14.8 Computation of Galois groups over $\mathbb{Q}$.

Idea. Get information about permutations in the Galois group of $f(x) \in \mathbb{Q}[x]$ by reduction to finite fields.

Wlog, let $f(x) \in \mathbb{Z}[x]$ be separable with roots $\alpha_1, \ldots, \alpha_n$.
Then
$$D(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in \mathbb{Z}.$$
Let p be prime such that $p \nmid D(f)$. Let $\bar{f}(x) \in F_p[x]$ be induced by $f(x)$ mod p.
Then $D(\bar{f}) \neq 0$ in F_p and $\bar{f}(x)$ is separable.

Theorem. *Let $f \in \mathbb{Z}[x]$ separable, p prime such that $p \nmid D(f)$, and*
$$Z_0 := \{\alpha \in \bar{\mathbb{Q}} \; : \; f(\alpha) = 0\},$$
$$Z_p := \{\beta \in \bar{F}_p \; : \; \bar{f}(\beta) = 0\}.$$
Then $\underbrace{\mathrm{Gal}(F_p(Z_p)/F_p)}_{=: G_p}$ *embeds into* $\underbrace{\mathrm{Gal}(\mathbb{Q}(Z_0)/\mathbb{Q})}_{=: G_0}$ *respecting the action on roots.*
Without proof. (algebraic number theory)

Have $\varphi : G_p \hookrightarrow G_0$, $\pi : Z_p \to Z_0$ bijection
such that $\forall g \in G_p \, \forall \alpha \in Z_p : \pi(g\alpha) = \varphi(g)\, \pi(\alpha)$

Corollary. *Assume $\bar{f}(x) = \bar{f}_1(x) \cdots \bar{f}_k(x)$ for distinct irreducible $\bar{f}_1(x), \ldots, \bar{f}_k(x)$ over F_p.*
Then there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}(Z_0)/\mathbb{Q})$ with cycle type $(\deg \bar{f}_1, \ldots, \deg \bar{f}_k)$.

Proof.

Corollary. *For each $n \in \mathbb{N}$, there exist $f(x) \in \mathbb{Z}[x]$ with Galois group S_n over $\mathbb{Q}$.*

Proof.

Fact. If a transitive $H \leq S_n$ contains an $(n-1)$-cycle and a transposition, then $H = S_n$.

Ex $\langle (1234), (13) \rangle \neq S_4$

Let $f_1 \in F_2[x]$ irreducible, $\deg f_1 = n$.

$f_2 \in F_3[x]$, $f_2 = g \cdot h$ for g irred, $\deg g = 2$, and h a product of irreducibles of odd degree.

$f_3 \in F_5[x]$, $f_3 = x \cdot p$ for p irreducible, $\deg p = n-1$.

Let $f(x) \in \mathbb{Z}[x]$ such that

1) f mod $2 = f_1$
2) f mod $3 = f_2$
3) f mod $5 = f_3$

$f(x)$ exists by Chinese Remainder Thm

Let G be the Galois group of $f(x)$ over $\mathbb{Q}$.

Then by 1) f is irreducible, G contains an n-cycle and hence is transitive on the n roots of $f(x)$.

by 2) G contains a transposition.

by 3) G contains an $(n-1)$ cycle.

Thus $G = S_n$ by Fact above. $\square$