Algebra II: Galois gps. of over some nice fields

Thm: Let $f(x) \in F[x]$ have simple roots, $G := Gal(f) = Gal(Split(f)/F)$. Suppose the orbits of G acting on f have $m_1, \dots, m_r$ elts, resp. Then $f = f_1 \cdots f_r$, f_j irred. of deg. m_j.

Pf: Assume f monic, with roots $\alpha_1, \dots, \alpha_m$, $m = \deg(f)$ over $K := Split(f)$. The monic factors of $f(x)/K$ correspond to subsets $S \subseteq \{\alpha_1, \dots, \alpha_m\}$

$$S \longleftrightarrow f_S = \prod_{\alpha \in S} (x - \alpha)$$

and f_S fixed by action of G (i.e. has coeffs in F) $\iff$ S is stable under G. Thus, the irred. factors of f in $F[x]$ are the polys f_S corr. to min subsets S stable under G, which are just the orbits of G on $\{\alpha_1, \dots, \alpha_m\}$.

To study $/\mathbb{Q}$, often combine with mod p info.

If F is finite of char p, then $G = Gal(f)$ is cyclic generated by $Frob_p$. Any $\sigma \in G$, as a permutation on the roots of f, the distinct orbits of σ corr. to factors in its cycle decomp. Thus, if $f = f_1 \cdots f_r$ is its factorization into distinct irreducibles, $\deg(f_j) = m_j$, then σ has cycle type $m_1, \dots, m_r$.

Lemma: R is a UFD with field of fractions F. $f(x) \in R[x]$ monic, P a prime ideal of R, $\bar{f}$ is the image of f in $(R/P)[x]$. If $f, \bar{f}$ have simple roots. Then the roots $\alpha_1, \dots, \alpha_n$ of f lie in a finite ext^n $R' \supseteq R$, and the reductions $\bar{\alpha}_i$ modulo PR' are the roots of $\bar{f}$! Moreover, $\mathrm{Gal}(\bar{f}) \subseteq \mathrm{Gal}(f)$, considered as subgps of $\mathrm{Sym}\{\alpha_1, \dots, \alpha_n\} = \mathrm{Sym}\{\bar{\alpha}_1, \dots, \bar{\alpha}_n\}$

Pf: Skip

combining $\rightsquigarrow$ **Theorem (Dedekind):** If $f(x) \in \mathbb{Z}[x]$ is monic of degree n, p a prime with $f \bmod p$ having simple roots ($\Leftrightarrow p \nmid \mathrm{disc}(f)$)

Suppose $\bar{f} = \prod f_i$, f_i irred of deg. n_i / $\mathbb{F}_p[x]$

Then $\mathrm{Gal}(f)$ has an elt of cycle type $\{n_i\}$

Ex: $f(x) = x^5 - x - 1$. $p \neq 2$.

Mod 2: $\bar{f} = x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$

mod 3: $\bar{f} = x^5 + 2x + 2$ is irreducible

$\rightsquigarrow$ $\mathrm{Gal}(f)$ contains $(ik)(lmn)$ and (12345)

$\Rightarrow$ also $(ik)(lmn)^3 = (ik) \Rightarrow G = S_5$.

Lemma: Transitive subgps of S_n containing a transposition and an $(n-1)$-cycle are S_n.

Pf: Assume by renumbering we have $(123\cdots(n-1))$ in the subgp. By transitivity, can transform the transposition into (in), some $1 \le i \le n-1$. Conjugating (in) by $(123\cdots(n-1))$ & its powers gives $(1n), (2n), \ldots, (n-1, n)$, which generate S_n.

Ex: Prove monic integral polys f_1, f_2, f_3 of deg. n s.t. 1). f_1 is irred. mod 2.

2). $f_2 \equiv$ (degree 1)·(irred. of deg. $n-1$) mod 3.

3). $f_3 \equiv$ (irred. of deg. 2)(product of 1 or 2 irred polys of odd degree) mod 5.

4). f_1, f_2, f_3 have simple roots.

Take $f = -15f_1 + 10f_2 + 6f_3$.

Then 1) $\Rightarrow$ $\mathrm{Gal}(f)$ is transitive (contains n-cycle as $f \equiv f_1 \pmod 2$ is irred)

2) $\Rightarrow$ $\mathrm{Gal}(f)$ has an $(n-1)$-cycle ($f \equiv f_2 \pmod 3$)

3) $\Rightarrow$ has a transposition (contains a prod of a trans. & commuting elt of odd order $\rightsquigarrow$ raise to correct odd power gives trans)

Lemma $\Rightarrow$ $\mathrm{Gal}(f) = S_n$

General Strategy: over $\mathbb{Q}$:

1). Factor f mod a sequence of primes not dividing $\mathrm{disc}(f)$ to find cycle types of elts of $\mathrm{Gal}(f)$.

Guaranteed to find primes giving those orders after not "too long" (Effective Chebotarev density)

2). Look up or classify the transitive subgps of S_n with order divisible by n + cycle types.

3). If this is insufficient, look at action on sets of subsets of r roots for some r.

Ex: $f(x) = x^5 - 2x + 7$. $G := \mathrm{Gal}(f)$.

mod 2: $\bar{f} = x^5 + 1 = (x+1)(x^4+x^3+x^2+x+1)$ ← Sep mod 2.

↠ check: $x^4+x^3+x^2+x+1$ irred. mod 2.

$\Rightarrow$ G contains a 4-cycle.

mod 7 (natural to try):

$\bar{f} = x^5 - 2x = x(x^4-2) = x(x^4-9) = x(x^2-3)(x^2+3)$

$= x(x^2-4)(x^2-3) = x(x^2-3)(x-2)(x+2)$

$\Rightarrow$ G contains a transposition

mod 13: check $\bar{f}$ irred. mod 13 $\Rightarrow$ f irred. / $\mathbb{Q}$

$\Rightarrow$ G transitive

$\Rightarrow$ $\boxed{G \cong S_5}$.