Lecture 7: Field Extensions

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

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: $= (x^2+1549x+2)(x^2+30,442x+2)$

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 <u>quadratic reciprocity</u> about when #s are squares mod n.

(e.g. if $76 = a^2 \bmod n$, then $\bar{p} = (x^2+ax+2)(x^2-ax+2)$)

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 $\{a_n t^n + a_{n+1} t^{n+1} + a_{n+2} t^{n+2} + \cdots\}$

↖ n may be negative.

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

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

Characteristic: Smallest n such that

$$n \cdot 1 = \underbrace{1+1+\cdots+1}_{n} = 0 \text{ in } F$$ or 0 if no such n exists.

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

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

Pf: Suppose $ch(F) = a \cdot b$. 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 $\begin{matrix} F \\ | \\ K \end{matrix}$.

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:

$$k \cdot (f_1 + f_2) = k \cdot f_1 + k \cdot f_2$$
$$k_1 (k_2 \cdot f) = (k_1 k_2) \cdot f$$
$$(k_1 + k_2) \cdot f = k_1 \cdot f + k_2 \cdot f$$
$$1_K \cdot f = f$$

} Axioms for a K-vector space all follow from field props.

Ex: ① $\mathbb{C}/\mathbb{R}$ 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 $\{\sqrt{2}, 1+\sqrt{3}i\}$...]

② $\underbrace{\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}}_{\text{subfield of } \mathbb{R}} / \mathbb{Q}$ has $\mathbb{Q}$ basis $\{1, \sqrt{2}\}$

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

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

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

$\Rightarrow p$ is prime

$\Rightarrow (p)$ is prime

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

So $F \xleftrightarrow{\text{bijection}} \left\{ \begin{array}{l} \text{polys of } K[x] \\ \text{of } \deg < \deg p \end{array} \right\}$

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

$$F = \mathbb{R}[x]/(x^2+1) = \left\{ ax + b + I \;\middle|\; a, b \in \mathbb{R} \right\}$$

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

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

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

$1 \longleftrightarrow 1$, $x \longleftrightarrow i$ $\quad$ or $\quad$ $1 \longleftrightarrow 1$, $x \longleftrightarrow -i$

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

Q: What's wrong with this?

A. x^3-1 factors into

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

$$\mathbb{Q}[x]/(x^2+x+1) \cong \mathbb{Q}(\zeta_3 = e^{2\pi i/3})$$