Last time: \( p(x) = x^4 - 72x^2 + 4 \) is irreducible in \( \mathbb{Z}[x] \) but is reducible in \( (\mathbb{Z}/n\mathbb{Z})[x] \) for every \( n \).

\[\begin{align*}
Ex: \mod 3 & : x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2) \\
\mod 5 & : x^4 + 3x^2 + 4 = (x^2 + x + 2)(x^2 + 4x + 2) \\
\mod 7 & : x^4 + 5x^2 + 4 = (x^2 + 1)(x^2 + 4) \\
\mod 31991 & : = (x^2 + 1549x + 2)(x^2 + 30,442x + 2)
\end{align*}\]

If \( p \) factors over \( \mathbb{Z}[x] \), by above it does so as \( (x^2 + ax + b)(x^2 + cx + d) \) with \( b \cdot d = 4 \Rightarrow b, d = \pm 1, \pm 4 \) or \( \pm 2, \pm 2 \). The mod 3 and 7 info gives contradictory things, so \( p \) is irreducible.

That \( p \) factors mod all \( n \) comes from quadratic reciprocity about when \#5 are squares mod \( n \).
(e.g. if \( 76 = a^2 \mod n \), then \( \overline{p} = (x^2 + ax + 2)(x^2 - ax + 2) \))

This in turn comes from understanding factorization in \( \mathbb{Z}[\zeta_n = e^{2\pi i/n}] \subseteq \mathbb{Q}(\zeta_n) \) via Galois theory.

So on to Chapter 13!
Field: A commutative ring w/ one where every nonzero element is a unit.

Ex: $\mathbb{Q}, \mathbb{Q}(S_p), \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

$\mathbb{C}(x) =$ rational functions $\frac{p(x)}{q(x)} =$ field of fractions of $\mathbb{C}[x]$.

$\mathbb{F}_p ((t)) =$ formal power series $\{ a_n t^n + a_{n+1} t^{n+1} + a_{n+2} t^{n+2} + \ldots \}$ where $n$ may be negative.

$p = 2: \frac{1}{1+t} = 1 + t + t^2 + t^3 + t^4 + \ldots$

$\mathbb{Q}_p -$ p-adic field

Characteristic: Smallest $n$ such that $n \cdot 1 = 1 + 1 + \ldots + 1 = 0$ in $F$ or 0 if no such $n$ exists.

Ex: $\text{ch}(\mathbb{Q}) = 0, \text{ch}(\mathbb{F}_p) = p, \text{ch}(\mathbb{F}_p ((t))) = p$.

Prop: If $\text{ch}(F) \neq 0$, then it is prime.

Pf: Suppose $\text{ch}(F) = a \cdot b$. Then

$(a \cdot 1) \cdot (b \cdot 1) = (ab) \cdot 1 = 0$

but neither $a \cdot 1$ or $b \cdot 1$ is 0, contradicting that $F$ is integral domain.
**Prime subfield**: subfield generated by 1.

Is $\mathbb{Q}$ if char = 0 or $\mathbb{F}_p$ when char = p.

**Field Extension** [Key concept!]. If $K$ is a subfield of $F$, we call $F$ an extension of $K$ and write $F/K$ or $F$.

$K$

Ex: $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{F}_p((t))/\mathbb{F}_p$

[Any field is an extension of its prime subfield.]

Consider $F/K$. Then $F$ is a $K$-vector space, since given $k \in K$ and $f \in F$ have $k \cdot f \in F$ sat:

\[
\begin{align*}
  k \cdot (f_1 + f_2) &= k \cdot f_1 + k \cdot f_2 \\
  k_1 (k_2 \cdot f) &= (k_1 k_2) \cdot f \\
  (k_1 + k_2) \cdot f &= k_1 \cdot f + k_2 \cdot f \\
  1_k \cdot f &= f
\end{align*}
\]

Axioms for a $K$-vector space all follow from field props.
Ex: \( \mathbb{C}/\mathbb{R} \) A basis for \( \mathbb{C} \) as an \( \mathbb{R} \)-vector space is \( \{1, i\} \) since \( \mathbb{C} = \{a+bi \mid a, b \in \mathbb{R}\} \).

[also \( \{\sqrt{2}, 1+\sqrt{3}i\} \ldots \)]

2. \( \mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\} \) has \( \mathbb{Q} \) basis \( \{1, \sqrt{2}\} \) \( \mathbb{Q} \) subfield of \( \mathbb{R} \)

3. \( \mathbb{R}/\mathbb{Q} \) Any basis is infinite, in fact uncountable.

Degree: \( [F:K] = \text{size of a } K \text{ basis} = \dim_K F \) for \( F \)

Ex: \( [\mathbb{C}:\mathbb{R}] = [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2 \), \([\mathbb{R}:\mathbb{Q}] = \infty\)

Building fields by adding roots: Start with a field \( K \) and a \( p(x) \in K[x] \) irreducible and nonconst. Then

\[ F = K[x]/(p(x)) \] is a field since \( K[x] \) is a PID

\( p \) is prime

(\( p \) is prime)

(\( p \) is maximal)
An elt of $F$ has the form $f(x) + I$ where $I = (p)$. Can assume $\deg f < \deg p$ since $f = qp + r$ with $\deg r < \deg p$ and $f + I = f - qp + I = r + I$

If $f, f'$ have $\deg < \deg p$, then $f + I = f' + I$ iff $f = f'$ in $K[x]/I$, since $\sim$ means $f - f' \in I$ and the only elt of $(p(x))$ of $\deg < \deg p$ is $0$.

So $F \leftrightarrow \{ \text{polys of } K[x] \}$

Ex: $K = \mathbb{R}$, $p = x^2 + 1$ which is irreducible (no roots in $\mathbb{R}$).

$$F = \frac{\mathbb{R}[x]}{(x^2 + 1)} = \{ ax + b + I \mid a, b \in \mathbb{R} \}$$

What is an $\mathbb{R}$-basis for $F$? $\{1, x\}$

In general $[F = K[x]/(p(x)) : K] = \deg p(x)$

since $1, x, x^2, \ldots, x^{\deg p - 1}$ is a $K$ basis for $F$. 
Now $F = \mathbb{R}[x]/(x^2+1)$ is isom to $\mathbb{C}$ via

\[
\begin{array}{c}
1 \leftrightarrow \rightarrow 1 \quad \text{or} \quad 1 \leftrightarrow \rightarrow 1 \\
x \leftrightarrow \rightarrow i \quad \leftrightarrow \rightarrow -i
\end{array}
\]

Ex: $\mathbb{Q}[x]/(x^3-1)$  

Q: What's wrong with this?

A. $x^3 - 1$ factors into 

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

$\mathbb{Q}[x]/(x^2+x+1) \cong \mathbb{Q}(\xi_3 = e^{2\pi i/3})$