $D(f) \in K$

(P) $f = x^2 + bx + c \Rightarrow D(f) = b^2 - 4c$

$f = x^3 + ax + b \Rightarrow D(f) = -(4a^3 + 27b^2)$

(P) $G_f = S_3 \Leftrightarrow D(f)$ not a $\square$ in K