63.1

Finite fields.

$\mathbb{F}_{p^n}$ = splitting field of $x^{p^n} - x$.

Unique up to isomorphism.

It is Galois / $\mathbb{F}_p$, with cyclic Galois group gen by

$$\sigma_p : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$$
$$x \longrightarrow x^p$$

By Galois theory,

$$\left\{ \begin{matrix} \text{subfields of} \\ \mathbb{F}_{p^n} \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{subgroups} \\ \text{of } \mathbb{Z}/n \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{Divisors} \\ d \mid n \end{matrix} \right\}.$$

$$\operatorname{Fix}(x \to x^{p^d}) \qquad\qquad d\mathbb{Z}/n\mathbb{Z} \longleftarrow d$$

$= \mathbb{F}_{p^d}$.

Notice that the restriction of $\sigma_p \in \operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ to $\operatorname{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \cong \dfrac{\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)}{\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})}$

is the same map.

Proposition. The multiplicative group of a finite field is cyclic.

Proof. Let $G = \mathbb{F}_{p^n}^\times$ with order $p^n - 1$.

Let m = LCM of orders of cyclic factors. Then $m \mid p^n - 1$.

(Recall: we have $G \cong (\mathbb{Z}/l_1) \times \cdots (\mathbb{Z}/l_m)$ for various l_i. maybe distinct or not.)

All $x \in \mathbb{F}_{p^n}^\times$ satisfy $x^m = 1$.

But $x^m - 1$ has at most m distinct roots!

So $m \geq p^n - 1$ and we get equality.

Cor. There is an irred poly of deg $n / \mathbb{F}_p$ for every $n \geq 1$.

Pf. $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$ for any generator θ.
So the min poly of any of them has degree n.
It will divide $x^{p^n} - x$.

Prop. $x^{p^n} - x$ is the product of all distinct irreducible monic polynomials in $\mathbb{F}_p[x]$ of degree dividing n.

Pf. This product divides $x^{p^n} - x$ by what we said above.
Conversely, if θ is a root of $x^{p^n} - x$, then $[\mathbb{F}_p(\theta) : \mathbb{F}_p] = d$ for some $d \mid n$, and it is a root of its minimal polynomial (which is irreducible).

Example. Find all irreducible cubics in $\mathbb{F}_2[x]$.
They are roots of $x^8 - x = x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$

$$= x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1).$$
(fool around)

Notice that a priori that thing has to factor.

Counting irreducible polynomials.

Definition. The Möbius function $\mu(n) : \mathbb{Z}^+ \to \{1, 0, -1\}$ is:

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is divisible by any square} > 1 \\ (-1)^r & \text{if } n \text{ has } r \text{ distinct prime factors.} \end{cases}$$

(So $\mu(1) = 1$.)

It is multiplicative: $\mu(m_1 m_2) = \mu(m_1)\mu(m_2)$ for $(m_1, m_2) = 1$.

(If we dropped the (m_1, m_2) condition, would be completely multiplicative. Not true of the Möbius function.)

63.3.

Möbius Inversion Formula.

Suppose $F(n) = \sum_{d|n} f(d)$,

then $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$.

Proof. Exercise!

Mobius Inversion, Highbrow version.

Define the arithmetic convolution of two arithmetic functions $f, g : \mathbb{Z}^+ \to \mathbb{C}$

$$f * g(n) = \sum_{d|n} f(d) g(\tfrac{n}{d}).$$

Then:

(1) Arithmetic functions form a ring (so $(f*g)*h = f*(g*h)$)

with identity $\delta(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{o/w}. \end{cases}$

(2) The inverse of the function $\mathbb{1}$ (i.e. $\mathbb{1}(n) = 1$ for all n) is μ.

Let's apply this!

Define: $\psi_p(d) = \#$ irred monic polys of degree d in $\mathbb{F}_p[x]$

Then we have (from our proposition)

$$p^n = \sum_{d|n} d\, \psi_p(d).$$

By MI, get $n\psi_p(n) = \sum_{d|n} \mu(d) p^{n/d}$

and so $\psi_p(n) = \frac{1}{n}\sum_{d|n} \mu(d) p^{n/d}$.

63.4.

Example. # irred monic polys of degree 10 over $\mathbb{F}_p$ is

$$\frac{1}{10}\left(p^{10}-p^{5}-p^{2}+p\right) \approx \frac{p^{10}}{10}.$$

Compare with the prime number theorem,

$$\#\{\text{primes} \le x\} \sim \frac{x}{\log x}.$$

Here (in a PID prime $\longleftrightarrow$ irreducible!) in $\mathbb{F}_p[x]$,

$$\#\{\text{primes of "size } p^n\text{"}\} \sim \frac{p^n}{\log_p(p^n)}$$

where the size of an irreducible polynomial f, the norm, is $N(f) = |\mathbb{F}_p[x]/(f)|$
$= p^{\deg(f)}$.

There is also a zeta function

$$\zeta_{\mathbb{F}_p[x]}(s) = \sum_{\substack{f\in\mathbb{F}_p[x]\\ \text{monic}}} p^{-(\deg f)\cdot s} = \sum_{n=0}^{\infty} p^{n-ns}$$

$$= \frac{1}{1-p^{1-s}}.$$

$$= \prod_{\substack{f\in\mathbb{F}_p[x]\\ \text{irreducible}}} \left(1+p^{-(\deg f)\cdot s}+p^{-2(\deg f)\cdot s}+\cdots\right)$$

Exercise. Prove the Riemann hypothesis.

$$= \prod_{f \text{ irred.}} \frac{1}{1-p^{-(\deg f)\cdot s}}.$$

You can keep pushing this analogy!

63.5 = 64.1

The algebraic closure.

If α is algebraic $/ \mathbb{F}_p$, then $\alpha \in \mathbb{F}_{p^n}$ for some n.

So $\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$.

This is not a disjoint union, but rather subject to inclusion maps $\mathbb{F}_{p^d} \hookrightarrow \mathbb{F}_{p^n}$ whenever $p | n$,

where we identify $\mathbb{F}_{p^d}$ with its image.

[Here we had a long impromptu discussion about the p-adics]

Composite extensions.

Proposition. Let K/F Galois, F'/F arbitrary.

Then KF' is Galois over F', with

$$\mathrm{Gal}(KF'/F') \cong \mathrm{Gal}(K/K \cap F').$$

$$\begin{tikzcd}
& KF' \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & F' \arrow[dl, dash] \\
& K \cap F' \arrow[d, dash] & \\
& F &
\end{tikzcd}$$

Pf.

Think of the Galois ness as obvious! (It's probably not yet.)

K is the splitting field of some f over F.

KF' is generated by the roots of f over F'.

(Maybe they're in F' now, maybe not.)

So It's the splitting field for f/F', hence Galois.

63.6 = 64.2.

Now, we have a homomorphism

$$\varphi : \mathrm{Gal}(KF'/F') \longrightarrow \mathrm{Gal}(K/F).$$
$$\sigma \longrightarrow \sigma|_K$$

Why is this? If $\sigma \in \mathrm{Gal}(KF'/F')$,
then σ must map K to K (i.e. $\sigma(K) = K$).
K/F is Galois, so every embedding of K fixing F
is an automorphism of K.
(And σ fixes F', hence a fortiori F).

What is the kernel? Anything acting trivially on K,
It must act trivially on F' also.
So it acts trivially on the compositum, hence is 1.

A related prop.

Proposition. Let K_1/F, K_2/F be Galois.
Then
(1) $K_1 \cap K_2$ is Galois $/F$
(2) K_1K_2 is Galois $/F$, and
$$\mathrm{Gal}(K_1K_2/F) \cong \{(\sigma, \tau) : \sigma|_{K_1\cap K_2} = \tau|_{K_1 \cap K_2}\}$$
$$\subseteq \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

Proof. (1) Given irred $p(x) \in F[x]$ w/ root in $K_1 \cap K_2$.
Since K_1 is Galois, all roots in K_1.
Same story for K_2. So p splits in $K_1 \cap K_2$.
So $K_1 \cap K_2$ Galois $/F$.

64.3.

Let K_1, K_2 be splitting fields for f_1, f_2 $/F$.
Then $K_1 K_2$ is the splitting field for $f_1 \cdot f_2$!

We have a homomorphism

$$\mathrm{Gal}(K_1 K_2 / F) \longrightarrow \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$$

$$\sigma \longrightarrow (\sigma|_{K_1}, \sigma|_{K_2}).$$

(Stare at this and convince yourself it's obvious.)

It is injective, because if $\sigma|_{K_1} = 1$, $\sigma|_{K_2} = 1$, then σ trivial on the whole thing

Image lies inside the subgroup H described earlier.

What is its order?

If $\sigma \in \mathrm{Gal}(K_1/F)$, how many $\tau \in \mathrm{Gal}(K_2/F)$ restrict to the same thing on $K_1 \cap K_2$?
$|\mathrm{Gal}(K_2 / K_1 \cap K_2)|$.

So: $|H| = |\mathrm{Gal}(K_1/F)| \cdot |\mathrm{Gal}(K_2/K_1 \cap K_2)|$

$\cancel{= |\mathrm{Gal}(K_1/F)|} \cdot \cancel{\dfrac{|\mathrm{Gal}(K_2/F)|}{|\mathrm{Gal}(K_1 \cap K_2/F)|}}$ iso. by previous!

$= |\mathrm{Gal}(K_1/F)| \cdot |\mathrm{Gal}(K_1 K_2 / K_1)|$

$= |\mathrm{Gal}(K_1 K_2 / F)|$.

So, to recap,

the image of $\mathrm{Gal}(K_1 K_2/F)$ under an injection is contained within a subgroup of the same size

$\longrightarrow$ must have equality.

Cor. (1) If K_1, K_2 Galois $/F$ with $K_1 \cap K_2 = F$, then $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$.
[immediate]

(2) If K is Galois over F, $\mathrm{Gal}(K/F) \cong G_1 \times G_2$ for some G_1, G_2, then $K = K_1K_2$ for fields K_1, K_2 which are Galois with $K_1 \cap K_2 / F$.

Use FT Galois theory!

$$\begin{tikzcd}[column sep=small]
 & 1 \arrow[dl, dash] \arrow[dr, dash] & & & & & K \arrow[dl, dash] \arrow[dr, dash] & \\
G_1 \arrow[dr, dash] & & G_2 \arrow[dl, dash] & \arrow[r, leftrightarrow] & {} & K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\
 & G & & & & & F &
\end{tikzcd}$$

Take $K_i = \mathrm{Fix}(G_i)$.

The G_i are normal in the direct product, hence K_i Galois $/F$.

Get an isomorphism of lattices, so that $K_1K_2 = K$, $K_1 \cap K_2 = F$ by group theory.

Galois closures:

Prop. If E/F finite separable, then E is contained in an extension K, Galois $/F$, and is minimal: In a fixed ~~Galois~~ alg closure, any other Galois ext. of F containing E contains K.
It is called the Galois closure of E over F.

Proof. Take, e.g., compositum of splitting fields for a basis of E/F.

64.5 = 65.1

The primitive element theorem:

If K/F is finite and separable, then $K = F(\theta)$ for some $\theta \in K$.

[Recall: in char 0, any finite extension is separable.]

Sometimes K/F is called a simple extension.

Prop. Let K/F be finite; then

$K = F(\theta)$ for some θ $\longleftrightarrow$ $\left\{\begin{array}{l}\text{there are only finitely} \\ \text{many subfields of } K \text{ containing } F\end{array}\right\}$

Proof of PET (using proposition).

Let K^c be the Galois closure of K/F. Also finite and separable.

Then $\left\{\begin{array}{c}\text{subfields of } K \\ \text{containing } F\end{array}\right\} \subseteq \left\{\begin{array}{c}\text{subfields of } K^c \\ \text{containing } F\end{array}\right\}$

$\updownarrow$

$\{\text{subgroups of } \mathrm{Gal}(K^c/F)\}$ which is finite!

64.6 = 65.2

Proof.

(1) If $K = F(\theta)$, and $F \le E \le K$, let:

$f \in F[x]$ min poly for θ / F.

$g \in E[x]$ min poly for θ / E.

Then $g | f$ in $E[x]$.

What field do the coeffs of g generate $/F$?

Clearly contained in E.

But the minimal poly for θ is the ~~same~~ still g over this field

So: $[K : E] = [K : \text{this field}]$. So it's E.

Now: factor f in $K[x]$. g must be a product of some of the factors. Finitely many choices $\Rightarrow$ these determine the E.

(2) Conversely, assume finitely many $F \le E \le K$.

Can assume F is infinite (finite field extensions always have a primitive element) —

Enough to show: $F(\alpha, \beta)$ can be generated by one element if $\alpha, \beta \in K$.

(Since fin. many E, eventually you run out of things to adjoin).

Try $F(\alpha + c\beta)$ for $c \in F$, and by pigeonhole find c, c' with $F(\alpha + c\beta) = F(\alpha + c'\beta)$.

Then α and β are in this field, so it's $F(\alpha, \beta)$. ☺

65.3

Cyclotomy.

prim nth root of unity.

Properties of the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

Recall ζ_n is a root of $\Phi_n(x) = \prod_{\substack{(a,n)=1 \\ 1 \le a \le n-1}} (x - \zeta_n^a)$.

Had $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$

and so by MI

$$\Phi_n(x) = \prod_{d \mid n} (x^n - 1)^{\mu(n/d)}.$$

This is in $\mathbb{Z}[x]$ by Gauss' Lemma.

Theorem. We have an iso.

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times \leftarrow \text{abelian}$$

$$\{\zeta_n \to \zeta_n^a\}. \longleftarrow a$$

(1) This defines a function on $\mathbb{Q}(\zeta_n)$ because ζ_n is a primitive element.

$\{\zeta_n \to \zeta_n^a\}$

(2) is an automorphism because ζ_n^a is another root of $\Phi_n(x)$.

(3) This map is a homomorphism because

$$\{\zeta_n \to \zeta_n^b\} \circ \{\zeta_n \to \zeta_n^a\} = \{\zeta_n \to \zeta_n^{ab}\}.$$

(4) It is injective by construction.

(5) Surjective because any auto determined by its action on ζ_n.

65.4

Example. $\mathbb{Q}(\zeta_5)/\mathbb{Q}$. degree 4, Galois gp $\mathbb{Z}/4$.
By Galois theory it has a unique quadratic subfield.

Claim. It is $\mathbb{Q}(\zeta_5 + \zeta_5^{-1})$.
How might we go looking for this?
(1) It is a real subfield, fixed by complex conj.
(2) To say the same thing, write
$$\sigma_i = \{\zeta_5 \to \zeta_5^i\}.$$
Then subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ are
$$\{\sigma_1\}, \{\sigma_1, \sigma_{-1}\}, \{\sigma_1, \sigma_2, \sigma_3, \underset{\sigma_{-1}}{\underset{\parallel}{\sigma_4}}\}.$$

Notice that $\sigma_{-1} = \{\zeta_5 \to \zeta_5^{-1}\}$ is complex conjugation.

A basis for $\mathbb{Q}(\zeta_5)$ is $1, \zeta_5, \zeta_5^2, \zeta_5^3$ ~~ζ_5^4~~:

(what about ζ_5^4? $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0$.
Proof 1. Draw the picture
Proof 2. Invariant when you multiply by ζ_5.)

$\zeta_5 \to \zeta_5^{-1}$ acts by
$$a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3$$
$$\downarrow$$
$$a_0 + a_1\zeta_5^4 + a_2\zeta_5^3 + a_3\zeta_5^2$$
$$= a_0 + (-a_1\zeta_5^3 - a_1\zeta_5^2 - a_1\zeta_5 - a_1) + a_2\zeta_5^3 + a_3\zeta_5^2$$
$$= (a_0 - a_1) - a_1\zeta_5 + (a_3 - a_1)\zeta_5^2 + (a_2 - a_1)\zeta_5^3.$$

So demand: $a_0 - a_1 = a_0$, $-a_1 = a_1$, $a_3 - a_2 = a_1$, $a_2 - a_1 = a_3$

$\implies a_1 = 0$, $a_0 =$ arbitrary, $a_3 = a_2$.

65.5

So the fixed field of $\{\sigma_1, \sigma_{-1}\}$ is exactly

$$\{a_0 + a_2(\zeta_5^2 + \zeta_5^3) : a_0, a_2 \in \mathbb{Q}\}$$

$$= \{a_0 + a_2(-1 - \zeta_5 - \zeta_5^4) : \text{"} \}$$

$$= \{(a_0 - a_2) + (-a_2)(\zeta_5 + \zeta_5^4) : \text{"} \}$$

$$= \{b_0 + b_1(\zeta_5 + \zeta_5^4) : b_0, b_1 \in \mathbb{Q}\}$$

$$= \mathbb{Q}(\zeta_5 + \zeta_5^{-1}).$$

This implies: $\zeta_5 + \zeta_5^{-1}$ satisfies a quadratic poly w/ coeffs in $\mathbb{Q}$.

Let $n = p$ prime, then $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.
Note, a cyclic group has a unique subgroup of order 2.

It is $\{a \in (\mathbb{Z}/p\mathbb{Z})^\times : a = b^2 \text{ for some } b \in \mathbb{Z}/p\mathbb{Z}\}$
the subgroup of quadratic residues.

So $H := \{\sigma_a\}$ is a subgroup of index 2.
what is its fixed field?

Let $\alpha_H := \sum_{\sigma \in H} \sigma(\zeta_p)$.

Then α_H is fixed by H.
If $\tau \in H$, $\tau(\alpha_H) = \sum_{\sigma \in H} \tau\sigma(\zeta_p)$

$$= \sum_{\sigma \in H} \sigma(\zeta_p)$$

because $H \to H$, $\sigma \mapsto \tau\sigma$ is a bijection.

65:6

<u>Claim.</u> α_H is <u>not</u> fixed by the entire Galois group.

If $\tau \notin H$,

$$\tau(\alpha_H) = \sum_{\sigma \in H} \underbrace{\tau\sigma(\zeta_p)}_{\text{sum over a nontrivial coset!}}$$

Since $\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$ is <u>also</u> a basis for $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, none of the terms coincide and α_H is <u>not</u> in $\mathbb{Q}$.

So α_H <u>not</u> fixed by any auto <u>not</u> in H.

In particular $\mathbb{Q}(\alpha_H) \neq \mathbb{Q}$. Get a quadratic field.

<u>Gauss sums.</u>

Define the <u>quadratic</u> <u>Gauss</u> <u>sum</u>

$$G_p := \sum_{a \pmod p} \left(\frac{a}{p}\right) e^{2\pi i a/p}.$$

Notice this is also

$$\sum_{a \pmod p} \left(\left(\left(\frac{a}{p}\right) + 1\right) e^{2\pi i a/p}\right) = \sum_{b \pmod p} e^{2\pi i b^2/p}.$$

$$= 1 + 2\alpha_H$$

as described above.

<u>Theorem.</u> (Gauss)

$$G_p = \begin{cases} p^{1/2} & \text{if } p \equiv 1 \pmod 4 \\ i p^{1/2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

(Note: Can evaluate $(G_p)^2$ much more easily.)

<u>Therefore:</u> quadratic subfield is $\begin{cases} \mathbb{Q}(\sqrt{p}) & p \equiv 1 \ (4) \\ \mathbb{Q}(\sqrt{-p}) & p \equiv 3 \ (4) \end{cases}$

66.1

More on cyclotomic fields.

Write $H < \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ any subgroup,

$$q_H := \sum_{\sigma \in H} \sigma \zeta_p .$$

Then, by construction $\tau q_H = q_H$ for any $\tau \in H$.

(In general $G \longrightarrow G$, $g \longrightarrow g' g$ bijection.)

So $q_H \in \mathrm{Fix}(H)$.

Conversely, if $\sigma' \notin H$, then $\sigma q_H \neq q_H$.

why? σ' will send the elements $\{\sigma \zeta_p : \sigma \in H\}$ to a disjoint set, and $\zeta_p \dots \zeta_p^{p-1}$ (i.e. $\{\sigma \zeta_p : \sigma \in G\}$) forms a basis for the extension

So: $\mathbb{Q}(q_H) = \mathrm{Fix}(H)$.

Examples. The unique subgroup of $\mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$ of index 2 is (for $p \neq 2$) complex conjugation.

So $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is the unique subfield of index 2.

[Exercise. Find a cubic poly satisfied by $\cos\left(\frac{2\pi}{7}\right)$.

The unique quadratic subfield is gen by

$$\sum_{\substack{\sigma \in \text{unique} \\ \text{idx } 2}} \sigma \zeta_p = \sum_{\left(\frac{a}{p}\right)=1} \zeta_p^a .$$

See DF for a cool picture.

66.2

~~Prop~~ Recall.

$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ for all n.

If n and m are coprime, what is $[\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) : \mathbb{Q}]$?

Have $[\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}][\mathbb{Q}(\zeta_m) : \mathbb{Q}]$

because the φ-fn is multiplicative.

But we had

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n, \zeta_m)/\mathbb{Q}(\zeta_n)) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\text{intersection})$$

and so the intersection must be trivial, with

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n, \zeta_m)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$$

~~which is the~~ and

$$\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm}).$$ } easy enough to prove directly.

The iso above is the Chinese Remainder Theorem

$$(\mathbb{Z}/nm)^\times \cong (\mathbb{Z}/n)^\times \times (\mathbb{Z}/m)^\times.$$

The Inverse Galois Conjecture.

Let G be a finite group.
Then $\exists$ a field K with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

This is hard.

Theorem. True for abelian G.

66.3

Proof.

If G is abelian, write

$$G \cong \mathbb{Z}/m_1 \times \mathbb{Z}/m_2 \times \cdots \times \mathbb{Z}/m_k .$$

Invoke a theorem from analytic number theory:
There exist infinitely many primes $p \equiv 1 \pmod{m_i}$.
Various proofs of various levels of difficulty.

For each i, choose K_i and F_i to make this work.

$$\begin{array}{c} K_i = \mathbb{Q}(\zeta_{p_i}) \\ | \\ F_i \\ | \\ \mathbb{Q} \end{array} \qquad [K_i : \mathbb{Q}] = p_i, \quad [F_i : \mathbb{Q}] = m_i$$

Then all the p's are coprime, so the $\mathbb{Q}(\zeta_{p_i})$ are disjoint.

Get $\mathrm{Gal}(F_i/\mathbb{Q}) \cong \mathbb{Z}/m_i$ for each i and

$\mathrm{Gal}(F_1 \cdots F_k/\mathbb{Q}) \cong$ desired direct product.

Big Class Field Theory Theorem. (Kronecker–Weber)
Let $K/\mathbb{Q}$ abelian. Then $K \subseteq \mathbb{Q}(\zeta_m)$ for some m.

In other words, cyclotomic extensions over $\mathbb{Q}$ can be generated by nice objects.

Exercise. Generalize $\mathbb{Q}$ to any field.
(If you solve it, tell people I was your thesis advisor)

66.4 = 67.1

See book for constructible n-gons.

Require $\varphi(n)$ be a power of 2.

e.g.

$$\cos\left(\frac{2\pi}{17}\right) = \frac{1}{16}\Big[-1+\sqrt{17}+\sqrt{2(17-\sqrt{17})}$$
$$+2\sqrt{17+3\sqrt{17}-\sqrt{2(17-\sqrt{17})}-2\sqrt{2(17+\sqrt{17})}}\Big].$$

Think back: If you know this, can construct a 17-gon!

Polynomials:

General problem. Given separable $f(x) \in F[x]$ compute its Galois group (i.e. of splitting fld / F.) $\mathrm{Gal}(K/F)$

We have an injection

$$\mathrm{Gal}(K/F) \hookrightarrow \mathrm{Sym}(\{\text{roots of } F\}) \cong \mathrm{Sym}(n)$$

where $\deg f = n$.

Example: Suppose f splits completely over F.

Then any $\sigma \in \mathrm{Gal}(K/F)$ must send a root of f to a root of the same irred factor.

They're all linear. So $\sigma = 1$.

We knew that already, since $K = F$.

Example. Let f be irreducible.

If α, α' are two roots of f, then there is an iso $F(\alpha) \to F(\alpha')$, $\alpha \longrightarrow \alpha'$ extending to an auto of K.

Implies that the image of $\mathrm{Gal}(K/F)$ in $\mathrm{Sym}(n)$ be transitive.

66.5 = 67.2

(Note: A subgroup $H \le \mathrm{Sym}(n)$ is <u>transitive</u> if, for all $i, j \in \{1, \dots, n\}$ there exists $\sigma \in H$ with $\sigma(i) = j$.)

Also have: if $f = f_1 \cdots f_k$ factorization into irreducibles, then

$$\mathrm{Gal}(K/F) \hookrightarrow \mathrm{Sym}(n_1) \times \cdots \times \mathrm{Sym}(n_k).$$

<u>Caution</u>. Does not say $\mathrm{Gal}(K/F) \cong H_1 \times \cdots \times H_k$ for $H_i \le \mathrm{Sym}(n_i)$.

The embedding could be <u>non-diagonal</u>.

(A subgroup of $G_1 \times \cdots \times G_k$ is <u>diagonal</u> if it is of the form $H_1 \times \cdots \times H_k$ for $H_i \le G_i$.

Non-example: $\langle (1,1) \rangle \le (\mathbb{Z}/n)^2$.

Want to solve inverse Galois for $\mathrm{Sym}(n)$.

<u>Def</u>. The <u>elementary symmetric functions</u> in $x_1, \dots, x_n$ are:

$$s_1 = x_1 + \cdots + x_n$$

$$s_2 = x_1 x_2 + \cdots + x_{n-1} x_n$$

$$\vdots$$

$$s_n = x_1 \cdots x_n.$$

In other words "<u>general</u> <u>poly</u> of degree n"

$$(x - x_1)(x - x_2) \cdots (x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} \cdots \pm s_n$$

66.6 = 67.3.

For any field F, consider the extension

$$F(x_1, x_2, \cdots, x_n) / F(s_1, \ldots, s_n).$$

It is Galois, because it is a splitting field!

The Galois group is exactly $\mathrm{Sym}(n)$.
Any permutation of $\{1, \ldots, n\}$
induces a permutation of $\{x_1, \ldots, x_n\}$
hence a distinct elt. of $\mathrm{Gal}(F(x_1, \ldots, x_n)/F(s_1, \ldots, s_n))$.

Conversely, any elt. of this group is determined by what it does to the x_i.

Why do we know $F(s_1, \ldots, s_n) = \mathrm{Fix}(\mathrm{Sym}(n))$
(and is not just contained in it)?

$[F(x_1, \ldots, x_n) : \mathrm{Fix}(\mathrm{Sym}(n))] = n!$ by Galois theory

$[F(x_1, \ldots, x_n) : F(s_1, \ldots, s_n)] \leq n!$ since
~~the generic poly~~
former is a splitting field of a poly of degree n

The first field contains the latter.
So get equality.

<u>Cor.</u> (Fund. Thm on symmetric functions)

Let $f(x_1, \ldots, x_n) \in F(x_1, \ldots, x_n)$ be <u>symmetric</u>:
invariant under permutation of the x_i.
Then it is a rational function of the s_i.

<u>Proof</u>. It's in $\mathrm{Fix}(\mathrm{Sym}(n)) = F(s_1, \ldots, s_n)$. <u>Done</u>.

<u>In fact</u>: True for polynomials

67.4.

Example.

$$\underbrace{x_1^2 + x_2^2 + x_3^2}_{\text{symmetric}} = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3).$$

Definition. If $\overbrace{(x-\theta_1)(x-\theta_2)\cdots(x-\theta_n)}^{f(x)} \in F[x]$,

the discriminant of f is $\prod_{i<j}(\theta_i - \theta_j)^2$.

Do not need to assume the factorization is over F (can be over an extension field).

The discriminant is a symmetric function in the θ_i and (at least if F is separable) it is defined/F.

More specifically, given

$(x - x_1)\cdots(x - x_n) \in F(x_1, \dots, x_n)[x]$, with disc $\prod(x_i - x_j)^2$

the discriminant is defined over $F(s_1, \dots, s_n)[x]$.

Recall that, if $\delta = \prod_{i<j}(\theta_i - \theta_j)$,

$\mathrm{Alt}(n) = \{\sigma \in \mathrm{Sym}(n) : \sigma(\delta) = \delta\}$.

(Here identify $\mathrm{Sym}(n)$ with $\mathrm{Sym}(\{\theta_1, \dots, \theta_j\})$).

In this case $\delta = \sqrt{D}$ is a square root of the discriminant D.

So, in the field extension

$F(x_1, \dots, x_n) / F(s_1, \dots, s_n)$ with Galois group $\mathrm{Sym}(n)$,

if $\mathrm{char}(F) \neq 2$, then $\sqrt{D}$ generates the fixed field of $\mathrm{Alt}(n)$, hence a quadratic extension.

62.5 = 68.1
What this implies:

In general, the Galois group of $f(x) \in F[x]$ is a subgroup of $Alt(n)$ iff its discriminant D is a square in F.

Same thing:

Galois group $\subseteq Alt(n)$

$\Updownarrow$

each element fixes $\prod_{i<j} (a_i - a_j) = \sqrt{D}$.

Example. $Disc(x^3 - x - 1) = -23$.

Since that poly. is irreducible $/\mathbb{Q}$, it generates a cubic extension K.

Let $\tilde{K}$ be the splitting field.

Then $\tilde{K} \not\subseteq Alt(3) = C_3$ and $\tilde{K} \ni \sqrt{-23}$.

So $\tilde{K}$ ~~generates~~ has Galois group $Sym(3)$.

Example. $Disc(x^3 - x^2 - 2x + 1) = 49$.

So the cubic ext. gen by that polynomial has Galois group C_3. (Not obvious.)

$67.6 = 68.2$

So how do you compute discriminants?

Given $f(x) = x^3 + ax^2 + bx + c.$

Step 1. $x = y - \frac{a}{3}$. (Doesn't change differences between the roots).

$g(y) = y^3 + py + q,$ $\quad p = \frac{1}{3}(3b - a^2)$

$q = \frac{1}{27}(2a^3 - 9ab + 27c)$

$\mathrm{Disc}(f) = \mathrm{Disc}(g).$

Now, $\mathrm{Disc}\, g = (\theta_1 - \theta_2)^2 (\theta_1 - \theta_3)^2 (\theta_2 - \theta_3)^2$

where $y^3 + py + q = (y - \theta_1)(y - \theta_2)(y - \theta_3)$

so that $\cancel{\theta_1 + \theta_2 + \theta_3 = 0}$

$\theta_1 \theta_2 \theta_3 = -q$

$\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3 = p$

$\theta_1 + \theta_2 + \theta_3 = 0$.

One clever trick.

$$\frac{dg}{dy} = (y-\theta_1)(y-\theta_2) + (y-\theta_1)(y-\theta_3) + (y-\theta_2)(y-\theta_3)$$

Plug in $\theta_3 \Rightarrow$ get $(\theta_3 - \theta_1)(\theta_3 - \theta_2)$ and so on.

So

$$\mathrm{Disc}(g) = -\left[\left(\frac{dg}{dy}\right)(\theta_1) \cdot \left(\frac{dg}{dy}\right)(\theta_2) \cdot \left(\frac{dg}{dy}\right)(\theta_3)\right]$$

But $\frac{dg}{dy} = 3y^2 + p$, get

$$-\mathrm{Disc}(g) = (3\theta_1^2 + p)(3\theta_2^2 + p)(3\theta_3^2 + p)$$

68.3,

So,

$$-\mathrm{Disc}(g) = 27(\theta_1\theta_2\theta_3)^2 + 9p(\theta_1^2\theta_2^2 + \theta_1^2\theta_3^2 + \theta_2^2\theta_3^2)$$
$$+ 3p^2(\theta_1^2 + \theta_2^2 + \theta_3^2) + p^3.$$

Now
$$\theta_1^2\theta_2^2 + \theta_1^2\theta_3^2 + \theta_2^2\theta_3^2 = (\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3)^2 - 2\theta_1\theta_2\theta_3(\theta_1 + \theta_2 + \theta_3)$$
$$= p^2$$

$$\theta_1^2 + \theta_2^2 + \theta_3^2 = (\theta_1 + \theta_2 + \theta_3)^2 - 2(\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3)$$
$$= -2p$$

So
$$-\mathrm{Disc}(g) = 27(-q)^2 + 9p(p^2) + 3p^2(-2p) + p^3$$
$$\mathrm{Disc}(g) = \mathrm{Disc}(f) = -4p^3 - 27q^2$$
$$= a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

Summary

Galois group of a cubic.

(1) Reducible? Then easy.

(2) Irreducible? Galois group is C_3 or D_3.

See if $\mathrm{Disc}(f) \in F^2$.

If it is then $K = F(\theta)$ for any root θ of f.

If it isn't then $K = F(\theta, \theta')$ for any two roots θ, θ' of f.

Also $K = F(\theta, \sqrt{D})$ with $D = \mathrm{Disc}(f)$.

Generators: Full symmetric group on $\theta, \theta', \theta''$
$\sqrt{D}$ is either left alone or flipped.

68.4.

Galois groups of quartics.

Reducible ⇒ can be $C_3, S_3, C_2, C_1, C_2 \times C_2$.
$F(\sqrt{D_1}, \sqrt{D_2})$

Irreducible ⇒ Galois acts transitively on the roots $\{\theta, \theta', \theta'', \theta'''\}$.

Transitive subgroups of S_4:
$S_4, A_4, D_4, C_2 \times C_2 = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$,
C_4.

Let's be clever. Define

$$\alpha_1 = (\theta + \theta')(\theta'' + \theta''')$$
$$\alpha_2 = (\theta + \theta'')(\theta' + \theta''')$$
$$\alpha_3 = (\theta + \theta''')(\theta' + \theta'')$$

Then Sym(4) acts transitively on $\{\alpha_1, \alpha_2, \alpha_3\}$.
Kernel of the action is V_4.
Stabilizer of any α_i is $\cong D_4$. (conjugate 2-Sylow subgroups).

Now,

$(x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = $ [something you can actually compute, w/ coeffs in F].

This is the resolvent cubic of f.

68.5.

Can compute:

(1) $\left[(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)\right]^2$

$$= \left[(\theta-\theta')(\theta-\theta'')\cdots(\theta''-\theta''')^2\right],$$ so

a quartic has the same discriminant as its resolvent cubic.

(2) Galois group $\leq A_4 \iff$ Disc is a square.

(3) Galois group $\leq V_4 = C_2 \times C_2$

$\iff$ Resolvent cubic factors over F.

(4) Galois group $\leq D_4$

$\iff$ Resolvent cubic has a root over F.

(with equality if only one root).

		$\leq A_4$?	$\leq V_4$?	$\leq D_4$?
	S_4	✗	✗	✗
Galois group	A_4	✓	✗	✗
	V_4	✓	✓	✓
	D_4	✗	✗	✓
	C_4	✗	✗	✓

68.6.

How to tell C_4 from D_4?

Group theory tels us $D_4 \cap A_4 = V_4$

$C_4 \cap A_4 \cong C_2$

$= \{1, (1\ 3)(2\ 4)\}$.

In this case $\sqrt{D} \notin F$, so factor the original quartic over $F(\sqrt{D})$.

Galois group of that is $G \cap A_4$.

Gal acts transitively on the roots $\longleftrightarrow$ Polynomial is irreducible.

So: Quartic factors over $F(\sqrt{D}) \Rightarrow C_4$.

Doesn't $\longrightarrow D_4$.

69.1

Fundamental Theorem of Algebra.

<u>Thm.</u> $\mathbb{C}$ is algebraically closed.

Need two stipulations.

1. Let $f(x) \in \mathbb{R}[x]$ be of odd degree. Then f has a root in $\mathbb{R}$.) So <u>no</u> extensions of $\mathbb{R}$ of odd degree.
2. Quadratic polys $\in \mathbb{C}[x]$ split over $\mathbb{C}[x]$.

<u>Proofs</u>. 1. IVT in calculus.

2. Compute directly.

Proof of FTA: If $f \in \mathbb{C}[x]$, f has a root in $\mathbb{C}$.

(a) Reduction. Can take $f \in \mathbb{R}[x]$.

Consider $f \cdot \bar{f}$. Conjugation invariant so in $\mathbb{R}[x]$.

(b) Let K = split field of $f/\mathbb{R}$,

Then $K(i)/\mathbb{R}$ is <u>Galois</u>.

Write $G = \mathrm{Gal}(K(i)/\mathbb{R})$

P_2 = any 2-Sylow subgroup of G.

$$
\begin{tikzcd}
1 \arrow[d, dash] & & K(i) \arrow[d, dash, "\text{2-power degree}"] \\
P_2 \arrow[dr, dash] & \xrightarrow{\mathrm{Fix}(\cdot)} & E \arrow[dr, dash, "\text{odd}"] & \\
& G & & \mathbb{R}
\end{tikzcd}
$$

Must have $[E : \mathbb{R}] = 1$ by Stipulation 1.

So $\mathrm{Gal}(K(i)/\mathbb{R})$, hence $\mathrm{Gal}(K(i)/\mathbb{C})$, is a 2-group.

But p-groups have subgroups of all possible orders!
Hence get a quadratic extension $\Rightarrow$ Stipulation 2.

69.2

Solvability by radicals.

Theorem. "The general quintic is insoluble."

What does that mean?

We say, $a \in \bar{F}$ can be solved by radicals if there is a series of extensions

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n = K$$

with $a \in K$ and $F_{i+1} = F_i(\sqrt[n_i]{a_i})$ for some $n_i \in \mathbb{Z}^+$, $a_i \in F_i$ for each i.

Think expressions like

$$\frac{1}{3}\left(\sqrt[3]{26+15\sqrt{3}} + \sqrt[3]{26-15\sqrt{3}} - 1\right)$$

which is the unique real root of $x^3 + x^2 - 2 = 0$.

Want to understand these root extensions.

If we like, can adjoin roots of unity to F first.

Def. An extension K/F is cyclic if it is Galois with cyclic Galois group.

~~Theorem~~ Proposition. Suppose F contains μ_n, the nth roots of unity. Also char$(F) \nmid n$.

Then, $F(\sqrt[n]{a})/F$ is cyclic with degree dividing n.

69.3
<u>Proof</u>. $F(\sqrt[n]{a})$ is the <u>splitting field</u> of $x^n - a$,

<u>because</u> $\mu_n \subseteq F$.

Define $\quad \mathrm{Gal}(K/F) \longrightarrow \mu_n$

$$\begin{array}{ccc} \sigma & \longrightarrow & \zeta_\sigma . \\ \| & & \| \\ \{\sqrt[n]{a} \to \zeta_\sigma \sqrt[n]{a}\} & & \dfrac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} , \end{array}$$

Since $\mathrm{Gal}(K/F)$ fixes ζ_σ, have $\zeta_{\sigma\tau} = \zeta_\sigma \zeta_\tau$.

Get a WD homomorphism. (Action on $\sqrt[n]{a}$ determines it.)

Injective because $\sqrt[n]{a}$ generates K/F.

The <u>converse</u> is true.

<u>Prop</u>. Let $\mathrm{char}(F) \nmid n$ and $\mu_n \subseteq F$, K/F <u>cyclic</u> of deg n

Then $K = F(\sqrt[n]{a})$ for some $a \in F$.

Will give a highbrow proof later.

Lowbrow proof.

"Lagrange resolvents"

$$(\alpha, \zeta) = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha)$$

for any $\alpha \in K$, $\zeta \in \mu_n$.

By direct computation,

$$\sigma(\alpha, \zeta) = \zeta^{-1}(\alpha, \zeta).$$

Therefore, $\sigma(\alpha, \zeta)^n = (\alpha, \zeta)^n$ so $(\alpha, \zeta)^n \in F$.

Recall <u>linear independence of automorphisms</u>.

There is some $\alpha \in K$ with $(\alpha, \zeta) \neq 0$ for any <u>primitive</u> $\zeta \in \mu_n$.

Fixing such ζ, (α, ζ) is in K and <u>not</u> any subfield

Therefore $K = F(\sqrt[n]{(a,\zeta)})$.

This forms the basis of Kummer theory (more later)

What this buys us: If $\alpha \in \bar{F}$ can be solved by radicals, there is a chain of cyclic extensions

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m \ni \alpha$$

with each K_{i+1}/K_i cyclic.

(Adjoin as many roots of unity as we want first.)

Moreover, ~~get~~ can choose K_n to be Galois $/F$.

whenever we adjoin $\sqrt[n_i]{a_i}$, do the same to all its Galois conjugates. By induction all the K_i are Galois $/F$.

What is $\mathrm{Gal}(K_m/F)$?

Look at $\mathrm{Gal}(K_m/K_i)$ above

$$\cancel{G_3 \subseteq G_2 \subseteq G_1 \subseteq 1}$$

$$G = G_0 \subseteq \cdots\cdots \subseteq G_{m-2} \subseteq G_{m-1} \subseteq G_m = 1.$$

We know: each G_i is normal in G

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

Therefore $\mathrm{Gal}(K_m/F)$ is a solvable group.

69.5

(1) Recall: A group G is solvable if there exists a chain

$$1 = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_n = G$$

with each H_{i+1}/H_i abelian.

We can replace "abelian" with "cyclic"
(break up into smaller parts)

(2) Subgroups and quotients of solvable groups are solvable

(3) If $H \trianglelefteq G$ and G/H are solvable, so is G.

We get, if $\alpha \in F$ can be solved by radicals ⇔ it is contained in K with $\mathrm{Gal}(K/F)$ solvable.

But, in fact, if α can be solved by radicals, its min poly $f(x)$ generates a solvable group.
(Quotient of $\mathrm{Gal}(K/F)$.)

Example. S_n is not solvable for $n \geq 5$.
(Group theory!)

Example. $x^5 - 6x + 3$.
irreducible / $\mathbb{Q}$ by Eisenstein at $p = 3$.
So G = Galois group $\subseteq S_5$ has order divisible by 5
hence has a 5-cycle.

It has 3 real roots exactly.
$f(-2) = -17$, $f(0) = 3$, $f(1) = -2$, $f(2) = 23$.
Do some calculus, Descartes' rule of signs etc.

So complex conjugation acts as a transposition in S_5.

And, any transposition and 5-cycle generate S_5.

<u>Theorem.</u> The poly $f(x)$ can be solved by radicals iff its Galois group is solvable.

<u>Proof.</u> $\Longrightarrow$ Let G be its Galois group.
We saw that there is a Galois extension K/F, in which f splits, such that $Gal(K/F)$ solvable
But G is a quotient of $Gal(K/F)$, hence solvable

$\Longleftarrow$: Let K be splitting field for $f(x) \in F[x]$ with $G = Gal(K/F)$ solvable.
Write
$$F = K_0 \subset K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n = K$$
with each K_{i+1}/K_i cyclic.

Let $F' = F\big(\text{all roots of unity w/ order dividing any } [K_{i+1} : K_i]\big)$.

Consider
$$F \subseteq F' \subseteq F'K_0 \subseteq F'K_1 \subseteq \cdots \subseteq F'K_n.$$

For each i, $F'K_{i+1}/F'K_i$ is cyclic too:
$$Gal(F'K_{i+1}/F'K_i) \longrightarrow Gal(K_{i+1}/K_i)$$
$$\sigma \longrightarrow \sigma|_{K_{i+1}}$$
an injective map
So these are <u>subgroups</u> of the cyclic $Gal(K_{i+1}/K_i)$, so cyclic.

(Recall:
$$Gal(F'K_{i+1}/F'K_i) \cong Gal(K_{i+1}/K_{i+1} \cap F'K_i))$$

Also have $F \subseteq F'$ a chain of cyclic extensions.

Use the converse theorem! Can be generated by radicals. //

See DF for Cardano formulas, etc.

Galois groups over $\mathbb{Q}$:

Let $f(x) \in \mathbb{Z}[x]$ separable.

Can we compute its Galois group?

Factor mod p, for some prime p.

If $p \nmid \mathrm{Disc}(f)$, then the polynomial will also be separable over $\mathbb{F}_p$.

Thm from algebraic NT.

In the above scenario, there is an injection

$$\mathrm{Gal}(\bar{f}/\mathbb{F}_p) \hookrightarrow \mathrm{Gal}(f/\mathbb{Q}).$$

Indeed, true as permutation groups on the roots.

Note also the LHS is cyclic.

Example. $x^5 - x - 1$, $\mathrm{Disc} = 19 \cdot 151$.

(mod 2), is $(x^2 + x + 1)(x^3 + x^2 + 1)$

(both factors irreducible)

So the Galois group $\subseteq S_5$ has an elt. conjugate to $(1\,2)(3\,4\,5)$.

(And hence a 2-cycle and a 3-cycle.)

(mod 3), is irreducible,

So must be irreducible / $\mathbb{Z}$. G contains a 5-cycle,

Hence is S_5.

70.3.

Proposition/exercise. Let p be a prime. If $G \le S_p$ contains a p-cycle and a transposition, then $G = S_p$.

False if p is not a prime!

Example. (1) $x^4 - x^3 - x^2 + x + 1$.

Reduce modulo various primes. Get:

* Sometimes it factors completely
* Sometimes two quadratic factors.
* Sometimes irreducible.

(2) $x^4 - x + 1$.

* All that, and (cubic) $\cdot$ (linear).

(3) $x^4 + 1$.

* All linear factors or two quadratic.

Never irreducible (mod p)

Basic theorem. Let $p \nmid \mathrm{Disc}(f)$, and suppose f reduces (mod p) into irred factors of degree $n_1, n_2, \dots, n_k$ with $n_1 + \dots + n_k = n = \deg(f)$.

Then: $\mathrm{Gal}(f/\mathbb{Q})$ contains a permutation of cycle type $(n_1, \dots, n_k)$.

70.4.

Example. Quartic polynomials.

$\mathrm{Gal}(f/\mathbb{Q})$	Cycle types
S_4	all: (4), (2 2), (3 1), (2 1 1), (1 1 1 1)
C_4	(4), (1 1 1 1), (2 2)
V_4	(1 1 1 1), (2 2)
D_4	(4), (1 1 1 1), (2 2)
A_4	(1 1 1 1), (2 2), (3 1)

So reduce (mod p) for lots of primes, see what cycle types occur.

Theorem. All the possible splitting types have to occur eventually.

But quantify "eventually"?

Even for $x^2 - a$ $\begin{cases} \text{splits if } \left(\frac{a}{p}\right) = 1 \\ \text{irred if } \left(\frac{a}{p}\right) = -1. \end{cases}$

Consider, e.g. $x^2 - q$ for q prime $\equiv 1 \pmod 4$.

Then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

So $x^2 - q$ $\begin{cases} \text{splits if } \left(\frac{p}{q}\right) = 1 \\ \text{irred if } \left(\frac{p}{q}\right) = -1. \end{cases}$

Theorem (Burgess)

Let q be an odd prime.

The least quadratic nonresidue (mod q) is $\ll p^{\frac{1}{4\sqrt{e}} + \varepsilon}$.

This sucks. But try to do better. (I DARE YOU)

70.5

Summary of the end:

* Transcendental extensions.

Note that $\mathbb{Q}(\pi) \cong \mathbb{Q}(t)$.

Given an arbitrary extension E/F, can find an intermediate $E \supseteq K \supseteq F$ s.t.:

E/K algebraic

K/F transcendental and "algebraically independent".

Iso to F(some number of indeterminates).

# of indeterminates is an invariant, the <u>transcendance degree</u> of E/F.

<u>Example</u>. Fraction field of $\mathbb{C}[x,y]/(y^2 - x^3 - x)$.

This has transcendence degree 1.

It is the "function field" of the <u>elliptic</u> <u>curve</u>

$$y^2 = x^3 + x.$$

It is not "purely transcendental": can't take $E=K$.

<u>Infinite Galois theory.</u>

Let E/F infinite degree. It's <u>Galois</u> if it's algebraic, normal, and separable.
(splitting field for some polys).

Lose a lot of theorems! Turns out to be

$$\varprojlim_{K \subseteq E} \mathrm{Gal}(E/F).$$