Lecture 27

- Finite fields calculations
- Solvability by radicals
- Instructor OH: Mon, Tues. next week @ 3:30–4:30 pm.

eg. $f(x) = x^5 + 2x^3 + 3$

$\mathbb{F}_2$ $\quad f(x) = x^5 + 1. = (x+1)\underbrace{(x^4+x^3+x^2+x+1)}_{\Phi_5(x) \quad (\text{over } \mathbb{F}_2)}$

If ζ is a 5^{th} root of unity over $\mathbb{F}_2$, then $\zeta^5 = 1$

$\Rightarrow$ either $\zeta = 1$ or order of ζ is 5.

σ_2 generates $Gal(\Phi_5(x)/\mathbb{F}_2)$.

But $\gcd(2,5) = 1 \Rightarrow \quad \underbrace{\zeta \xmapsto{\sigma_2} \zeta^2 \xmapsto{\sigma_2} \zeta^4 \xmapsto{\sigma_2} \zeta^3 \xmapsto{\sigma_2} \zeta}_{\text{all} \neq 1.}$

Gal group acts transitively on roots of $\Phi_5(x)$

$\Rightarrow \Phi_5(x)$ is irred over $\mathbb{F}_2$!

$\Rightarrow Gal(f(x)/\mathbb{F}_2) \cong C_4$.

Exercise How many roots of $\Phi_n(x)$ are there in $\mathbb{F}_{p^k}$?

Order of ζ divides n and also $p^k - 1$.

$\mathbb{F}_3$ $\quad f(x) = x^5 + 2x^3 = x^3(x^2+2) = x^3(x^2-1) \rightsquigarrow$ splits.

$\Rightarrow Gal(f(x)/\mathbb{F}_3) \cong C_1 \ (= \{1\})$.

($\mathbb{F}_5$) $f(x) = x^5 + 2x^3 + 3$

Find linear factors: note $\alpha^5 \equiv \alpha \bmod 5 \quad \forall \alpha \in \mathbb{F}_5$.

Clearly $f(0) \neq 0$

$f(1) = 6 \neq 0$

$f(2) = 2 + 1 + 3 \neq 0$

$$\left.\begin{array}{l} f(-2) = -2 - 1 + 3 = 0 \\ f(-1) = 0 \end{array}\right\} \begin{array}{l}(x+1)(x+2) \\ = x^2+3x+2 \text{ is a factor.}\end{array}$$

Divide:

$$\begin{array}{rl}
 & x^3 + 2x^2 - x - 1 = h(x) \\
x^2+3x+2 \,\big) & x^5 + 0x^4 + 2x^3 + 0x^2 + 0x + 3 \\
 & -(x^5 + 3x^4 + 2x^3) \\
 & -3x^4 + 0x^3 \\
 & -(2x^4 + x^3 + 4x^2) \\
 & -x^3 + x^2 \\
 & -(-x^3 - 3x^2 - 2x) \\
 & 4x^2 + 2x + 3 \\
 & = -x^2 - 3x - 2 \\
 & = -(x^2 + 3x + 2)
\end{array}$$

Finally, $h(x)$ is reducible iff it has a linear factor

Check that it doesn't.

One way: $D_x f(x) = 5x^4 + x^2 = x^2$ only has 0 as roots

$\Rightarrow$ $f(x)$ is separable. Any roots $h(x)$ has are different from $-1, -2$, and we know $h(x) \mid f(x)$. $h(x)$ is irred.

$\Rightarrow \mathrm{Gal}(f(x)/\mathbb{F}_5) \cong C_3$.

Solvability by radicals

Algebraic operations: $+, -, \times, \div, \sqrt[n]{\ }$

eg. Quadratic formula gives roots of $f(x) = x^2 + bx + c$ in terms of these operations.

There exist formulas for cubics & quartics (ugly ones).

Discussion today:

thm There does not exist a "quintic formula"

↳ relates to solvability of groups.

Recall A finite group G is solvable if there is a chain of subgroups

$$1 = G_s \leq G_{s-1} \leq G_{s-2} \leq \cdots \leq G_1 \leq G_0 = G$$

where each G_i / G_{i+1} is cyclic.

Fact If $N \trianglelefteq G$, G/N both solvable, then G is also.

Defns / Notation

- For $a \in F$, let $\sqrt[n]{a}$ denote any root of $x^n - a \in F[x]$ in a splitting field.
- $F(\sqrt[n]{a})$ is a "simple radical extension"
- A Galois extension K/F is cyclic if $\mathrm{Gal}(K/F)$ is cyclic.
- As we have seen, over $\mathbb{F}_p$, roots of $x^n - 1$ are still called n^{th} roots of unity (except when $p \mid n$ then the only roots are 1)

<u>Main idea</u> $+, -, \times, \div$ are just operations on a field. The nestedness of your radicals tells you how many simple radical extensions you need to do before you capture all the roots of $f(x)$.

eg. $$-1+\sqrt{17}+\sqrt{2(17-\sqrt{17})}+2\sqrt{17+3\sqrt{17}-\sqrt{2(17-\sqrt{17})}-2\sqrt{2(17-\sqrt{17})}}$$

needs at most 4 extensions
(see ruler + compass construction of 17-gon)

<u>dfn.</u> An algebraic element α over F can be <u>expressed by radicals</u> / <u>solved for in terms of radicals</u> if $\alpha \in K$ where

$$F = K_0 \subset K_1 \subset \cdots \subset K_s = K$$ $\leftarrow K$ is a "root extension" of F

where, for all $0 \le i \le s-1$,

$$K_{i+1} = K_i(\sqrt[n_i]{a_i}) \text{ for some } a_i \in K_i.$$

Simple radical extensions

prop. Let F be a field where $\operatorname{char} F \nmid n$. (eg char 0)
If F contains the n^{th} roots of unity (ie ζ_n) then
$F(\sqrt[n]{a})/F$ is cyclic, of degree dividing n.

Pf. Sketch Let $K = F(\sqrt[n]{a})$.

- $\mu_n = \underline{\text{cyclic}}$ group of n^{th} roots of unity

  char 0 ✓ char p? Still cyclic. Take splitting field of $x^n - 1$. Gal gp is cyclic!

- If $\sigma \in \operatorname{Gal}(K/F)$, then $\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}$ for some $\zeta_\sigma \in \mu_n$.
- Check that
$$\begin{aligned} \operatorname{Gal}(K/F) &\longrightarrow \mu_n \\ \sigma &\longmapsto \zeta_\sigma \end{aligned}$$
is a group hom.

  Kernel $= \{\sigma \mid \zeta_\sigma \sqrt[n]{a} = \sqrt[n]{a}\} = \{1\}$.

  $\Rightarrow \operatorname{Gal}(K/F) \hookrightarrow \mu_n$. //

Actually:

prop. Let F be a field with characteristic not dividing n, and F contains the n^{th} roots of unity.
Then
$$K/F \text{ cyclic} \iff K \cong F(\sqrt[n]{a}) \quad \text{for some } a \in F.$$

(Pf. omitted)

Recall: $F = K_0 \subset K_1 \subset \dots \subset K_s = K$ $\leftarrow$ K is a "root extension" of F

$$K_{i+1} = K_i(\sqrt[n_i]{a_i}) \text{ for some } a_i \in K_i.$$

Lemma. If $\alpha \in K$ a root extension of F, then α is is contained in a Galois root extension of F, and each extension is cyclic.

Pf. Sketch.

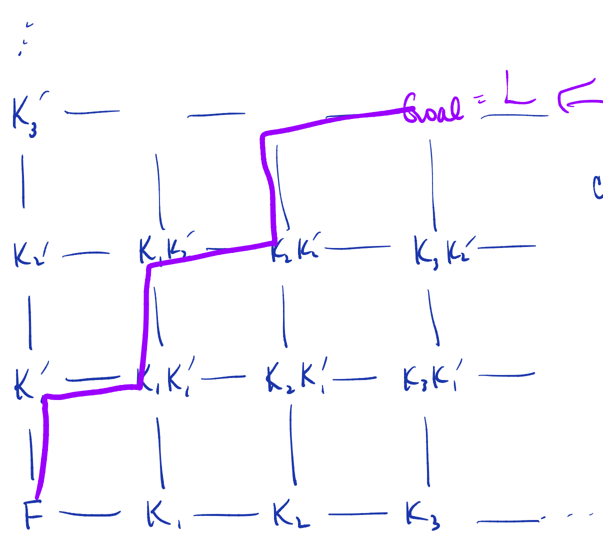
- Let L be the Galois closure of K/F ie

$$\begin{array}{c} L \\ | \\ K \\ | \\ F \end{array}$$

smallest $L \supset K$ s.t. this is Galois.

- Then observe that if $\sigma \in \mathrm{Aut}(L/F)$, we get another chain $F = \sigma K_0 \subset \sigma K_1 \subset \dots \subset \sigma K_s = \sigma K$ where $\sigma K_{i+1}/\sigma K_i$ is still a simple radical ext. gen'd by $\sigma(\sqrt[n_i]{a_i})$.

- Cobble them together Rough idea



composite of root extensions is still a root extension.

(take any path)

each segment is a simple radical ext.

$\rightsquigarrow$ L is a Galois root extension of F.

So WLOG we may assume K/F is Galois now.

Let F' be the extension of F containing all the n_i^{th} roots of unity.

$$F = K_0 \subset K_1 \subset \cdots \subset K_s = K$$

$$\Downarrow$$

$$F \overset{\text{cyclic!}}{\subset} F'F = F'K_0 \subset F'K_1 \subset \cdots \subset F'K_s = F'K$$

$$\begin{tikzcd} & F'K \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "\text{Gal.}"] & \\ F' \arrow[dr, dash, "\text{Gal}"'] & & K \arrow[dl, dash, "\text{Gal}"] \\ & F & \end{tikzcd}$$

<u>Fact</u>. Composite of 2 Galois extensions is still Galois.

(Use Fund Thm, eg. & normal subgroups)

Each extension here is still a simple rad. ext $\Longrightarrow$ cyclic. $\boxtimes$

Lemma. If $\alpha \in K$ a root extension of F, then α is is contained in a Galois root extension of F, and each extension is cyclic.

thm A polyn $f(x) \in F[x]$ is solvable by radicals iff its Galois group is solvable.

eg. $-1+\sqrt{17}+\sqrt{2(17-\sqrt{17})}+2\sqrt{17+3\sqrt{17}-\sqrt{2(17-\sqrt{17})}-2\sqrt{2(17-\sqrt{17})}}$

(Pf. is just rehash of all we've already discussed.)

---

thm There does not exist a "quintic formula"

↳ ie $\exists$ quintic that is not solvable by radicals.

eg/pf./Fact

The general quintic $f(x) = x^5 - a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ over $F(a_0, \ldots, a_4)$ is separable, with Galois group S_5.

But S_5 is not solvable. (A_5 is not solvable)

Quintics

<u>Fact</u> $\mathrm{Gal}(f(x)/\mathbb{Q})$ transitive whenever $f(x)$ irreducible.

There are 5 transitive subgroups of S_5

$$\begin{tikzcd}[column sep=small]
 & S_5 \;\; 120 \arrow[dl, dash] \arrow[dr, dash] & \\
60 \;\; A_5 \arrow[d, dash] & & F_{20} = C_5 \rtimes C_4 \;\; 20 \arrow[dll, dash] \arrow[ddl, dash] \\
10 \;\; D_5 \arrow[dr, dash] & & \\
 & C_5 \;\; 5 &
\end{tikzcd}$$

solvable.