Project graded
H/W 7 due Tues. 3/14
Final exam: Thurs. 3/23 8:30-11:30 Room 200-205 (see email)

---

Thm (Cardano & others, 1545):

$x^3+px+q=0$ has sol'ns

$$x = \underbrace{\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}}_{A} + \underbrace{\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}}_{B} \quad \text{s.t. } AB=-p$$

$$A^3 = \frac{1}{27}(\alpha, \rho), \quad B^3 = \frac{1}{27}(\alpha, \rho^2)$$

Quartic: Solve resolvent cubic, then roots of quartic can be expressed as sums of square roots of these roots (see notes from last time)

---

Today: §14.8: Galois gps. / $\mathbb{Q}$
Wed: §14.9: Infinite ext'ns
Fri: Review OR further topic (Kummer ext'ns or connections to modular forms)

---

Note: Galois gps. are canonically subgps. of symmetric gps. (up to conjugation) by viewing automorphisms as permutations of the roots.

Def: $H_1, H_2 \leq S_n$ are <u>permutation isomorphic</u> if $\exists$ bijection $\{1,..,n\} \xrightarrow{\varphi} \{1,..,n\}$ s.t. $\sigma \longmapsto \varphi\sigma\varphi^{-1}$ is an isom $H_1 \xrightarrow{\sim} H_2$.

Example: $n=4$.

$\langle \overset{\sigma}{(12)} \rangle$ and $\langle \overset{\sigma'}{(23)} \rangle$ are permutation isomorphic.

Let $\varphi: \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \\ 4 \mapsto 4 \end{array}$ $\quad \varphi^{-1}: \begin{array}{l} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \\ 4 \mapsto 4 \end{array}$ $\quad \varphi\sigma\varphi^{-1}: \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \\ 4 \mapsto 4 \end{array} = \sigma'$

But

$\langle (12) \rangle$ and $\langle (12)(34) \rangle$ are not perm. isom.

Prop: If $H_1, H_2$ perm. isom., then $\exists$ isom. $H_1 \xrightarrow{\sim} H_2$ s.t. every pair of elts has the same cycle type.

---

Let $f(x) \in \mathbb{Z}[x]$, $f$ sep, $\deg f = n$. Then, $D \in \mathbb{Z}_{\neq 0}$. Let $p$: prime, $p \nmid D$. Let $\bar{f}(x) \in \mathbb{F}_p[x]$ be the reduction of $f$ mod $p$. Then, $\bar{f}$ sep.

Thm (see Lang VII, Thm 2.9): $\mathrm{Gal}_{\mathbb{F}_p}(\bar{f})$ is perm. isom. to a subgp. of $\mathrm{Gal}_{\mathbb{Q}}(f)$.

Let $f = \underbrace{\bar{f}_1 \cdots \bar{f}_k}_{\substack{\text{irred. of} \\ \deg n_i}} \in \mathbb{F}_p[x]$

Recall: $\mathrm{Gal}(\bar{f})$ is cyclic. (Prop. 15)

Let $\langle \sigma \rangle = \mathrm{Gal}(\bar{f}) \subseteq S_n$

$$\sigma = \underbrace{(\quad\quad)}_{n_1} \underbrace{(\quad)}_{n_2} \cdots \underbrace{(\quad)}_{n_k}$$

Cor 41: $\exists\, \sigma \in \mathrm{Gal}(f)$ s.t. $\sigma$ has cycle type $(n_1, \dots, n_k)$.

Ex: $f(x) = x^5 - x - 1$, $D = 2869 = 19 \cdot 151$

$p = 2$: $f(x) = (x^2 + x + 1)(x^3 + x^2 + 1)$

$p = 3$: $f(x)$ irred.

$\mathrm{Gal}(f)$ contains a $(2,3)$-cycle $\sigma = (ab)(cde)$, $\sigma^3 = (ab)$ transposition

and a 5-cycle. So $\mathrm{Gal}(f) = S_5$.

**Prop 42:** For all $n \in \mathbb{Z}_{\geq 1}$, $\exists$ infinitely many (primitive) polys. $f(x) \in \mathbb{Z}[x]$ s.t. $\mathrm{Gal}_{\mathbb{Q}}(f) = S_n$

Pf sketch:

Fact: If $H \leq S_n$, $H$ transitive, $H$ contains 2-cycle, $(n-1)$-cycle, then $H = S_n$.

Let

$$f_2(x) = (\text{irred. deg. } n) \in \mathbb{F}_2[x]$$

$$f_3(x) = \begin{cases} (\text{irred. deg. } 2)(\text{irred. deg. } n-2), & \text{if } n \text{ odd} \\ x(\text{irred. deg. } 2)(\text{irred. deg. } n-3), & \text{if } n \text{ even} \end{cases} \in \mathbb{F}_3[x]$$

$$f_5(x) = x(\text{irred. deg. } n-1)$$

By the Chinese Remainder Thm. (for polys.) $\exists f(x) \in \mathbb{Z}[x]$ s.t.

$$f(x) \equiv f_2(x) \bmod 2 \leftarrow \text{transitive}$$

$$f(x) \equiv f_3(x) \bmod 3 \leftarrow \text{2-cycle}$$

$$f(x) \equiv f_5(x) \bmod 5 \leftarrow (n-1)\text{-cycle.}$$

Thus, $\mathrm{Gal}(f) = S_n$.

Cor 41 is good for showing Gal(f) is <u>large</u>, not so good for showing it's <u>small</u>.

Def: Let $A \subseteq \mathbb{N}$, $B \subseteq A$. We say the <u>density</u> of $B$ in $A$ is $\alpha \in [0,1]$ if

$$\lim_{N \to \infty} \frac{|B \cap \{1, \ldots, N\}|}{|A \cap \{1, \ldots, N\}|} = \alpha.$$

Let $\deg f = n$, and let $T$ be a "cycle-type". Let $A$ be the set of primes, and let $B$ be the set of primes s.t. $\mathrm{Gal}_{\mathbb{F}_p}(\bar{f})$ is generated be an element of cycle type $T$.

Thm: The density of $B$ in $A$ is

$$\frac{\{\sigma \in \mathrm{Gal}(f) \mid \sigma \text{ is cycle-type } T\}}{n!} = \begin{array}{l}\text{proportion of elts.} \\ \text{of } \mathrm{Gal}(f) \text{ w/} \\ \text{cycle type } T.\end{array}$$

Pf: Special case of Chebotarev Density Thm.

So, reduce modulo first $b$ primes where $b \geq n!$, and pretty good chance you have determined $\mathrm{Gal}(f)$.

Example: $n = 5$.

Transitive subgps. of $S_5$ (up to isom.):

| # eltr. of each cycle type | 1 | 2 | (2,2) | 3 | (3,2) | 4 | 5 |
|---|---|---|---|---|---|---|---|
| $\mathbb{Z}_5$ | 1 | 0 | 0 | 0 | 0 | 0 | 4 |
| $D_{10}$ | 1 | 0 | 5 | 0 | 0 | 0 | 4 |
| $F_{20}$ "Frobenius gp" | 1 | 0 | 5 | 0 | 0 | 10 | 4 |
| $A_5$ | 1 | 0 | 15 | 20 | 0 | 0 | 24 |
| $S_5$ | 1 | 10 | 15 | 20 | 20 | 30 | 24 |

$f(x) = x^5 + 15x + 12$ $\quad D = 2^{10} 3^4 5^5 \to$ not a square,

so $\mathrm{Gal}(f) \nsubseteq A_5$

$\mathrm{Gal}(f) = F_{20}$ or $S_5$

Reduce modulo small rimesp $p \geq 7$: no 2-cycles or (3,2)-cycles, so $\mathrm{Gal}(f)$ is probably $F_{20}$.

Pf uses a deg 15 resolvent poly.