Theorem 6.1 (Dedekind)

Suppose $f \in \mathbf{Z}[X]$ is a monic polynomial of degree n with distinct roots in a splitting field (i.e. discriminant $D \neq 0$). Suppose p is a prime such that the reduction $\bar{f}$ of f mod p also has distinct roots (i.e. p does not divide D). If $\bar{f} = g_1 \dots g_M$ is the factorization of $\bar{f} \in \mathbf{F}_p[X]$ into distinct irreducible factors, with $\deg g_i = r_i$, then $\mathrm{Gal}(f) \leq S_n$ has an element of cycle type $(r_1, \dots, r_M)$.

Proof (non-examinable). Given f as in the statement of (6.1) with roots $\alpha_1, \dots, \alpha_d$, we set $L = \mathbf{Q}(\alpha_1, \dots, \alpha_d)$ its splitting field. Note that $L/\mathbf{Q}$ is finite (say of degree N) with a spanning set (**not** usually a basis)

$$\{\alpha_1^{i_1} \dots \alpha_d^{i_d} \ : \ 0 \leq i_j < d\}. \qquad (*)$$

Because $f \in \mathbf{Z}[X]$ is a monic polynomial, these also form a set of generators for the ring $R = \mathbf{Z}[\alpha_1, \dots, \alpha_d]$ considered as a $\mathbf{Z}$-module, i.e. an abelian group. So $R \subset L$ is a torsion-free finitely generated abelian group of some rank r, i.e. $R \cong \bigoplus_{i=1}^{r} \mathbf{Z}$, and the Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ acts on R by permuting the α_i.

Taking (free) generators of this free abelian group, and the corresponding elements $a_1, \dots, a_r \in R$, then these are also linearly independent over $\mathbf{Q}$, i.e. are linearly independent in $L/\mathbf{Q}$. Therefore $r \leq N = [L : Q]$.

However, given a basis $e_1, \dots, e_N$ for $L/\mathbf{Q}$, note that each e_i may be written in terms of a linear combination of the spanning set $(*)$ with coefficients in $\mathbf{Q}$, and hence by taking appropriate multiples we may assume that all the $e_i \in \mathbf{R}$. Hence $e_1, \dots, e_N$ are independent elements of the above free abelian group, and so $N \leq r$.

Summing up: R is a free abelian group of rank $N = [L : \mathbf{Q}]$, with $R = \bigoplus_{i=1}^{N} \mathbf{Z}e_i$, for suitable $e_1, \dots, e_N \in R$. Moreover $pR \neq R$ and R/pR is a finite ring with p^N elements.

Now choose a maximal ideal of R/pR (Zorn's lemma clearly not needed for this!), yielding a maximal ideal $P \lhd R$ with $P \supseteq pR$. The quotient ring $F = R/P$ is then a finite field of characteristic p, since $\mathbf{Z} \hookrightarrow R$ induces a field homomorphism $\mathbf{Z}/p\mathbf{Z} \hookrightarrow R/P$, a finite extension of degree m say. Under the quotient homomorphism $\phi : R \to F$, the factorization $f = \prod_i (X - \alpha_i)$ is mapped to a factorization $\bar{f} = \prod_i (X - \bar{\alpha}_i)$, where $\bar{\alpha}_i = \phi(\alpha_i)$ and $F = \mathbf{F}_p(\bar{\alpha}_1, \dots, \bar{\alpha}_d)$, where by assumption the $\bar{\alpha}_i$ are also distinct. So we have a bijection specified between the roots of f in L and the roots of $\bar{f}$ in F.

The action of G on R (permuting the α_i) descends to an action on R/pR; let $H' \leq G$ be the subgroup sending the maximal ideal P to itself. Therefore any $\sigma \in H'$ gives rise to an automorphism of F over $\mathbf{F}_p$ defined by $x + P \mapsto \sigma(x) + P$, giving a homomorphism $H' \to H := \mathrm{Gal}(F/\mathbf{F}_p)$. Moreover an element of $H' \leq S_d$ has the **same** cycle type as its image in $H = \mathrm{Gal}(F/\mathbf{F}_p) \leq S_d$, and so in particular the above homomorphism $H' \to H$ is injective.

If we can prove that $H' \hookrightarrow H$ is surjective also, there then exists $\sigma' \in H'$ with the same cycle type as the Frobenius generator of H, which we saw before cyclically permutes the roots of each g_j, and so has cycle type $(r_1, \ldots, r_M)$ as claimed. We are therefore reduced to proving:

MAIN CLAIM. The map $H' \hookrightarrow H$ is a bijection.

Let $\{P_i \ : \ 1 \leq i \leq s\}$ denote the set of maximal ideals containing pR (or, recalling the well-known result that a finite integral domain is a field, equivalently the set of prime ideals containing pR), and let $m_i := [R/P_i : \mathbf{F}_p]$ for each i. If $P_1 = P$, then $m_1 = m$.

Now apply the Chinese Remainder Theorem:

$$R/\bigcap_{i=1}^{s} P_i \cong R/P_1 \times \cdots \times R/P_s,$$

where the LHS has order $\leq |R/pR| = p^N$ and the RHS has order p^t, where $t = \sum_{i=1}^{s} m_i$. Therefore $N \geq \sum_{i=1}^{s} m_i$.

Suppose images of P under G are $\{P_1 = \sigma_1(P), \ldots, P_r = \sigma_r(P)\}$, where $r \leq s$ and with say $P_1 = P$, then we have induced isomorphisms $\bar{\sigma}_i : R/P \to R/P_i$ for $1 \leq i \leq r$. Thus for $1 \leq i \leq r$,

$$m_i = [R/P_i : \mathbf{F}_p] = [R/P : \mathbf{F}_p] = m = |H|.$$

In particular $N \geq rm$.

But $|H| \geq |H'|$ implies that $rm = r|H| \geq r|H'| = |G|$ by the orbit–stabilizer theorem, where $|G| = N$. Thus $rm = N$ and $|H'| = N/r = m = |H|$. Therefore the identification $H' \hookrightarrow H$ is an isomorphism, proving the MAIN CLAIM, and hence the theorem.

Remark. In fact, we have also shown above that $r = s$ and that $\bigcap_{i=1}^{s} P_i = pR$.