

Lecture #11 (04/12/2024)

Computing the Galois group (of a polynomial)

- Recommended reading (by Keith Conrad)

"Galois groups as permutations groups"

&

"Galois groups of cubics and quartics"
(char $\neq 2$)

Throughout, let $K = \mathbb{Q}$, $f \in \mathbb{Q}[X]$ irred. of deg n
and $G = \text{Gal}(S_{F_{\mathbb{Q}}}(f) / \mathbb{Q})$.

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!

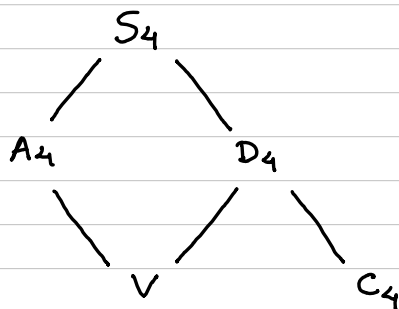
the action on the roots is transitive

$n=3$ S_3 or A_3

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

↑
order 8

The lattice is



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

$\alpha \notin \mathbb{Q}^{x5}$

↑
order 10

$\simeq$ affine transformations

$$\begin{aligned} \mathbb{F}_5 &\longrightarrow \mathbb{F}_5 & a \in \mathbb{F}_5^x, b \in \mathbb{F}_5 \\ x &\longmapsto ax + b \end{aligned}$$

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

* In general,

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

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 $G \not\leq A_n$)

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 $f \equiv \prod_{i=1}^k g_i \pmod{p}$

with each g_i monic & irred and let

$d_i = \deg g_i$. Then G contains a permutation
of cycle type $(d_1, \dots, d_k)$ ← This means that

we have 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 ($\in \mathbb{F}_p$) $\Leftrightarrow$

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

Examples

of the form $x^4 + ax + b$
 $a = -1, b = -1$

$$\textcircled{1} \quad f(x) = x^4 - x - 1 \Rightarrow \Delta(f) = -283 = -27 - 256$$

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

$$\text{In fact } f \equiv (x+4)(x^3 + 3x^2 + 2x + 5) \pmod{7}$$

$\Rightarrow G$ contains a 3-cycle

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

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

$$\textcircled{2} \quad f(x) = x^5 - x - 1, \quad \Delta(f) = 19 \times 151$$

$$\text{over } \mathbb{F}_2 \quad f \equiv (1+x+x^2)(1+x^2+x^3) \Rightarrow \text{type } (2,3)$$

$\leadsto$ cube is transposition

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

$$\leadsto G = S_5$$

$$\textcircled{3} \quad f(x) = x^6 + x^4 + x + 3, \quad -\Delta(f) = 5 \times \text{huge prime}$$

$$p=3 \text{ gives } f \equiv x(x+2)(x^4 + x^3 + 2x^2 + 2x + 2)$$

$\leadsto \exists$ 4-cycle

$$p=11 \text{ gives } f \equiv (x+6)(x^5 + 5x^4 + 4x^3 + 9x^2 + x + 6)$$

$\leadsto \exists$ 5-cycle

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

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

$$\Rightarrow |G| = 4 \text{ or } 12 \quad \left(\text{We have eliminated } S_4, D_4 \text{ and } C_4 \right)$$

$$\text{over } \mathbb{F}_3 \quad f \equiv (x+1)(x^3 + 4x^2 + x + 2)$$

$$\rightarrow G \text{ contains a 3-cycle} \Rightarrow |G| \text{ is divisible by 3}$$

$$\rightarrow G = A_4$$

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)
 $\rightarrow$ Corollary also says $G = S_3$ if you prefer

Corollary 2 $f \in \mathbb{Z}[x]$ monic, irred. / @
of deg p odd prime, $\Delta(f)$ a square.

If $\exists$ q prime not dividing $\Delta(f)$ such that
 $f \bmod q$ 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 $\Rightarrow \text{Gal}(f) \subset A_7$
- $/\mathbb{F}_5$ f is irred. $\Rightarrow \exists$ 7-cycle
- $/\mathbb{F}_{23}$ $f \equiv (\text{quadratic})(\text{quadratic})(\text{cubic})$
 $\Rightarrow \exists (2, 2, 3)$ permutation
its square is a 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.



A_3



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 all its roots are real.
- Here is an example of a family with Galois group A_3 :

Take $\alpha \in \mathbb{Z}$ odd and consider

$$f(x) = x^3 - \alpha x + \alpha. \text{ Then } \Delta(f) = \alpha^2(4\alpha - 27).$$

So, it suffices to show we can choose

α s.t. $4\alpha - 27$ is a square:

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

$$\Rightarrow \text{need } \beta^2 + 3 \equiv 0 \pmod{4}$$

$\Rightarrow \beta$ 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)

$$\text{Take } f(x) = x^3 + 2x^2 + 5x + 3$$

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

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

$$\text{and } \Delta(f) = \Delta(g) = 199 \neq 0 \leadsto G = S_3$$

In general,

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

$$\left\{ \begin{array}{l} x = y - b/3a \end{array} \right.$$

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

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

- 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 $\text{Gal}(f_4) = C_4$, then $\Delta(f) > 0$.
- (B) C_4 does not contain a transposition.
- (C) If $\text{Gal}(f_4) = C_4$ or D_4 , then
 $\text{Gal}(f_4) = D_4 \Leftrightarrow f \text{ is irred. } / \mathbb{Q}(\sqrt{\Delta})$