Lecture #11 (20/11/2025)

Computing the Galois group (of a polynomial)

- Recommended reading (by Keith Conrad)

"Galois groups as permutations groups"

&

"Galois groups of cubics and quartics" (char ≠ 2)

Throughout, let $K = \mathbb{Q}$, $f \in \mathbb{Q}[x]$ irred. of deg n and $G = \mathrm{Gal}(SF_{\mathbb{Q}}(f)/\mathbb{Q})$.

Question: Given f, how to compute G ?

Step 0: We should know how to check if f is indeed irreducible $/\mathbb{Q}$ (e.g. Eisenstein criterion + (possibly) change of variables).

Useful: If $\exists$ p prime s.t. $\deg f \bmod p = \deg f$ and f is irred. $/\mathbb{F}_p$, then f is irred. $/\mathbb{Q}$

Step 1 We view G as a transitive subgroup of S_n. So, for small n we should know the transitive subgroups!

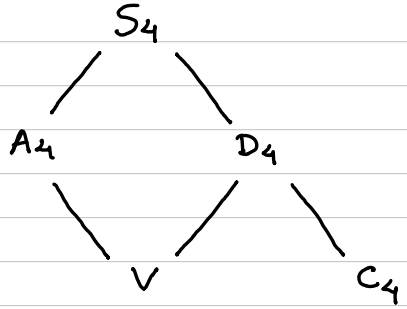
transitive: the action on the roots is transitive

$n=3$ S_3 or A_3

$n=4$ S_4, A_4, D_4, V or C_4

D_4: order 8

The lattice is



$n=5$ S_5, A_5, $\mathrm{Gal}(x^5-\alpha)$, D_5 or C_5

$\alpha \notin \mathbb{Q}^{\times 5}$

D_5: order 10

$\simeq$ affine transformations

$\mathbb{F}_5 \longrightarrow \mathbb{F}_5$, $a \in \mathbb{F}_5^\times$, $b \in \mathbb{F}_5$

$x \longmapsto ax+b$

Step 2 Can we eliminate S_n?

Recall that $G \leq A_n \Leftrightarrow \Delta(f) \in \mathbb{Q}^2$

(the discriminant is a square)

Thus, we should know how to compute $\Delta(f)$. If we know the roots of f great,

for $n \leq 4$ $\exists$ formulas...

otherwise we can use known formulas:

f	$\Delta(f)$
x^2+ax+b	a^2-4b
x^3+ax+b	$-(4a^3+27b^2)$
x^4+ax^2+b	$16b(a^2-4b)^2$
x^4+ax+b	$-27a^4+256b^3$
x^5+ax+b	$2^8a^5+5^5b^4$

* In general,

$$\Delta(x^n+ax+b) = (-1)^{n(n-1)/2}\left((-1)^{n-1}(n-1)^n a^n + n^n b^{n-1}\right)$$

Step 3 if we know that $G \leq A_n$ it is useful to know group properties of A_n and its subgroups.
In particular, it is useful to know which types of permutations we have (cycle type).

We can then try to apply Dedekind's recipe:
(also applies if $G \not\leq A_4$)

Theorem (Dedekind) Let $f(x) \in \mathbb{Z}[x]$ be monic & irreducible / $\mathbb{Q}$ of deg n.
Pick a prime p that does not divide $\Delta(f)$.

Write $f \equiv \prod_{i=1}^{k} g_i \mod p$
with each g_i monic & irred and let $d_i = \deg g_i$. Then G contains a cycle of type $(d_1, \cdots, d_k)$.
(a product of k - disjoint cycles of length d_i)

Note that to apply Dedekind's recipe we need to be able to write the decomposition of f into a product of irreducibles.

So, we need a criterion for deciding irreducibility over $\mathbb{F}_p$:

Rabin's test

Given $f(x) \in \mathbb{F}_p[x]$ of deg n. f is irreducible $(/\mathbb{F}_p) \iff$

- f divides $x^{p^n} - x$ AND
- $\gcd\left(f, x^{p^{n/q}} - x\right) = 1 \quad \forall\, q$ prime divisor of d

Examples

of the form X^4+aX+b
$a=-1, b=-1$

① $f(X) = X^4 - X - 1 \Rightarrow \Delta(f) = -283 = -27-256$

283 is a prime $\Rightarrow$ not a square $\Rightarrow G \not\subseteq A_4$

In fact $f \equiv (X+4)(X^3+3X^2+2X+5) \mod 7$

$\Rightarrow$ G contains a 3-cycle

Now, f has 2 real roots $\Rightarrow$ G contains a transposition

($G \leq S_n$ transitive contains transposition + $(n-1)$-cycle $\Rightarrow G = S_n$)

② $f(X) = X^5 - X - 1$, $\Delta(f) = 19 \times 151$

$/\mathbb{F}_2$ $f \equiv (1+X+X^2)(1+X^2+X^3)$ $(2,3) \rightsquigarrow$ take cube

$\rightarrow$ contains a transposition

$/\mathbb{F}_5$ f is irreducible $\Rightarrow$ G contains a 5-cycle

$\rightsquigarrow G = S_5$

③ $f(X) = X^6 + X^4 + X + 3$, $-\Delta(f) = 5 \times$ huge prime

$p=3$ gives $f \equiv X(X+2)(X^4+X^3+2X^2+2X+2)$

$\rightsquigarrow \exists$ 4-cycle

$p=11$ gives $f \equiv (X+6)(X^5+5X^4+4X^3+9X^2+X+6)$

$\rightsquigarrow \exists$ 5-cycle

(4) $f(x) = x^4 - 8x + 12$ $= 2^{12}\,3^4$

$a = -8,\ b = 12 \Rightarrow \Delta(f) = 576^2 \Rightarrow G \leq A_4$

$\Rightarrow |G| = 4$ or 12 (We have eliminated S_4, D_4 and C_4)

$/\mathbb{F}_5 \quad f \equiv (x+1)(x^3 + 4x^2 + x + 2)$

$\rightsquigarrow$ G contains a 3-cycle $\Rightarrow |G|$ is divisible by 3

$\rightsquigarrow$ $G = A_4$

Some consequences of Dedekind's recipe:

Corollary 1 $f \in \mathbb{Z}[x]$ monic, irred. $/\mathbb{Q}$ of deg p prime. If $\exists$ q prime not dividing $\Delta(f)$ such that $f \bmod q$ has $p-2$ roots in $\mathbb{F}_q$, then $G = S_p$.

example $f(x) = x^3 + 5x + 4$, $\Delta(f) = -4 \times 233$

$\Delta(f)$ not a square $\Rightarrow$ $G = S_3$

Now, $/\mathbb{F}_5$ f has a root ($x = 1$ or -4 if you prefer)
$\rightsquigarrow$ Corollary also says $G = S_3$

Corollary 2 $f \in \mathbb{Z}[x]$ monic, irred. $/\mathbb{Q}$ of deg p odd prime, $\Delta(f)$ a square.
If $\exists$ q prime not dividing $\Delta(f)$ such that f mod q has $p-3$ roots in $\mathbb{F}_q$, then $G = A_p$.

example $f(x) = x^5 + 20x + 16$
$\Delta(f) = 2^{16} \times 5^6$ a square $\Rightarrow$ $G \leq A_5$

Now, $/\mathbb{F}_7$ f has 2 roots ($x = 4, x = 5$)

In general, we will also often use the following.

Proposition For $n \geq 2$ and $G \leq S_n$ transitive, if G contains a transposition and a p-cycle for some $p > n/2$, then $G = S_n$.

Proposition For $n \geq 3$ and $G \leq S_n$ transitive, if G contains a 3-cycle and a p-cycle for some $p > n/2$, then $G = A_n$ or S_n.

example $f(x) = x^7 - 56x + 48$

- $\Delta(f)$ is a square $\Rightarrow$ $\mathrm{Gal}(f) \subset A_7$
- / $\mathbb{F}_5$ f is irred. $\Rightarrow$ $\exists$ 7-cycle
- / $\mathbb{F}_{23}$ $f \equiv$ (quadratic)(quadratic)(cubic)
  $\Rightarrow$ $\exists$ a 3-cycle $(2,2,3) \rightsquigarrow$ take square gives 3-cycle

$\Rightarrow G = A_7$

Cubics and quartics revisited

- For $f \in \mathbb{Q}[x]$ irred. of deg 3, it is enough to check if $\Delta(f)$ is a square or not.
  - square $\rightarrow A_3$
  - not $\rightarrow S_3$
- The generic (irred.) cubic has Galois group S_3.
- If $f \in \mathbb{Q}[x]$ irred. of deg 3 has Galois group A_3, then <u>all</u> its roots are real.
- Here is an example of a family with Galois group A_3:

Take $\alpha \in \mathbb{Z}$ odd and consider $f(x) = x^3 - \alpha x + \alpha$. Then $\Delta(f) = \alpha^2(4\alpha - 27)$.

So, it suffices to show we can choose α s.t. $4\alpha - 27$ is a square:

* $4\alpha - 27 = \beta^2 \Rightarrow \alpha = \frac{\beta^2+27}{4}$

$\Rightarrow$ need $\beta^2 + 3 \equiv 0 \mod 4$

$\Rightarrow$ β has to be odd

* Writing $\beta = 2K+1$ for some $K \in \mathbb{Z}$ yields $\alpha = K^2+K+7$. Thus, for any integer K, the polynomial

$$x^3 - (K^2+K+7)x + (K^2+K+7)$$

has Galois group A_3.

- Another example (Δ is invariant under change of coordinates)

Take $f(x) = x^3 + 2x^2 + 5x + 3$

Then letting $x = y - \frac{2}{3}$ we transform

f into $g(y) = y^3 + \frac{11}{3}y + \frac{7}{27}$

and $\Delta(f) = \Delta(g) = 199 \neq 0 \rightsquigarrow G = S_3$

In general,

$$ax^3 + bx^2 + cx + d$$

$$\downarrow \qquad x = y - b/3a$$

$$y^3 + \alpha y + \beta \text{, where}$$

$$\alpha = \frac{3ac - b^2}{3a^2} \quad \text{and} \quad \beta = \frac{2b^3 - 9abc + 27a^2d}{27a^3}$$

- For quartics the story is more complicated (see Lecture # 10)

Proposition Given $f(x) = x^4 + ax^3 + bx^2 + cx + d$ (irred.), we have that

resolvent

$$r(f) = x^3 + Ax^2 + Bx + C, \text{ where}$$

$$A = -b$$

$$B = ac - 4d$$

$$C = -(a^2d + c^2 - 4bd)$$

In particular, when $a=b=0$ we have that

$$r(f) = X^3 - 4dX - c^2$$

$$\Delta(f) = -27c^4 + 256d^3$$

In general, to determine G we have:

$\Delta(f)$	$r(f)$	G
$\neq \square$	irred.	S_4
$= \square$	irred.	A_4
$\neq \square$	red.	D_4 or C_4
$= \square$	red.	V

Question: D_4 or C_4 ?

(A) If $\mathrm{Gal}(f_4) = C_4$, then $\Delta(f) > 0$.

(B) C_4 does not contain a transposition.

(C) If $\mathrm{Gal}(f_4) = C_4$ or D_4, then

$\mathrm{Gal}(f_4) = D_4 \iff f$ is irred. / $\mathbb{Q}(\sqrt{\Delta})$