Suppose $F$ is a field and $f: \mathbb{C}[x] \rightarrow F$ is a ring homomorphism. Then either

1. $f$ is injective ($\ker(f) = (0)$)
2. $\ker(f) = (x-\alpha)$, $\alpha \in \mathbb{C}$ (namely $\ker(f)$ is maximal).

**Proof:** In $\mathbb{C}[x]$, we've shown in class maximal ideals are the same as $(x-\alpha)$, $\alpha \in \mathbb{C}$. So if $\ker(f) = (x-\alpha)$, then we're done. Assume $\ker(f) \neq (0)$ and since it's not maximal, we have $\ker(f) = (h(x), g(x))$ w/ $h, g$ irreducible $\Rightarrow \deg(h), \deg(g) \geq 1$. 

[Principal idea: domain, every looks like $\ker(f)$]
\[ \ker(f) = (h(x)g(x)) \iff h(x), g(x) \in (h(x)g(x) = \ker(f)) \]

Let's apply \( f \) to \( h(x)g(x) \):

\[ 0 = f(h(x)g(x)) = f(h(x)) \cdot f(g(x)) \in \mathbb{F} \]

Since \( \mathbb{F} \) is a field

\[ \Rightarrow h(x) \text{ or } g(x) \in \ker(f) = (h(x)g(x)) \]

\[ \Rightarrow \ker(f) = 0. \quad \text{(Works for } \mathbb{F} \text{ an integral domain)} \]
Abstract symbols

\[ \text{ev} : \overline{F_2} [x] \rightarrow \text{Fun} (\overline{F_2}, \overline{F_2}) \]

\[ f(x) \mapsto \phi \in \text{Fun} (\overline{F_2}, \overline{F_2}) \]

\[ \text{deg. } \phi (a) = f(a) \quad \forall a \in \overline{F_2} \]

\[ p = 7 : \quad x^6 + 5x + 1 \in \overline{F_2} [x] \]

\[ (1, 5, 0, 0, 1, 0, 1, 1) \]

\[ (8, 2, 3, 4, 8, 6) \]
$$\chi_a(x) = \begin{cases} 1 & x = a \\ 0 & x \neq a \end{cases} \quad g(a) \neq 0.$$ 

$$f(x) = g(x) \cdot g(a)^{-1}$$

$$\text{iff} \quad x - b \mid f(x)$$

$$\text{iff} \quad \forall b \neq a \quad x - b \mid g(x)$$

$$g(x) = \prod_{b \neq a} (x - b), \quad g(a) = \prod_{b \neq a} (a - b) \neq 0$$
Q: Special case of Bezout's Thm

Ramification points of Riemann surfaces
Ex: Let \( L = V(ax + by + c) = \{(x, y) : ax + by + c = 0\} \subseteq \mathbb{C}^2 \).

Let \( f \in \mathbb{C}[x, y] \) be a degree \( d \) irreducible poly.

Show that \( V(f) \cap L \) has at most \( d \) points,

unless \( V(f) \supseteq L \). (\( \deg(f) \leq (ax + by + c) \iff ax + by + c \mid f \) )

So I want to do an even more specialized version which will illuminate the approach.

Take \( a = c = 0, b = 1 \) \( \Rightarrow L = V(y) = \{(x, 0)\} \).
Let $f(x, y) = \sum_{j=0}^{d} f_j(y) \times j$ where $f_j(y)$ is a polynomial in $y$ of degree $\leq d-j$.

What is $V(y)$? $V(y) = \{(x, 0)\}$

$= \{(x, y) : y = 0\}$

$V(f) \cap L = V(f) \cap V(y) \iff$ Solution to

$\{(x, 0) : \sum_{j=1}^{d} f_j(0) \times j = 0\}$

In particular, $f_j(0) \in \mathbb{C}$, has $\leq d$ roots.
\[ o = \sum_{j=0}^{d} f_j(0) \mathbf{x}^j \in \mathbb{C}[\mathbf{x}] \quad \text{of deg} \leq d \quad \text{(i.e., if) } \]
\[ f_j(0) \neq 0, \quad \text{is of degree } d, \quad \deg(f) = \max_{f_j(0) \neq 0} j. \]

We know every polynomial over \( \mathbb{C} \) with degree \( e \leq d \) has \( e \) roots, hence

\[ |V(f) \cap \mathbb{C}| = e = \deg(f) \leq d. \]
For general case, use a similar argument but w/ $y = -\frac{a}{b}x - \frac{c}{b}$ instead of 0.
Ramification:

(Thm 11.9.16)

\[ f(x,y) \in \mathbb{C}[x,y] \]

\[ O \to \mathbb{C} \]

\[ \mathbb{R}^2 \]

\[ \mathbb{R} \]

\[ \mathbb{C}^2 \]

\[ \pi_x \]

\[ \pi_y \]

\[ y = (x-1) \times (x+1) \]

\[ |\pi_y^{-1}(y_0)| = 2 \leftarrow \text{Ramifies} \]

Ramification points are where the preimage of
the projection is not "full"
Ex: Does the following Riemann surface have ramification points? If so, where?

\( f(x,y) = y^2 - x^3 + x^2 + x = 0 \) ← The set of \((x,y)\) making this true is called a Riemann surface

Sol: Need to check if \( f \) and \( \frac{\partial f}{\partial y} \) share any roots.

\[ \frac{\partial f}{\partial y}(x,y) = 2y = 0 \iff y = 0 \] (only root of \( \frac{\partial f}{\partial y} \))
$y=0$ is only root of $\frac{\partial f}{\partial y}$, let's plug into $f(x,y)=0$. 

\[ f(x,0) = -x^3 + x^2 + x = 0 = -\left(x^3 - x^2 - x\right) = -x(x^2 - x - 1) \]

**Quadratic formula** $\Rightarrow$ 

\[ x = \frac{1 \pm \sqrt{5}}{2} = \varphi, \bar{\varphi} \]  

(Golden ratio)

\[ f(x,0) = -x(x-\varphi)(x-\bar{\varphi}) = 0 \]

$\Rightarrow$ roots are $0, \varphi, \bar{\varphi}$. $\Rightarrow$ $\frac{\partial f}{\partial y} \neq 0$ share the roots $(0,0), (\varphi,0), (\bar{\varphi},0)$. 

**Claim:** $0, \varphi, \bar{\varphi}$ are ramification points.
Claim: $f$ ramifies at $0, \varphi, \overline{\varphi}$.

$\Pi^{-1}(0) = \{ (0, y) : y^2 - 0 \cdot \varphi \cdot (0 - \varphi) = 0 \} = \{ (0, y) : y^2 = 0 \} = \{ (0, 0) \}$

$\Pi^{-1}(\varphi) = \{ (\varphi, y) : y^2 - \varphi \cdot (\varphi - \varphi) \cdot (\varphi - \overline{\varphi}) = 0 \} = \{ (\varphi, 0) \}$

$\Pi^{-1}(\overline{\varphi}) = \{ (\overline{\varphi}, y) : y^2 - \overline{\varphi} \cdot (\varphi - \overline{\varphi}) \cdot (\overline{\varphi} - \varphi) = 0 \} = \{ (\overline{\varphi}, 0) \}$

Since these are each of size 1 (<2), these are ramification points.
Ex: \[ f(x,y) = y - x(x-1)(x+1) = 0 \]

does not ramify as a projection to complex \( x \)-plane since

\[ \frac{\partial f}{\partial y} = 1 \neq 0 \implies f \not\equiv \frac{\partial f}{\partial y} \text{ can never share a root, so no ramification.} \]

\( \text{Take } x = \pm \frac{\sqrt{3}}{3} \text{.} \)
Q: 
- Irreducible polys in \( \mathbb{F}_p[x] \) using "Sieve of Eratosthenes"

- Example of poly \( f(x) \) which is irreducible over \( \mathbb{Q} \) (in \( \mathbb{Q}[x] \)) but reducible mod every prime
Sieve of Eratosthenes: An algorithm to find all prime numbers up to a given limit, $L \in \mathbb{Z}_{>0}$. (Around 2000 or more years old)

How: Write all numbers up to $L$ i.e. starting at 2 (first prime), cross out all multiples of 2 up to $L$. Then cross out all multiples of 3, then all multiples of 5 i.e. so on. List remaining at the end will be all primes less than $L$. 
$L = 30: \overline{1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 19\ 20\ 21\ 22\ 23\ 24\ 25\ 26\ 27\ 28\ 29\ 30}

\Rightarrow \text{The set of primes } \leq 30 \text{ is}

\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}

* If \( F \) is a field, \( \text{IF} \times \text{IF} \) is a PID *
Let's try to find all irreducible (\(=\) prime) polynomials in \(\mathbb{F}_2[x]\) of degree \(\leq 4\). \(\mathbb{F}_2 = \{0, 1\}\):

\[
\begin{align*}
&1, \quad x, \quad x + 1, \quad x^2, \quad x^2 + 1, \quad x^2 + x, \quad x^2 + x + 1, \quad x^3, \quad x^3 + 1, \quad x^3 + x, \\
&x^3 + x + 1, \quad x^3 + x^2, \quad x^3 + x^2 + 1, \quad x^3 + x^2 + x, \quad x^3 + x^2 + x + 1, \quad x^4, \quad x^4 + 1, \quad x^4 + x, \\
&x^4 + x + 1, \quad x^4 + x^2, \quad x^4 + x^2 + 1, \quad x^4 + x^2 + x, \quad x^4 + x^2 + x + 1, \quad x^5, \quad x^5 + 1, \quad x^5 + x, \\
&x^5 + x^2, \quad x^5 + x^2 + 1, \quad x^5 + x^2 + x, \quad x^5 + x^2 + x + 1, \quad x^6, \quad x^6 + 1, \quad x^6 + x, \\
&x^6 + x^2, \quad x^6 + x^2 + 1, \quad x^6 + x^2 + x, \quad x^6 + x^2 + x + 1, \quad x^7, \quad x^7 + 1, \quad \ldots
\end{align*}
\]
\[(x^2 + x + 1)^2 = (x^2 + x + 1)(x^2 + x + 1) = x^4 + x^3 + x^2 + x^3 + x^2 + x + x^2 + x + 1\]

\[= x^4 + x^2 + 1 \quad \text{Reducible !!!}\]

\[\Rightarrow \text{All primes = irreducibles in } F_2[x] \text{ of degree at most 4 are}\]

\[\{1, x, x+1, x^2+1, x^3+1, x^4+x+1, x^4+x^3+x+1, x^4+x^3+1\}\]
Example of poly $f(x)$ which is irreducible over $\mathbb{Q}[x]$ but reducible in $\mathbb{F}_p[x]$ for every prime.

Consider $f(x) = x^4 + 1 \in \mathbb{Z}[x]$.

Claim 1: $x^4 + 1$ is irreducible over $\mathbb{Q}$.

Motivation: "complex analytic". Since $\mathbb{Q} \subseteq \mathbb{C}$, $\mathbb{Q}[x] \subseteq \mathbb{C}[x]$ so if $f$ reduces in $\mathbb{Q}$, it better match up with the reduction over $\mathbb{C}$. 

$\sqrt[4]{3} = 3^{\frac{1}{4}} = 3$

$z_4 = e^{\frac{\pi i}{4}}$

$x^4 + 1 = 0 \iff x^4 = -1 \quad (\overline{x}_4 = e^{\pi i} = -1)$

$\overline{x}_4 = -1$

$f(x) = x^4 + 1$ has 4 roots $\pm 1, \pm i$

$x^4 + 1 = (x - 1)(x + 1)(x - i)(x + i)$

$f$ is irreducible over $\mathbb{Q}$.

$\mathbb{Q}[x] \not\cong \mathbb{Q}^4$
Second approach: Eisenstein criteria.

If \( f(x) \) has rational root, then so does \( f(x+1) \) (same holds for irreducibility over \( \mathbb{Q} \)). So let's look at

\[
f(x+1) = (x+1)^4 + 1 = (x^4 + 4x^3 + 6x^2 + 4x + 1) + 1 \\
= x^4 + 4x^3 + 6x^2 + 4x + 2.
\]

Take \( p = 2 \) in Eisenstein:  
① \( p = 2 \mid a_0, a_2, a_3, a_4 = 2, 4, 6, 4 \)  
② \( p = 2 \times a_0 = a_4 = 1 \)  
③ \( p^2 = 4 \times a_0 = 2 \)  
By Eisenstein, \( x^4 + 1 \) is irreducible.
Q: Finish showing $x^4 + 1$ is reducible mod every prime (but irreducible over $\mathbb{Q}$ [by Eisenstein]).

Group actions & Cauchy's Thm (for $p | |G|$, $\exists g \in G$ s.t. $\text{ord}(g) = p$)
Claim: $X^4 + 1$ is reducible mod every prime.

Sol.: We do this by investigating certain elements in $\mathbb{F}_p$ & checking whether they are squares.

Case 1: If $-1$ is a square (mod $p$). (works for $p = 2$)

$\Rightarrow \exists r \in \mathbb{F}_p$ s.t. $r^2 \equiv -1$ (mod $p$). Then

$X^4 + 1 = X^4 - (-1) \equiv X^4 - r^2 \equiv (X^2 - r)(X^2 + r) \pmod p$

$\Rightarrow$ reducible.
Case 2: If 2 is a square mod p

\[ \Rightarrow \exists s \in \mathbb{F}_p \text{ s.t. } s^2 \equiv 2 \pmod{p}. \]

Then

\[ x^4 + 1 = x^4 + 2x^2 + 1 - 2x^2 = (x^2 + 1)^2 - 2x^2 \]

\[ \equiv (x^2 + 1)^2 - (sx)^2 \equiv ((x^2 + 1) - sx)(x^2 + 1 + sx) \pmod{p} \]

\[ \Rightarrow \text{reducible}. \]

Case 3: If neither -1 or 2 is a square mod p

\[ \Rightarrow -2 \text{ is a square s.t. } \exists t \in \mathbb{F}_p \text{ s.t. } t^2 \equiv -2 \pmod{p}. \]
We have that $\mathbb{F}_p^*$ is a cyclic group. Fact we'll use.

So $\exists a \in \mathbb{F}_p^*$ s.t. $\langle a \rangle = \mathbb{F}_p^*$, i.e. every non-zero element is a power of $a$.

Since $-1 \notin 2$ were not squares, $\exists n, m \in \mathbb{Z}_{\geq 0}$ s.t.

$-1 \equiv a^{2n+1} \pmod{p}$ and $2 \equiv a^{2m+1} \pmod{p}$. Well,

$-2 \equiv (-1)(2) \equiv a^{2n+1} a^{2m+1} \equiv a^{2(n+m+1)} \pmod{p}$

$\& -2$ is a square (of $a^{n+m+1}$) mod $p$. 
So $\exists t \in \mathbb{F}_p$ st. $t^2 \equiv -2 \pmod{p}$. Then $(-2x^2) = -(tx)^2$.

\[
X^4 + 1 = X^4 - 2x^2 + 1 + 2x^2 = (X^2 - 1)^2 + 2x^2 \\
\equiv (X^2 - 1)^2 - (tx)^2 \equiv ((x^2 - 1) - tx)((x^2 - 1) + tx) \pmod{p}.
\]

$\Rightarrow$ reducible.

This covers all primes, we have $X^4 + 1$ is reducible mod every prime, but irreducible over \mathbb{Q}.
Note: $x^2 + 1$ is reducible mod every prime $p$.

Not: $p \equiv 1 \pmod{4}$ (Quadratic reciprocity)

In this case, $-1$ is a square mod $p$. 
**Group Actions**

Let $G$ be a group, $X$ be a set. A group action of $G$ on $X$ is a map $\cdot : G \times X \to X$ s.t.

$1_G \cdot x = x \quad \forall x \in X$

$g \cdot (h \cdot x) = (gh) \cdot x \quad \forall g, h \in G, \forall x \in X$

**Ex:** Any group acts on itself by left-multiplication: $g \cdot x = gh$
Given \( x \in X \), define the orbit of \( x \), \( \text{orb}(x) \) or \( O_x \), is

\[
X \ni O_x = \{ g \cdot x : g \in G \} = \{ y \in X : \exists g \in G : y = g \cdot x \}
\]

the stabilizer of \( x \) is \( \text{Stab}(x) = \{ g \in G : g \cdot x = x \} \leq G \)

* In general, \( \text{Stab}(x) \) is not normal

Thm: (Orbit-Stabilizer) For a group \( G \) s.t. \( |G| < \infty \), \( \forall x \in X \)

\[
|G| = |O_x| \cdot |\text{Stab}(x)|.
\]

\[
\frac{G}{\text{Stab}(x)} \cong O_x \; \text{as sets, not groups}
\]
Thm. (Cauchy) Let $|G| = p^m < \infty$, w/ $(p, m) = 1$, $p$ prime.

Then $\exists g \in G$ s.t. $\text{ord}(g) = p$. ($\bigcup p \mid |G|)$

Pr: Let $X = \{ (g_1, \ldots, g_p) \in G^p : g_1 g_2 \cdots g_p = 1 \}$

$\bigcirc$ $|X| = |G|^{p-1}$.

Why? Once $g_1, \ldots, g_{p-1}$ are chosen, this uniquely defines $g_p$, i.e.,

$g_p = (g_1 \cdots g_{p-1})^{-1} \in G$. Since there are $|G|^{p-1}$ choices for $g_1, \ldots, g_{p-1}$, it follows that $|X| = |G|^{p-1}$. 
2. \( \mathbb{Z}/p\mathbb{Z} \) acts on \( X \) by cyclically permuting entries.

Since \( p \mid |G| \Rightarrow |X| = |G|^p \), we have \( p \mid |X| \). Hence, we get an action of \( \mathbb{Z}/p\mathbb{Z} \) on \( X \) by cyclic permutation, i.e.

\[ k \in \mathbb{Z}/p\mathbb{Z} \text{ acts on } X \text{ by } k \mapsto \text{shift right } k \text{ places} \]

\[ k \cdot (g_1, \ldots, g_p) = (g_{k+1}, \ldots, g_p, g_1, \ldots, g_{p-k}) \]

Shift every thing right \( k \) places.

\( 0 \cdot (g_1, \ldots, g_p) = (g_2, \ldots, g_p) \quad (k \cdot (\ldots) = (k+1) \cdot (\ldots)) \Rightarrow \text{Group action!} \)
3. Use Orbit-Stabilizer fact that orbits partition $X$.

$\exists \Theta_1, \ldots, \Theta_r \ni x. \Theta_i \neq \Theta_j$ for some $x_i \in X, \Theta_i \cap \Theta_j = \emptyset$

for $i \neq j, i, j \in \{1, \ldots, r\}, \bigcup_{i=1}^{r} \Theta_i = X$. Take cardinalities, we get

$\left| X \right| = \sum_{i=1}^{r} \left| \Theta_i \right|$. By orbit-stabilizer, since $\mathbb{Z}/p\mathbb{Z}$ acts

on $X$, \( p = \left| \mathbb{Z}/p\mathbb{Z} \right| = 1 \left| \Theta_i \right| \left| \text{Stab}(x_i) \right| \Rightarrow \left| \Theta_i \right| = 1, p \). So

suppose $\Theta_1, \ldots, \Theta_r$ are of size $p$, \( \Theta_{r+1}, \ldots, \Theta_r \) are of

size 1.
\[ |X| = \sum_{i=1}^{r} 1^{|O_i|} = \sum_{i=1}^{n} 1^{|O_i|} + \sum_{i=n+1}^{r} 1^{|O_i|} \]

There must be at least one orbit \( O \) of size 1, i.e.

\[ O \equiv \sum_{i=1}^{n} O + \sum_{i=n+1}^{r} 1^{|O_i|} \pmod{p} \]

\[ \neq 0 \]

\[ \Rightarrow \exists \text{ another orbit } O_x \text{ of size 1.} \]

\[ \Rightarrow x = (g, \ldots, g) \text{ for some } g \in G \] but \( x \in X \) so \( g^p = 1 \), i.e. \( g \) has order \( p \).
Discussion 5

Q: \[ \text{If } K \subseteq I \subseteq R, \text{ then} \]

\[ \frac{R}{K} \twoheadrightarrow \frac{R}{I} \quad (\twoheadrightarrow = \text{Surjection}) \]

\[ \text{Examples of } | \mathcal{O}_{\sqrt{p}} / I | \]

\[ \wedge \text{algebraic number theory} \]
Suppose $R$ is a (comm) ring, $I \subseteq R$ is an ideal, and $K \leq I$ is an additive subgroup. Prove that $R/K$ surjects onto $R/I$.

(Indeed, this shows that to show $Q_{\text{fd}}/I$ is finite for non-zero ideal $I$, it suffices to find $K$ (additive subgroup of $I$) and show that $Q_{\text{fd}}/K$ is finite. Here, we take $K = I/I$)

Proof: We check 2 things: 1) An map $R/K \to R/I$ (well-defined)

2) The map is surjective
To show the 1st things, we'll show something more general: Let $\Psi : R \to S$ (R, S - rings) be a homomorphism of rings & suppose $K \subseteq \text{Ker}(\Psi)$ is an additive subgroup. Then $\exists \overline{\Psi} : R/K \to S$.

Claim: $\exists \overline{\Psi} : R/K \to S$.

Proof of claim: For $r + K \in R/K$, define $\overline{\Psi} : R/K \to S$ by $\overline{\Psi}(r + K) := \Psi(r)$. i.e. if $r_1 + K = r_2 + K$

We have to show its well-defined:
Need to show \( \overline{\varphi} \) is well-defined: if \( r_1 + k = r_2 + k \), then \( \overline{\varphi}(r_1 + k) = \overline{\varphi}(r_2 + k) \).

So \( r_1 + k = r_2 + k \Rightarrow \exists k_2 \in K \) s.t.
\[
\begin{align*}
r_1 &= r_2 + k_2 \text{ as elements of } R.
\end{align*}
\]

\[
\Rightarrow \overline{\varphi}(r_1 + k) = \overline{\varphi}((r_2 + k_2) + k) = \overline{\varphi}(r_2 + k_2)
\]
\[
= \varphi(r_2) + \varphi(k_2) = \varphi(r_2) = \overline{\varphi}(r_2 + k).
\]

(Since \( k_2 \in K \leq \text{ker}(\varphi) \))
Let $S = \mathbb{R}/I$ and $\varphi = \pi : \mathbb{R} \to \mathbb{R}/I$ be the canonical projection. So $\ker(\pi) = I$ and $K \subseteq I \implies \exists \pi : \mathbb{R}/K \to \mathbb{R}/I$.

(2) Showing $\tilde{\pi} : \mathbb{R}/K \to \mathbb{R}/I$ is surjective. This is true because for $r + I \in \mathbb{R}/I$, consider $\tilde{r} + K \in \mathbb{R}/K$. Well $\tilde{r} + K \to r + I \in \mathbb{R}$.

$\tilde{\pi}(r + K) = \pi(\tilde{r}) = r + I \implies \tilde{\pi}$ is surjective.
Ex: If \( R/I \) is finite, then the number of ideals in \( R \) containing \( I \) is finite.

\[ \begin{align*}
\text{Pr: } & \text{This is a direct consequence of the} \\
& \text{correspondence theorem: } \exists \text{ bijection between} \\
\{ \text{Ideals } J \subseteq R \text{ s.t.} I \subseteq J \} & \leftrightarrow & \{ \text{Ideals in } R/I \} \\
J & \mapsto & \pi_\mathcal{C}(J) = \{ \pi_\mathcal{C}(j) : j \in J \} \\
& = \{ r + I \in R/I : \exists j \in J \text{ s.t. } r + I = \pi_\mathcal{C}(j) \} \\
\pi_\mathcal{C}^{-1}(L) & = \{ r \in R : \pi_\mathcal{C}(r) \in L \} & \leftrightarrow & L \subseteq R/I
\end{align*} \]
Since $R/I$ is finite, it contains finitely many ideals, hence there are only finitely many ideals in $R$ containing $I$.

This idea of using the correspondence theorem is instrumental in all parts of algebra. It holds for groups w.r.t. subgroups, rings w.r.t. ideals, and in general to modules w.r.t. submodules.
Example of computing $|O_{\sqrt{-5}}/I|$.

Consider $O_{\sqrt{-5}}$ and $I = (2 \sqrt{-5})$.

Since $-5 \equiv 3 \pmod{4}$, we have

$$O_{\sqrt{-5}} = \mathbb{L}(1,\sqrt{-5}) = \left\{ a + b \sqrt{-5} : a, b \in \mathbb{Z} \right\}$$

$$= \left\{ a + b \sqrt{5} i : a, b \in \mathbb{Z} \right\}$$

$\Rightarrow$ $I = \mathbb{L}(\alpha, \beta)$, for some $\alpha, \beta \in \mathbb{R}$.
Well, $2\sqrt{5} \in \mathbb{I} \Rightarrow (2\sqrt{5})(-\sqrt{5}) = -10 \in \mathbb{I}$

$\Rightarrow 10 \in \mathbb{I}$, & 10 is the smallest integer

$\mathbb{N}$, $10 \in \mathbb{I}$. $\Rightarrow \mathbb{I} = \mathbb{L}$

$(6,3\sqrt{5}) \Rightarrow (6,2\sqrt{5} + \sqrt{5}) \equiv (6,\sqrt{5})$ in $\mathbb{Q}[\sqrt{5}]/\mathbb{I}$

Parallellogram

w/ vertices

$0, \alpha, \beta, \alpha + \beta$
What this shows is

\[ 10 \sqrt{5} / |I| = \# \text{ of lattice points} \]

in the parallelogram with vertices 0, \( \alpha \), \( \beta \), \( \alpha + \beta \) \&

not including the top \&

right edge.

\[ = 20. \]
In class, it was shown $\mathbb{Q}_{\sqrt{-5}}/\mathbb{Z}$ is finite by showing $\mathbb{Q}_{\sqrt{-5}}/\mathbb{I}$ is finite.

Is this surjects onto $\mathbb{Q}_{\sqrt{-5}}/\mathbb{I}$. What is $|\mathbb{O}_{\sqrt{-5}}/\mathbb{I}|$?

$I = (10, 2\sqrt{-5}, \bar{I} = (10, -2\sqrt{-5})$

$n = gcd(\alpha \bar{\beta}, \beta \bar{\alpha}, \alpha \beta + \bar{\alpha} \bar{\beta}) = (100, 20, 0) = 20$

$n = (100, 20, \sqrt{-5}, -\sqrt{-5}, 20) = (n) = (20)$
\[ \mathbb{Q} \sqrt{-5} / \mathbb{Z} = \{ a + b \sqrt{-5} : a, b \in \mathbb{Z}/20\mathbb{Z} \} \]

\[(20) \]

\[ |\mathbb{Q} \sqrt{-5} / \mathbb{Z}| = \left| \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \right| = 20 \cdot 20 = 400. \]

\[ |\mathbb{Q} \sqrt{-5} / \mathbb{Z}| = 20 \]
Discussion 6 5/7

Q: Examples of calculations for minimal polys → Field Theory
In class yesterday, it was shown that if $\alpha \in \beta$ are algebraic over $\mathbb{F}$, then 

$\alpha + \beta, \alpha \cdot \beta, \alpha / \beta$ ($\beta \neq 0$)

are also algebraic over $\mathbb{F}$. In general, finding minimal poly of $\alpha + \beta, \alpha \beta, \alpha / \beta$

is quite difficult. ($\alpha$ algebraic iff $\exists \mathbb{F}(\alpha): \mathbb{F}(\alpha) < \infty$)
Ex: Let $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$. Then $\alpha \neq \beta$ are algebraic over $\mathbb{Q}$ ($\mathbb{P}_{\sqrt{2}}(x) = x^2 - 2$, $\mathbb{P}_{\sqrt{3}}(x) = x^2 - 3$).

What is $\mathbb{P}_{\alpha + \beta}(x) = \mathbb{P}_{\sqrt{2} + \sqrt{3}}(x)$ over $\mathbb{Q}$?

1. $\mathbb{P}_{\alpha + \beta}(x) = \mathbb{P}_{\sqrt{2} + \sqrt{3}}(x)$ over $\mathbb{Q}$?

2. $\mathbb{P}_{\alpha \beta}(x) = \mathbb{P}_{\sqrt{2} \cdot \sqrt{3}}(x) = \mathbb{P}_{\sqrt{6}}(x)$ over $\mathbb{Q}$?

Sol: 2 is easier, so let's look at it first. We have $\mathbb{P}_{\sqrt{6}}(x) = x^2 - 6 = (x - \sqrt{6})(x + \sqrt{6})$ is irreducible over $\mathbb{Q}$ (HW5: $ax^2 + bx + c$ irr $\iff b^2 \leq 4ac$)
Therefore, \( P_{\sqrt{6}}(x) = x^2 - 6 \) is the minimal poly for \( \alpha \cdot \beta = \sqrt{6} \).

\[ N(x) \]

\( \overline{\alpha} \): We've seen that \( \mathbb{C} \), then \( \overline{\mathbb{C}} \) is.
In general, if \( \alpha \) is of degree 2 over \( \mathbb{C} \), then \( \alpha \overline{\alpha} \in \mathbb{C} \). To study the minimal poly of \( \alpha + \beta \), we need to know about \( \alpha \) & \( \beta \)'s conjugates, i.e. other roots of their minimal polys.
Namely, we have for \( \alpha = \sqrt{2} \), let

\[ \overline{\alpha} = -\sqrt{2} \quad (\text{this is b/c the other root of } P_{\sqrt{2}}(x) = x^2 - 2 \text{ is } -\sqrt{2}. \quad \text{Similarly}, \]

\[ = (x - \sqrt{2})(x + \sqrt{2}) \]

define \( \beta = -\sqrt{3} \) (for same reason). Now let's consider the following numbers, \( \alpha, \omega, \beta \).

\[ \alpha + \beta, \overline{\alpha} + \beta, \alpha + \overline{\beta}, \overline{\alpha} + \overline{\beta} \quad \text{All possible numbers obtained by conjugating} \]
Consider $f(x) = (x - (\alpha + \beta))(x - (\overline{\alpha} + \beta))(x - (\alpha - \beta))(x - (\overline{\alpha} + \beta))$

\* Note: $\overline{\alpha} = -\alpha$, $\overline{\beta} = -\beta$. $(x-y)(x+y) = x^2 - y^2$

\[= (x - (\alpha + \beta))(x + (\alpha + \beta))(x - (\alpha - \beta))(x + (\alpha - \beta))\]

\[= \left(x^2 - (\alpha + \beta)/\alpha \right)^2 \left(x^2 - (\alpha - \beta)/\alpha \right)^2\]

\[= x^4 - (\alpha + \beta)^2(x^2 + \alpha - \beta)^2 \in \Omega[x]\]
\[ \begin{align*}
&= X^4 - \left( (\alpha + \beta)^2 + (\alpha - \beta)^2 \right) X^2 + (\alpha + \beta)^2 (\alpha - \beta)^2 \\
&= X^4 - \left( \alpha^2 + 2\alpha \beta + \beta^2 + \alpha^2 - 2\alpha \beta + \beta^2 \right) X^2 + (\alpha^2 - \beta^2)^2 \\
&= X^4 - (2\alpha^2 + 2\beta^2) X^2 + (\alpha^2 - \beta^2)^2 \\
&= \left( \alpha = \sqrt{2} \right) \quad \beta = \sqrt{3} \\
&= X^4 - 2 (2+3) X^2 + (2-3)^2 \\
&= X^4 - 10X^2 + 1 = f(x) \in \mathbb{Q}[x] \\
\Rightarrow \quad f(x) &= \frac{P}{\sqrt{2} + \sqrt{3}} = X^4 - 10X^2 + 1 \text{ is minimal poly for } \sqrt{2} + \sqrt{3}.\end{align*} \]
We see here
\[ \deg(P_{x+\beta}(x)) > \deg(P_x(x)), \deg(P_{\beta}(x)) \]

However \[ \deg(P_{x+\beta}(x)) = \deg(P_x(x)), \deg(P_{\beta}(x)) \]

but in general, we need not have equality here. Arithmetic surrounding minimal polynomials is complicated but doable.
Ex: You are given that $\pi$ and $e$ are transcendental over $\mathbb{Q}$ (i.e. not algebraic, so not a root of a finite degree poly w/ coefficients in $\mathbb{Q}$). Assuming this transcendence, prove that at most one of $e+\pi$ or $e\pi$ is rational.

Pt: Assume $e+\pi$ and $e\pi$ are rational. Consider

$$f(x) = (x-e)(x-\pi) = x^2 - (e+\pi)x + e\pi \in \mathbb{Q}[x]$$
However, $f(e) = f(\pi) = 0 \Rightarrow \deg(f) = 2 < \infty$. This means that $e$ and $\pi$ are algebraic, but this contradicts the transcendence of both $e$ and $\pi$. Hence, not both $e$ and $e + \pi$ are rational (i.e., at least one is irrational).
Ex: We want to show
\[ \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) \]

\[ \{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q} \} \]

has basis \( \{ 1, \sqrt{2}, \sqrt{3}, \sqrt{6} \} \).

Sol: To show these fields are the same, we'll show "\( \subseteq \)" and "\( \supseteq \)". \( \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \).

"\( \supseteq \)" Since \( \sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \), \( \Rightarrow \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \).
"≤"  We want to show \( \sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3}) \).

Since \((\sqrt{2}+\sqrt{3}) \in \mathbb{Q}(\sqrt{2}+\sqrt{3})\), so is \((\sqrt{2}+\sqrt{3})^2 = 2 + \sqrt{6} + 3 \Rightarrow \sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})

\[ \sqrt{6} (\sqrt{2} + \sqrt{3}) = 2\sqrt{3} + 3\sqrt{2} = \sqrt{2} \]

\[-2(\sqrt{2}+\sqrt{3}) = -2(\sqrt{2}+\sqrt{3}) \]

\[ \sqrt{2} = \sqrt{6} (\sqrt{2} + \sqrt{3}) - 2 (\sqrt{2}+\sqrt{3}) \in \mathbb{Q}(\sqrt{2}+\sqrt{3}) \]

\[ \sqrt{3} = 3 (\sqrt{2} + \sqrt{3}) - \sqrt{6} (\sqrt{2}+\sqrt{3}) \in \mathbb{Q}(\sqrt{2}+\sqrt{3}) \]

\[ = 3\sqrt{2} + 3\sqrt{3} - 3\sqrt{2} - 2\sqrt{3} \]

\[ \Rightarrow \mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3}) \Rightarrow \text{Equality!} \]
Discussion 7  5/14

Q: \[ \rightarrow \text{Simplified version of primitive element thm:} \]

\[ \alpha, \beta \text{ algebraic } \implies [\mathbb{K}(\beta) : \mathbb{K}] = 2 \]

\[ \implies \mathbb{K}(\alpha, \beta) = \mathbb{K}(\alpha + c\beta) \text{ for some } c \in \mathbb{K} \]

\[ \rightarrow \text{Example w/ constructibility} \]
In class yesterday, it was mentioned that for the poly \( f(x) = x^3 - 2 \), adjoining \( 3\sqrt{2} \) to \( \mathbb{Q} \) is not enough to get the splitting field for \( f \) (namely, you also need one more root, just take \( \sqrt[4]{3} \) (this is b/c other roots are \( 3\sqrt{2} \pm \sqrt{3}, \frac{3\sqrt{2}}{2} \pm \frac{3\sqrt{3}}{2} \) when \( \mathbb{Z}_3 = e^{\frac{2\pi i}{3}}, z_3 = \frac{-1}{2} + i\frac{\sqrt{3}}{2} \)).
Last section, we showed

\[ \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) , \]

which shows \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) is a simple extension (generated by a single element).

We'll show we can do the same w/ \( \mathbb{Q}(\sqrt{2}, i\sqrt{3}) \) (i.e. its generated by a single element).
Prop: Let \( \alpha, \beta \) be algebraic over \( \mathbb{Q} \).

Assume \( [\mathbb{Q}(\beta):\mathbb{Q}] = 2 \). Then \( \exists c \in \mathbb{Q} \) such that \( \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + c\beta) \).

[In comparison to \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}), c = 1 \)]

Pf: We have \( \mathbb{Q}(\alpha + c\beta) \subseteq \mathbb{Q}(\alpha, \beta) \) from definition. We want to show other inclusion. Let \( f(x) \) and \( g(x) \) be the minimal polynomials of \( \alpha \) and \( \beta \) respectively, over \( \mathbb{Q} \).
Then we have

\[ x_1, \ldots, x_n \text{ are roots of } f(x) \]

\[ \beta_1, \beta_2 \text{ are roots of } g(x) \]

Since \([\mathbb{A}(\beta): \mathbb{A}] = 2\), this implies \(\beta_1 \neq \beta_2\).
Now pick \(c \in \mathbb{A} \setminus \{0\}\) that is different from

\[(x - x_i)(\beta - \beta_2) \quad i = 2, \ldots, n\]
Consider the polynomial \( h(x) = f(\alpha + c\beta - c\xi) \in \mathbb{Q}(\alpha + c\beta)[x] \).

From this definition, we see

\[
\begin{align*}
\text{Want these properties:} & \\
\text{1.} & \quad h(\beta) = 0 \quad (h(\beta) = f(\alpha + c\beta - c\beta) = f(\alpha) = 0) \\
\text{2.} & \quad h(\beta_2) \neq 0 \quad (\text{how we chose our } c) \\
\end{align*}
\]

\[
f(\alpha + c\beta - c\beta_2) = f\left(\alpha + c(\beta - \beta_2)\right) \neq 0
\]
Since both $h(x)$ & $g(x)$ satisfy

$$h(\beta) = g(\beta) = 0,$$

the minimal poly of $\beta$ over $\mathbb{C}(\alpha+c\beta)$ divides $h(x)$ & $g(x)$. But not every root of $g(x)$ is a root of $h(x)$, hence the minimal poly of $\beta$ over $\mathbb{C}(\alpha+c\beta)$ has degree 1, so $\beta \in \mathbb{C}(\alpha+c\beta)$. Thus $\alpha = \alpha+c\beta-c\beta \in \mathbb{C}(\alpha+c\beta)$. The fields are equal.
Remark: The proof is good to show us why the field extensions are equal but doesn't necessarily provide good means for calculating a good $c$ which makes this work easier.

In fact \( \text{Cl}(\alpha, \beta) = \text{Cl}(\alpha + c \beta) \)

for any \( c \in \mathbb{C} \setminus \{0\} \), \((\alpha - \alpha_i)(\beta - \beta_i)\) for \( i = 2, \ldots, n \).
Ex: If \( \alpha = \sqrt[3]{2} \), \( \beta = i\sqrt{3} \) (\( p_{i\sqrt{3}}(x) = x^2 + 3 \)),

the number \( c = 1 \) should work, i.e.,

\[ \text{Cl}(\sqrt[3]{2}, i\sqrt{3}) = \text{Cl}(\sqrt[3]{2} + i\sqrt{3}) \]

However, showing directly is a lot of work by hand.
Ex: Is it possible to construct a square whose area is equal to that of a given triangle? (i.e., if I give you an equilateral triangle, can you give me a square that has the same area?)

Sol: Suppose that the side length is equal to 1. \[ h = \frac{\sqrt{3}}{2} \implies \text{Area} = 2 \cdot \frac{1}{2} \cdot \frac{\sqrt{3}}{2} \cdot \frac{1}{2} = \frac{\sqrt{3}}{4} \]
The area is \( \frac{\sqrt{3}}{4} \), so for a square to have area \( \frac{\sqrt{3}}{4} \) it must have side length \( \sqrt{\frac{\sqrt{3}}{4}} \). Since \( \sqrt{\frac{\sqrt{3}}{4}} \) is obtained by a sequence of square roots & field operations, it is constructible.

\[ \triangle \rightarrow \left\{ \cdot \right\} = \sqrt{\frac{\sqrt{3}}{4}} \]
Ex: The measure of a given angle is $\frac{180^\circ}{n}$, where $n$ is not divisible by 3. Prove that the angle can be trisected by straightedge and compass.

Pf: We want to show $\frac{60}{n}$ is constructible. Showing $3|n$ is the same as saying $\gcd(n, 3) = 1$. So $\exists s, t \in \mathbb{Z}$ s.t. $s \cdot n + t \cdot 3 = 1$. 
So we have integers $s$ and $t$ with

$$s \cdot n + t \cdot 3 = 1.$$ 

Multiply both sides by $\frac{60}{n}$

$$\Rightarrow s \cdot 60 + t \cdot \frac{180}{n} = \frac{60}{n}$$

$\mathbb{Z}$ constructible $\mathbb{Z}$ given

$$\Rightarrow \frac{60}{n} \text{ is constructible as it is sum of } \frac{1}{4} \text{ multiples of constructible angles.}$$
Ex: We've shown \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) \).

We can also show \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} - \sqrt{3}) \) by showing:

\[
(\sqrt{2} - \sqrt{3})^2 = 2 - 2\sqrt{6} + 3 \Rightarrow \sqrt{6} \in \mathbb{Q}(\sqrt{2} - \sqrt{3})
\]

\[
\sqrt{6}(\sqrt{2} - \sqrt{3}) = 3\sqrt{2} - 2\sqrt{3} = \sqrt{2} \in \mathbb{Q}(\sqrt{2} - \sqrt{3})
\]

\[-2(\sqrt{2} - \sqrt{3}) = -2(\sqrt{2} - \sqrt{3})
\]

\[\text{1. Is it is obvious } \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2} - \sqrt{3})? \quad \text{Y}
\]

\[\text{2. Is it is obvious } \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \frac{1}{2} \sqrt{3})? \quad \text{N}
\]
1. The reason $\text{Cl}(\sqrt{2} + \sqrt{3}) = \text{Cl}(\sqrt{2} - \sqrt{3})$ is $\text{Cl}(\sqrt{2} + \sqrt{3}) = \text{Cl}(\sqrt{2} + \sqrt{3}) = \text{Cl}[x] \setminus \frac{p_{\sqrt{2} + \sqrt{3}}(x)}{p_{\sqrt{2} + \sqrt{3}}(x)} = (\star)$.

3. $p_{\sqrt{2} + \sqrt{3}}(x) = x^4 - 10x + 1$ has $\sqrt{2} - \sqrt{3}$ as another root, $p_{\sqrt{2} + \sqrt{3}}(x) = p_{\sqrt{2} - \sqrt{3}}(x)$.

$(\star) = \text{Cl}[x] \setminus \frac{p_{\sqrt{2} + \sqrt{3}}(x)}{p_{\sqrt{2} + \sqrt{3}}(x)} = \text{Cl}(\sqrt{2} - \sqrt{3})$. 
Discussion 8

Q: Go over $\text{Gal}(\mathbb{Q}(\sqrt[3]{p})/\mathbb{Q})$

$\cong \mathbb{F}_p^\times$ $G(\mathbb{Q}(\sqrt[3]{p})/\mathbb{Q})$ (p prime)

→ Results on extensions

→ Irreducibility of $x^p - x + \alpha$ for $\alpha \neq 0$ in $\mathbb{F}_p$
Let $\zeta_p$ be a primitive $p$th root of unity, $p$ prime ($\zeta_p = e^{2\pi i/p}$). Show

$$G(Q(\zeta_p)/Q) = \mathbb{F}_p^*.$$ 

**Sol:** We have the following lemma:

**Lem:** If $\alpha$ and $\alpha'$ are roots of the same irreducible polynomial $f \in \mathbb{F}[x]$, then there exists a unique isomorphism $\phi: \mathbb{F}[^*x] \rightarrow \mathbb{F}[\alpha']$ such that $\phi(r) = r \quad \forall r \in \mathbb{F}$ and $\phi(\alpha) = \alpha'$. 

1. $\phi(r) = r \quad \forall r \in \mathbb{F}$ 
2. $\phi(\alpha) = \alpha'$
For \( \zeta_p = \text{primitive } p\text{th root of unity}, \) it and all its powers are roots of \( x^{p-1}. \) Roots of \( x^{p-1} \) are \( 1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}. \) However, this is not irreducible. But

\[
\Phi_p(x) = p\text{th cyclotomic} = \frac{x^{p-1} - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1
\]

is irreducible w/ roots \( \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}. \)

I from HW
Since $p$ is prime, $\mathbb{C}_p(\mathbb{F}_p) = \mathbb{C}_p(\mathbb{F}_p^j)$ for any $j = 1, 2, \ldots, p-1$. (Reason: look at bases as vector spaces over $\mathbb{C}_p$, i.e., $\{1, \mathbb{F}_p, \mathbb{F}_p^2, \ldots, \mathbb{F}_p^{p-1}\}$ is a basis for both). The lemma says that for any $j \in \{1, \ldots, p-1\}$ there exists a bijection $\phi_j : \mathbb{C}_p(\mathbb{F}_p) \rightarrow \mathbb{C}_p(\mathbb{F}_p^j)$ such that $\phi_j(\mathbb{F}_p) = \mathbb{F}_p^j$.

Want to know how to multiply $\phi_j$'s.

concatenation
For $j, j' \in \{1, \ldots, p-1\}$, we have

\[ \psi_j \circ \psi_{j'} (\mathcal{S}_p) = \psi_j (\mathcal{S}_p \circ \mathcal{S}_p \cdots \mathcal{S}_p) = \psi_j (\mathcal{S}_p)^{j'} \]

\[ \mathcal{S}_p \circ \mathcal{S}_p \cdots \mathcal{S}_p = (\mathcal{S}_p)^{j'} \]

\[ j' \text{ times} = \mathcal{S}_p^{j'} \]

\[ = \psi_{jj'} (\mathcal{S}_p) \]

\[ \Rightarrow \psi_j \circ \psi_{j'} = \psi_{jj'} \text{ \hspace{1cm} Multiplication of maps ($\psi_j$'s) is same as multiplying the indices} \]
Multiplication in $G(\mathcal{O}(\mathbb{F}_p)/\mathcal{O})$ is same as in $\mathbb{F}_p^\times$. Also, they both are of size $p-1$. Hence

$$G(\mathcal{O}(\mathbb{F}_p)/\mathcal{O}) \cong \mathbb{F}_p^\times$$

Details of isomorphism:

$$\varphi_j \mapsto j$$

$$\{ \varphi_j \mapsto j \}$$
Ex: Let \( p = 5 \). \( \zeta_5 = 5^{th} \) root of unity.

Its minimal poly is \( X^4 + X^3 + X^2 + X + 1 \), which has roots \( \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4 \). Define \( \varphi_j \in G(\zeta_5) \) by \( \varphi_j(\zeta_5) = \zeta_5^j \), \( j = 1, 2, 3, 4 \).

\( \varphi_j(1) = 1 \) for \( r \in \mathbb{C} \).

\[
\begin{align*}
\varphi_1(\zeta_5) &= \zeta_5 \\
\varphi_2(\zeta_5) &= \zeta_5^2 \\
\varphi_3(\zeta_5) &= \zeta_5^3 \\
\varphi_4(\zeta_5) &= \zeta_5^4 = \zeta_5
\end{align*}
\]

Note: \( 4 \cdot 2 \equiv 3 \pmod{5} \).
Consider $\varphi_4 \circ \varphi_3 (S_5) =^\sim \varphi_4 (S_5^3) = \varphi_2 (S_5^3) = \varphi_2 (S_5) = ^\uparrow$

$\therefore 4 \cdot 3 = 12 \equiv 2 \pmod{5}$

Takeaway: $G(\varphi_2(S_5))/\langle \varphi_2 \rangle \cong \mathbb{F}_5^\times \leftarrow \text{cyclic of order } 5-1 = 4 \cong \mathbb{Z}/4\mathbb{Z}$. 
Ex: What if \( p \) isn't prime?

Let \( p=4, \ Z_4 = 4^{th} \) root of unity

\[ \Rightarrow i \]

Note though that minimal poly of \( i \) over \( \mathbb{Q} \) is \( x^2+1 \), so \( \exists \! \! \! \exists i : \mathbb{Q}(i) \to \mathbb{Q}(i) \)

\( \therefore \) this is the only non-trivial map in \( G(\mathbb{Q}(i)/\mathbb{Q}) \), namely, \( \varphi(a+bi) = a-bi = a+bi \)
So \( \left| G(\mathcal{O}(i)/\mathcal{O}) \right| = 2 \neq 3 = |\text{GF}_4^x| \).

\( \Rightarrow \ G(\mathcal{O}(\mathfrak{b}_4)/\mathcal{O}) \neq \text{GF}_4^x \).  

Very Geometric  

(look at last slides)

Takeaway: For non-primes \( n \), we have

\[ G(\mathcal{O}(\mathfrak{b}_n)/\mathcal{O}) \neq \text{GF}_n^x \]  

this doesn't even make sense for \( n \) not a prime power.
Goal is to prove the following:

**Lem:** Let $H \leq \text{Aut}(IK)$ be finite and $F = IK^H = \text{Fix}(H) = \{ \alpha \in IK : \varphi(\alpha) = \alpha \ \forall \varphi \in H \}$. Then

$$[IK : IF] = [IK : IK^H] < \infty.$$  

(In fact, $[IK : IK^H] = |H|$ ← to be shown tomorrow)

We'll break this into 2 parts.
Lemma 1: If $K$ is an algebraic extension of $F$ satisfying $[K:F] = \infty$, for every $n > 0$ there exists $\alpha \in K$ such that $[F(\alpha) : F] > n$. (Has elements of unbounded order)

Proof: Let $n \in \mathbb{Z}_{\geq 0}$ be fixed. Since $[K:F] = \infty$, there exists $\alpha_1 \in K \setminus F$. If $[F(\alpha_1) : F] > n$, we're done. Otherwise, since $[F(\alpha_1) : F] < \infty$, there exists $\alpha_2 \in K \setminus F(\alpha_1)$. Then $[F(\alpha_1, \alpha_2) : F(\alpha_1)] > 1 \implies [F(\alpha_1, \alpha_2) : F] < \infty$.

By the primitive element thm, since $[F(\alpha_1, \alpha_2) : F] < \infty$...
\[ \exists \alpha_3 \in \text{F}(\alpha_1, \alpha_2) \setminus \alpha_1, \quad \text{F}(\alpha_1, \alpha_2) = \text{F}(\alpha_3). \]

If \([\text{F}(\alpha_3) : \text{F}] > n\), we're done. Otherwise, continue this procedure. Idea is that with each \( \alpha_i \) adjoined, the degree of the extension strictly increases. So eventually (after finitely many steps) we have \( \alpha_k \) such that

\[ [\text{F}(\alpha_k) : \text{F}] > n. \]
Lemma 2: If $K$ is an algebraic extension of $K^H$, then $[K^H(\alpha):K^H]$ divides $|H|$ for $\alpha \in K$.

(w/o proof/look in rec. notes 5/20)

Proof of Lemma: Suppose for sake of contradiction that $[K:K^H] = \infty$. Then $\forall n \in \mathbb{Z}_{>0}, \exists \alpha \in H, [K^H(\alpha):K^H] > n$ (from Lem 0). However, by Lem 0 we have that $\forall \alpha \in K$, $[K^H(\alpha):K] \mid |H|$. If we take $n > |H|$, $\exists \alpha \in K$ s.t.

$[K^H(\alpha):K^H] > n > |H| \iff [K^H(\alpha):K^H] \mid |H|$. \qed
Q: $\rightarrow$ Fundamental Theorem of Galois Theory (FTGT)

$\rightarrow$ Example of FTGT at play
Thm (Fundamental Theorem of Galois Theory, FTGT) (also called the Galois correspondence)

Let $K/F$ be a Galois extension, i.e. $G = G(K/F)$.

Then there is a bijection

$$
\left\{ \text{Subfields } E \text{ of } K \text{ containing } F \right\} \leftrightarrow \left\{ \text{Subgroups } H \text{ of } G \right\}
$$

$$
K^H \leftrightarrow H \quad G(K/F) \downarrow \quad \text{such that } \quad a \in G : a(E) = E
$$
Under this correspondence,

1. (inclusion reversing) If \( E_1 \), \( E_2 \) correspond to \( H_1 \), \( H_2 \) respectively, then \( E_1 \leq E_2 \) if and only if \( H_1 \supseteq H_2 \).

2. \([K:E] = |H|\) \& \( |E:F| = [G:H] \leftarrow \text{index of } H \text{ in } G\).

\([G:H]\) is the size of \( G/H \), or its the # of right (or left) cosets of \( H \) in \( G \).

\(1K/E\) is always Galois w/ \( G(1K/E) \cong H \subseteq E\).
4. \( E/F \) is Galois if H is normal in G.

If this is the case, then

\[
G(E/F) \cong G/H
\]

\[
\text{If } \frac{|E|}{|G:H|} = |G/H|.
\]

**Moral of the story:**

The problem of studying intermediate fields of a Galois extension is the same as studying subgroups of the Galois group.

* This correspondence gives uniqueness properties:
  - If \( H \) fixes \( E \), then \( |E| = |KH| \).
Ex.: Let $L = \text{splitting field of } x^4 - 2 \text{ over } \mathbb{Q}$, so $F = \mathbb{C}$. Find all intermediate fields $\mathbb{Q} \subset E \subset \mathbb{C}$ draw lattice diagram (field inclusions).

First, $x^4 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 2$. Let $\alpha = \sqrt[4]{2}$ be the positive real root of $x^4 - 2$. Then all roots are $\alpha, \alpha \sqrt[4]{2}, \alpha^2, \alpha^3, \alpha^4$. But $\mathbb{Z}_4 = \text{primitive } 4\text{th root of unity} = i \ (i^2 = -1 \Rightarrow i^4 = 1)$.

$\Rightarrow$ All roots are $\frac{\alpha}{4}, i\alpha, -\alpha, -i\alpha$. Some are in $\mathbb{Q}$. 


$K$ must contain $i$ as $i = \frac{\alpha_i}{\alpha} \in K$, hence $K$ is not real. Since $\alpha \in \mathbb{R}$, $\mathbb{C}(\alpha) \subseteq K$ (want $\mathbb{C}(\alpha) \neq K$). Let $E = \mathbb{C}(\alpha)$, which has basis $B=\{1, \alpha, \alpha^2, \alpha^3\}$ over $\mathbb{C}$; since $\alpha^2 + 1$ is irreducible over $\mathbb{C}(\alpha)$, $E$ has $i$ as a root, it is its minimal poly. Namely, $\mathbb{C}(\alpha, i)$ is degree 2 over $E$ w/ basis $\{1, i\}$. So $K = \mathbb{C}(\alpha, i)$, w/ basis $\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$ over $\mathbb{C}$.
\[ [L: \mathbb{Q}] = 8 \] Since \( L/K \) is Galois (\( L \) is a splitting field), we know \( |\text{Gal}(L/K)| = 8 \).

So we have to find 8 automorphisms of \( L = \mathbb{Q}(\alpha, i) \) which fix \( \mathbb{Q} \).

\[ [L: \mathbb{Q}] = [\mathbb{Q}(\alpha, i): \mathbb{Q}] = [\mathbb{Q}(\alpha, i): \mathbb{Q}(i)] \cdot [\mathbb{Q}(i): \mathbb{Q}] \]
\[ = 2 \cdot 4 \]

Since \( \{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\} \) are a basis for \( L/K \), any \( \sigma \in \text{Gal}(L/K) \) is defined by its action on sums of \( \alpha \) and \( i \). Since automorphisms break up over products
To \( \sigma \in G(\mathbb{K}/\mathbb{F}) \) is defined by \( \sigma(x), \sigma(i) \). Any automorphism must send \( x \) to another root of its minimal poly.

Define \( \sigma, \tau \in G(\mathbb{K}/\mathbb{F}) \) by

\[
\sigma : \begin{cases}
\alpha \mapsto i\alpha \\
i \mapsto i
\end{cases} \\
\tau : \begin{cases}
\alpha \mapsto \alpha \\
i \mapsto -i
\end{cases}
\]

\[
\sigma^2(x) = \sigma(i\alpha) = \sigma(i) \sigma(\alpha) = i(i\alpha) = -\alpha
\]

\[
\sigma^3(x) = \sigma(\sigma^2(\alpha)) = \sigma(-\alpha) = -i\alpha
\]

\[
\tau^2(x) = \tau(i\alpha) = \tau(i) \tau(\alpha) = i(-i\alpha) = -\alpha
\]

\[
\tau^3(x) = \tau(\tau^2(\alpha)) = \tau(-\alpha) = -i\alpha
\]

\[
\tau^4(x) = \tau(\tau^3(\alpha)) = \tau(-i\alpha) = \alpha
\]

\[
\sigma \tau \sigma^{-1} = \tau
\]
\[ \langle \sigma, \tau \rangle \geq 1 = \frac{\langle \sigma \rangle \langle \tau \rangle}{\langle \sigma \cap \tau \rangle} = \frac{4 \cdot 2}{1} = 8. \]

\[ |G(\mathbb{K}/\mathbb{F})| = 8 \Rightarrow G(\mathbb{K}/\mathbb{F}) = \langle \sigma, \tau | \sigma^2 = \tau^2 = 1, \sigma \tau \sigma^{-1} = \tau \rangle. \]

Other relations = commutation relation
b/w \( \sigma \) \& \( \tau \).

Let's look at \( \tau \sigma \tau^{-1} \) (conjugate \( \sigma \) by \( \tau \)). \( \tau^{-1} = \tau \).

\[ \tau \sigma \tau (\alpha) = \tau (\sigma (\alpha) = \tau (i \alpha) = i) \tau (\alpha) = -i \alpha \]

\[ \Rightarrow \tau \sigma \tau (i) = \tau (\sigma (-i) = \tau (-i) = i = \sigma^{-1} (i) \Rightarrow \tau \sigma \tau^{-1} = \sigma^{-1} \]

\[ \]
\[ G(1k/1F) = \langle \sigma, \tau | \sigma^4 = \tau^2 = 1, \sigma^2 = \tau \sigma \tau^{-1} = \sigma^{-1} \rangle \]

\[ \cong D_4 \]

I dihedral group on square

Symmetries of \( \square \)

Dihedral condition
In the book, we have lattice of subgroups of $D_4^2$:

$$D_4 = \langle \sigma, \tau \mid R \rangle$$

- $H_1 = \{ 1, \sigma^2, \tau, \sigma^2 \tau \}$
- $H_2 = \{ 1, \sigma, \sigma^2, \sigma^3 \}$
- $H_3 = \{ 1, \sigma^2, \sigma \tau, \sigma^3 \}$
- $H_4 = \{ 1, \tau \}$
- $H_5 = \{ 1, \sigma^2 \}$
- $H_6 = \{ 1, \sigma^2 \}$
- $H_7 = \{ 1, \sigma \}$
- $H_8 = \{ 1, \sigma^2 \}$

- $\{ 1 \}$
This gives lattice of intermediate fields

\[ K_{H_1} = \mathbb{Q}(\alpha^2) \]
\[ K_{H_2} = \mathbb{Q}(i) \]
\[ K_{H_3} = \mathbb{Q}(i^2) \]
\[ K_{H_4} = \mathbb{Q}(\alpha i) \]
\[ K_{H_5} = \mathbb{Q}(i^2) \]
\[ K_{H_6} = \mathbb{Q}(\alpha, i) = K \]
Q: Find fixed fields corresponding to subgroups of $G(\mathbb{K}/\mathbb{H})$.

→ Class Equation
Ex. Consider $K = \text{splitting field of} \ X^4 - 2$ over $\mathbb{Q} = \mathbb{Q}(\alpha, i)$ for $\alpha = \sqrt[4]{2}$. We showed last time

$$G(\mathbb{Q}(\alpha, i)/\mathbb{Q}) \cong D_4$$

$\sigma_0 : \{ \begin{array}{c} \alpha \mapsto i\alpha \\ i \mapsto i \end{array} \}

\tau : \{ \begin{array}{c} \alpha \mapsto \alpha \\ i \mapsto -i \end{array} \}$
$D_4$ has the following lattice of subgroups:

$D_4 = \langle \sigma, \tau | 1 \rangle$

$[D_4 : H_i] = 2$

$H_1 = \{1, \sigma^2, \tau, \sigma^2 \tau \}$
$H_2 = \{1, \sigma, \sigma^2, \sigma^3 \}$
$H_3 = \{1, \sigma^2, \sigma \tau, \sigma^3 \tau \}$
$H_4 = \{1, \tau \}$
$H_5 = \{1, \sigma^2 \tau \}$
$H_6 = \{1, \sigma^2 \}$
$H_7 = \{1, \sigma \}$
$H_8 = \{1, \sigma^2 \}$
$H_2$: Since $[\mathbb{D}_4 : H_2] = 2$, $K^{H_2}$ is a degree 2 extension of $\Omega$. \[ [G:H] = [K^H:F] \]

fixed by $H_2 = \{1, \sigma, \sigma^2, \sigma^3\}$. Since $\sigma(i) = i$

$\Rightarrow \sigma^j(i) = i \forall j \in \{0, \ldots, 3\}$. So $i \in K^{H_2}$, $\Rightarrow$

$\Omega(i) \subseteq K^{H_2}$ but both are degree 2 extensions

$\Rightarrow |K^{H_2}| = \Omega(i)$
$H_6$. So $H_6 = \{1, \sigma^2\}$ and $[H_2 : H_6] = 2$, so

$\mathbb{Q}^{H_6}$ is a degree 2 extension over $\mathbb{Q}(i) = \mathbb{Q}^{H_2}$. We need to find what is fixed by

$\sigma^2$. Well, $\sigma^2(\alpha) = \sigma(i\alpha) = i^2 \alpha = -\alpha$

$\Rightarrow \sigma^2(\alpha^2) = \sigma^2(\alpha) \quad \sigma^2(\alpha) = (-\alpha)(-\alpha) = \alpha^2$

$\Rightarrow \sigma^2$ is identity fix $\alpha^2$. $\Rightarrow \mathbb{Q}^{H_6} = \mathbb{Q}(i, \alpha^2)$

$\mathbb{Q}(i)(\alpha^2) = \mathbb{Q}(\alpha^2, i)$

$P_{\alpha^2, (i)}(x) = x^2 - 2 \quad \text{b/c} \quad P(\alpha^2) = \alpha^4 - 2 = 0$
We know \( \tau(\alpha) = \alpha \) \( \in H_4 \) = \{1, \tau, \tau^2, \tau^3\}.

Also, by looking at sizes, we have \([D_4 : H_4] = 4\). Well \( \alpha \) is degree 4 over \( \mathbb{Q} \) fixed by \( H_4 \Rightarrow |K^{H_4}| = \mathbb{Q}(\alpha)\).
$H_i$: By inclusion & guessing, we'll see that $\Omega(\alpha^2) = |K^{H_i}|$ for $H_i = \{1, \sigma^2, \tau, \sigma^2 \tau\}$.

By previous work, we know $\sigma^2(\alpha^2) = \alpha^2$, $\tau(\alpha^2) = \alpha^2$, $\Rightarrow \sigma^2(\tau(\alpha^2)) = \sigma^2(\alpha^2) = \alpha^2$.

$\Rightarrow \alpha^2$ is fixed by $H_i$, i.e. $\alpha^2$ is degree 2 over $\Omega \left( \mathbb{P}_2, \alpha \right) = x^2 - 2$.

Since $H_i \leq H_1$, $\Rightarrow |K^{H_1}| = |K^{H_i}| = \Omega(\alpha^2)$. [Boxed]
H₅: For \( H₅ = \mathbb{Z}/3 \), we have

\[
\begin{align*}
\sigma^2(x) &= -\alpha, \quad \sigma^2(i) = i \leftrightarrow \sigma^2 \text{ gives } -1 \text{ to } \alpha \\
\tau(x) &= \alpha, \quad \tau(i) = -i \leftrightarrow \tau \text{ gives } -1 \text{ to } i
\end{align*}
\]

\[
\Rightarrow \quad \sigma^2 \tau(x i) = \sigma^2 \left( \tau(x) \tau(i) \right) = \sigma^2(\alpha (-i)) = \sigma^2(\alpha) \sigma^2(-i) = (-\alpha)(-i) = \alpha i
\]

\[
\Rightarrow \quad H₅ \text{ fixes } \alpha i, \quad \text{since } \alpha i \text{ is a root of } x^4 - 2, \text{ its degree over } \mathbb{Q}(\alpha) \text{ is } 4. \text{ And also } [D₄:H₅] = 4 \Rightarrow \quad \left[ \mathbb{Q}(\alpha) : \mathbb{Q}(i, \alpha) \right]
\]
$H_3$: We have $H_3 = \{1, \sigma^2, \sigma \tau, \sigma^3 \tau\}$.

$\sigma^2(x^2) = x^2$, $\sigma^2(i) = i \implies \sigma^2(x^2i) = x^2i$.

$\sigma \tau(x^2i) = \sigma(\tau(x^2) \tau(i)) = \sigma(x^2(-i)) = \sqrt{-1} \cdot \sqrt{-1} = \sigma(x) \sigma(x) \sigma(-i) = (i \sigma)(i \sigma)(-i) = x^2i$.

$\sigma^3 \tau(x^2i) = \ldots = x^2i$.

Note $P_{x^2i}(x) = x^2 + 2$ since $(x^2i)^2 + 2 = -x^4 + 2 = 0$.

$\Rightarrow [\Omega(x^2i): \Omega] = 2 = [D_4: H_3] \implies K^{H_3} = \Omega(x^2i)$. 
$H_7$: Our group $H_7 = \{1, \sigma \}$ is of size 2, so it must fix $\alpha + \sigma_2(\alpha)$, the reason for this is if we apply either $id$ or $\sigma_2$ to $\alpha + \sigma_2(\alpha)$, we're left again with $\alpha + \sigma_2(\alpha) = \sum \psi(\alpha)$. And by direct calculation, $\psi \in H_7$

$\alpha + \sigma_2(\alpha) = \alpha + \sigma(\alpha) = \alpha + i\alpha$ & this is degree 2 over $\Omega(\alpha^2i) \Rightarrow |K|^{H_7} = \Omega(\alpha + i\alpha)$
$H_8$: We do this similarly to $H_7$ but w/ $H_8 = \{1, \sigma^3 \tau \}$. Note

$\alpha + \sigma^3 \tau (\alpha)$ is fixed by $H_8$, i.e.,

$\alpha + \sigma^3 \tau \alpha = \alpha + \sigma^3 (\alpha) = \alpha - i\alpha$. We don't try this for $i$. Since

$i + \sigma^3 \tau (i) = i + \sigma^3 (-i) = i - i = 0$ which is always fixed. $\Rightarrow K^{H_8} = \Omega (\alpha - i\alpha)$. 
In conclusion, we usually draw the following:

\[
K^G = C_\ell
\]

\[
K^H_1 = C_\ell(\alpha \bar{z})
\]
\[
K^H_2 = C_\ell(i)
\]
\[
K^H_3 = C_\ell(\alpha^2 i)
\]
\[
K^H_4 = C_\ell(\alpha)
\]
\[
K^H_5 = C_\ell(\alpha i)
\]
\[
K^H_6 = C_\ell(i, \alpha^2)
\]
\[
K^H_7 = C_\ell(\alpha + i\alpha)
\]
\[
K^H_8 = C_\ell(\alpha - i\alpha)
\]

\[
C_\ell(\alpha, i)
\]
\[ \mathcal{C}(x, i) \]

\[ \mathcal{C}(x, i) \]

\[ \mathcal{C}(x^2, i) \]

\[ \mathcal{C}(x + i) \]

\[ \mathcal{C}(x^2) \]

\[ \mathcal{C}(i) \]

\[ \mathcal{C}(i x^2) \]