Next week: Monday finish film on solvable polynomials, continue to transcendental extensions.

Practice: \( \frac{d}{dx}(x^n-1) = nx^{n-1} \) only divisible by \( x \), so relatively prime to \( x^n - 1 \). By derivative criterion for separability \( x^n-1 \) has \( n \) distinct roots when \( n \to \infty \), e.g. over \( \mathbb{Q} \).

If \( \alpha, \beta \) roots of \( x^n - 1 \) is some field then

\[(\alpha \beta)^n = \alpha^n \beta^n = 1, (x^{-1})^n = (x^n)^{-1} = 1 \quad \text{so} \quad \alpha \beta, \frac{1}{\alpha} \text{ are also roots.} \]

- \( \mu_n \) is a cyclic group of order \( n \).

What is the point? We know \( \mu_n = \{ e^{2\pi i k/n} \mid k \text{ mod } n \} \).

Well, if we embed everything in \( \mathbb{C} \), can take this pov. But we also want to be able to take an abstract pov.
Dividing \( \mu_n \) by orders of the elements (has \( \#(\mathbb{Z}/d\mathbb{Z}) \) elements of order \( d \) for each \( d|n \))

Have \( \prod (x - s) = \prod \prod (x - s)^{\text{ord}_d(x)} \)
\[ \text{seq}_{n \text{ prime}} \text{ord}_d(x) \text{ \text{div}\, n} \text{seq}_{d \text{ divides } n} \text{ \text{div}\, n} \]

(1) Note: If \( s_n \) is a root of \( \Phi_n \)

Then \( s_n^n = 1 \) (\( \Phi_n | x^n - 1 \)).

But \( s_n^n \neq 1 \) if \( d < n \) (\( \Phi_n \) is prime to \( \Phi_d \) and \( x^n - 1 \) has \( n \) distinct roots)

So \( s_n \) is an element of order \( n \) in \( \mathbb{Z}^* \), so \( \mu_n \subset \mathbb{Z}^* \).

In particular \( \text{Gal}(\Omega s_n) = \text{Gal}(\mu_n) \) is the splitting field of \( \Phi_n \) and \( x^n - 1 \) over \( \Omega \).

Now if \( \sigma \in \text{Gal}(\Omega s_n), \Omega \) then \( \sigma(s_n) \) is a root of \( x^n - 1 \) but not of \( x^d - 1 \) if \( d \neq n \) (because \( s_n \) is a root of the first but not of the second)
so \( \sigma(\in) \) is another primitive root of unity of order \( n \) (being a primitive root of unity is an algebraic fact \( \tau \), so preserved by field acts.)

\[ \sigma(\in) = \tau^{j(\in)} \text{ for some } j \in (\mathbb{Z}/n\mathbb{Z})^* \]

Now if \( \sigma \in \text{Gal}(\mathbb{Q}(\in) : \mathbb{Q}) \)

then \[ (\sigma \tau)(\in) = \sigma(\tau(\in)) = \sigma(\tau^{j(\in)}) = \sigma(\tau^{j(\in)}) \]

\[ = (\tau^{j(\in)})^{j(\in)} = \tau^{j(\in)j(\in)} = \tau \]

\( \Rightarrow j : \mathbb{C} \to (\mathbb{Z}/n\mathbb{Z})^* \) is a \( \mathbb{C} \) hom.

It's injective since if \( j(\omega) = 1 \) then \( \sigma(\in) = \in \)

so the fixed field of \( \sigma \) is \( \mathbb{Q}(\in) \).

Let's look at \( \Phi_n(x) \), it has degree \( \phi(n) \)

since \( \#P_n = \phi(n) \) (see above)

For \( \sigma \in \text{Gal}(\mathbb{Q}(\in) : \mathbb{Q}) \), \( \sigma \) must map \( P_n \) to itself since

Thus \( \sigma(\prod_{\in P_n} (x - \in)) = \prod_{\in P_n} (x - \sigma(\in)) = \prod_{\in P_n} (x - \in') = \Phi_n \)
(Aside: Action of $\text{Aut}( \mathbb{F}_p )$ extends to $L[\times I]$. $x$ is fixed. This action is by ring automorphisms.)

So $(\mathbb{F}_p)^n = \mathbb{F}_p$ means coefficients of $G$ are in the fixed field of $G$.

(By the Gauss Lemma, since $x^n - 1$, $\mathbb{F}_p$ are monic, $x^n - 1 \in \mathbb{Z}[x] \Rightarrow \Phi_n \in \mathbb{Z}[x]$.)

Fact: $G = (\mathbb{F}_p \times \mathbb{Z})^\times$, $G$ acts transitively on $\Phi_n$, so $\Phi_n$ is irreducible.

$\Phi_{p^r} = \left\{ \Phi_{p^r} \mid \Phi_{p^r} \neq 1 \right\} = p^{pr} - p^{pr-1}$

So $\Phi_{p^r} = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = \frac{\Phi^{p^{r-1}}}{x^{p^{r-1}} - 1} = \Phi_p(x^{p^{r-1}})$

This is irreducible: $\mathbb{Z}[x]$.

mod $p$ we have

\[ \Phi_{p^r} = \frac{x^{p^r} - 1^{p^r}}{x^{p^{r-1}} - 1^{p^{r-1}}} = \frac{(x - 1)^{p^r}}{(x - 1)^{p^{r-1}}} \equiv (x - 1)^{p^{r-1}}(p^r) \]

so if $\Phi_{p^r}$ could be factored in $\mathbb{Z}[x]$,
Say $\phi_{pr} = f \cdot g$, then mod $p$ we'd have
\[ \tilde{f} = (x-1)^a, \quad \tilde{g} = (x-1)^b, \quad a+b = pr \cdot (p-1) \]
But then $a, b > 0$ (as monic)
Here $\tilde{f}(1) = 0, \tilde{g}(1) = 0$
\[ \Rightarrow p \mid f(1), p \mid g(1), \quad p^2 \mid f(1)g(1) = \Phi_{pr}(1) \]
But $\Phi_{pr}(1) = \Phi_{p}(f^{p-1}) = \Phi_{p}(1) = p \Rightarrow \exists \epsilon$. \\
\[ \Rightarrow [\mathbb{Q}(\sqrt[p^r]{\epsilon}) : \mathbb{Q}] = \deg \Phi_{pr} = \Phi(p^r) \]
so injective map $\text{Gal}(\mathbb{Q}(\sqrt[p^r]{\epsilon}) : \mathbb{Q}) \to (\mathbb{Z}/p^r\mathbb{Z})^*$
is surjective \\
(\# \text{Gal}(\mathbb{Q}(\sqrt[p^r]{\epsilon}) : \mathbb{Q}) = [\mathbb{Q}(\epsilon) : \mathbb{Q}] = p^r - 1)

(number theory: $(\mathbb{Z}/p^r\mathbb{Z})^*$ is cyclic if $p$ is odd) \\
(proof by induction: suppose $a$ has order $\Phi(p)$ mod $p^r$, can $a^{\Phi(p)} \equiv 1 \pmod{p^{r+1}}$?)
maybe, but examine $(a + p^{r+1})^k \pmod{p^{r+1}}$
Galois theory: fields $0 < K < \mathbb{Q}(\sqrt[p]{5})$ s.t. 
$[K: \mathbb{Q}] = 2$ are in bijection with subgroups $H \leq \text{Gal}(\mathbb{Q}(\sqrt[p]{5}); \mathbb{Q})$ s.t. $[G:H] = 2$

But $G$ is cyclic, so has a unique subgroup of each order dividing $p-1$.

Then $G/H \cong C_2 = \{ \pm 1 \}$

Conversely, if $\chi : G \to C_2$ is a non-trivial homomorphism then $\ker(\chi)$ has index 2, so $\ker(\chi) = H$ and $\chi$ is the quotient map $G \to G/H$.

(Or $G$ is cyclic, let $a \in G$ be a generator.
Then $\chi$ is determined by $\chi(a)$, if $\chi(a) = 1$ then $\chi = 1$ so $\chi(a) = -1$ have at most one hom. The Legendre symbol \( \left( \frac{a}{p} \right) = a^{p-1} \mod p \) is such a map.)

Let $g = \sum_{\sigma \in S} \sigma(5)$

Let $\tau \in G$. Then $\tau(5) = \sum_{\sigma \in S} \tau(\sigma(5)) \tau(\sigma(5)) \tau(\sigma(5))$
\[
\sum_{\sigma \in \mathcal{G}} x(\sigma)(\tau_0)(\cdot) = x(\cdot) \sum_{\sigma \in \mathcal{G}} x(\sigma)
\]

\[
\tau_{\pm 1} = \pm 1
\]

\[
\tau(\pm 1) = \pm 1
\]

\[
\tau(\cdot) = \sum_{\sigma \in \mathcal{G}} x(\sigma) = \tau(\cdot) = \tau(\cdot) = \tau(\cdot)
\]

(taking a "trace" twisted by \(x\) we get an element transforming like \(x^-\))

(element \(g\) is a joint eigenvector for \(G\) acting on \(\mathcal{D}(\mathfrak{g})\), eigenvalue of \(\sigma\) is \(x(\sigma^-)\))

(more on this in \(\text{SU}(2)\) "representation theory")

\[\text{Core: if } \tau \in \mathcal{H} = \text{Ker}(x) \text{ then } \tau(\sigma) = g \]

so \(g \in \text{Fix}(\mathbb{H}) = K\)

Also, if \(g \not\in \mathcal{H}\) then if \(T \not\in \mathfrak{H}\), \(x(T) = 1\),

\[\tau(\sigma) = -g + g, \text{ so } g \not\in \mathcal{D}\]

(warning: if we replace \(\tau\) with \(\tau\), we get \(\sum_{\sigma \in \mathcal{G}} x(\sigma) - \sigma(1) - \sum_{\sigma \in \mathcal{G}} x(\sigma) = \tau(1) - 1\)

and this is zero (change vars to \(\sigma \rightarrow \sigma^{-1}\) )
Set \( \sum \chi(\sigma) = (\sum \chi(\sigma)) \cdot \chi(\tilde{r}) \) if \( \chi(\tilde{r}) = -1 \), this forces \( \sum \chi(\sigma) = 0 \).

Check: \( q^2 = p \cdot (-1)^x \neq 0 \)

(to check if \( p \) is a square mod \( q \) need to evaluate \( p^{\frac{q-1}{2}} \) mod \( q \). Instead look at \( q^{q-1} \). Use \( q^2 = \sum (\cdot)^q \) mod \( q \)

Interestingly fields:

\( \mathbb{Q}(\sqrt[3]{p}, \sqrt[3]{p^2}, \sqrt[3]{p^3}, \ldots) \)

Also \( \mathbb{Q}(\sqrt[3]{n}, \sqrt[3]{n^2}) \) which is the maximal abelian extension of \( \mathbb{Q} \)

Embedding \( \mathbb{K}(\sqrt[3]{a}) \rightarrow \mathbb{M}_2(\mathbb{K}) \)

\( a + b \varpi \rightarrow (a b a) \).
(other kind of abelian subalgebra $(a, b)$)

More generally, embed $K(a)$ in $M_\alpha(K)$

$\alpha \mapsto \begin{pmatrix} 1 & \cdots & \alpha & \cdots & 1 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & -\alpha \end{pmatrix}$ — coefficients of min poly.

called "companion matrix":

$\begin{pmatrix} 0 & \cdots & -\alpha_1 \\ 1 & \cdots & -\alpha_2 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & -\alpha_{d-1} \end{pmatrix}$

$\text{char poly of a companion matrix is}$

$x^d - \sum_{i=0}^{d-1} \alpha_i x^i.$

---

Let $L/K$ be finite extension, let $x \in L$

let $\sigma \in \text{End}_K(L)$ be the map $\sigma(x) = x$.

Set $\text{Tr}_{L/K} x = \text{Tr}_K(\sigma)$ $\in K$

$\text{N}_{L/K} x = \det_K(\sigma) \in K$

claims if $L$ is separable,
\[ \text{Tr}_K \alpha = \sum_{\mu \in \text{Hom}_K(L/N)} \mu \alpha \quad \text{N some (any) normal extension} \]

\[ N_K \alpha = \mathbf{E}(\alpha) \]

In particular if \( L/K \) Galois, \( \text{Hom}_K(L/K) = \text{Gal}(L/K) \)

(\text{to see that these combos are in } K, \text{ act by } \text{Gal}(N/K) \text{ which permutes } \text{Hom}_K(L/K) \)

If \( \mu : L \to N \), \( \circ : N \to N \) then \( \circ \mu \) is another map \( L \to N \).

So \( \circ (\text{Tr}) = \circ \left( \sum_{\mu \in \text{Hom}_K(L/K)} \mu \alpha \right) = \sum_{\mu \in \text{Hom}_K(L/K)} \circ \mu (\alpha) \)

\[ = \sum_{\mu \in \text{Hom}_K(L/K)} (\circ \circ \mu) (\alpha) = \sum_{\mu \in \text{Hom}_K(L/K)} \mu (\alpha) = \text{Tr} \alpha \]

Start with \( L = K(\alpha) \)

\[ \text{Tr}(m_{\alpha}) = ? \quad N = ? \]

1. Matrix of \( m_{\alpha} \) = companion matrix, take trace, det.
Let $f$ be the min poly of $\alpha$. Then $f(\alpha) = 0$, so $f(m_\alpha) = 0$

$$f(m_\alpha) = m_{f(\alpha)} = \prod (m_\alpha) = m_\alpha;$$

Cayley–Hamilton: char poly of $m_\alpha$ kills $m_\alpha$

so it's a multiple of $f$.

But they both have degree $[k(\alpha) : k] = 1$ so $f = \text{char poly}$.

So $\text{Tr}_{k(\alpha)}^{k} \alpha = -a_{d-1}$ is sum of roots

$$= \sum_{\mu \in k(\alpha) - k} \mu(\alpha)$$
We know $O(\sqrt{3}) = O(\sqrt{3})$

H: $[O(\sqrt{3}) : \mathbb{Q}] = 4$, contains $O(\sqrt{5})$

Ask: does $O(\sqrt{3})$ contain a cubic subfield?

We need $\mathbb{V}$ to be of order 3, so need

$3(p-1) \neq p^2 - 1$ if $p \equiv 1 (p)$ have a cubic subfield

$p \equiv 2 (p)$ cannot.

Let $x : \mathbb{G} \to \mathbb{G} = \mathbb{Z}_1 / \mathbb{Q}$, $w^3 = \mathbb{O}(\sqrt{3})$

Look at $g \geq \mathbb{O}(\sqrt{3}) \cap (x - 1)(x) = g \cdot x^{-1}(x)

$g^2 \in \mathbb{Q}$, so to go $O(\sqrt{3})$ is the cubic field.

(l prime, $p \equiv 1 (p)$, look at subfield of

$O(p)$ of degree $l$ over $\mathbb{Q}$

$k = O(g)$ where $g^k \in \mathbb{Q}$.)
If $x: G \to C^k$

Make $y(x) = \sum_{\sigma \in G} x(\sigma) \sigma(\tilde{s})$ a-priori in field contains

if $x=1$, set trace. Typically, values of $x$