Lecture 7: Field extensions

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

Ex: mod 3, have $x^4+1 = (x^2+x+2)(x^2+2x+2)$
mod 5, have $x^4+3x^2+4 = (x^2+x+2)(x^2+4x+2)$
mod 7, have $x^4+5x^2+4 = (x^2+1)(x^2+4)$
mod 31911, $= (x^2+1549x+2)(x^2+30442x+2)$

So if p factors over $\mathbb{Z}[x]$ must be $= (x^2+ax+b)(x^2+cx+d)$ with $b \cdot d = 4 \Rightarrow b, d = \pm 1, \pm 4$ or $\pm 2, \pm 2$. The mod 3 + 5 info gives contradictory things, so p is irreducible.

That p always factors mod n comes from quadratic reciprocity about when #s are squares mod n.
(e.g. if $76 = a^2$, then $p(x) = (x^2+ax+2)(x^2-ax+2)$)
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!

(Martin review of chap. 11.)

Field: A comm. ring w/ one where every nonzero elt is a unit.

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

$\mathbb{C}(x) =$ 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.

$\mathbb{Q}_p$ - padic field

Characteristic: Smallest n such that

$n \cdot 1 = \underbrace{1+1+\cdots+1}_{n} = 0$ 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 a prime.

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

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

but neither term on the LHS is 0, contradicting that F is an int. domain. $\blacksquare$

Prime subfield: Subfield gen by 1.

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

[Key!]

Field Extension: If K is a subfield of F,

then say that F is an extension of K and

write F/K or
$$\begin{array}{c} F \\ | \\ K \end{array}.$$

rational fns

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.

$$\left.\begin{aligned} k\cdot(f_1+f_2) &= k\cdot f_1 + k\cdot f_2 \\ k_1\cdot(k_2\cdot f_2) &= (k_1k_2)\cdot f \\ (k_1+k_2)\cdot f &= k_1\cdot f + k_2\cdot f \\ 1_K\cdot f &= f. \end{aligned}\right\}$$

Axioms for a K-vector space all follow from props of fields.

Ex: ① $\mathbb{C}/\mathbb{R}$ What is a basis for $\mathbb{C}$ as an $\mathbb{R}$ vector space? A. $\{1, i\}$ since

$\mathbb{C} = \{a+bi \mid a, b \in \mathbb{R}\}$

or $\{\sqrt{2}, 1+\sqrt{3}i\}$ or...

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

Basis for $\mathbb{Q}(\sqrt{2})$ as a $\mathbb{Q}$ vector space: $\{1, \sqrt{2}\}$

③ $\mathbb{R}/\mathbb{Q}$ A basis has to infinite, in fact uncountable since $\mathbb{R}$ is uncountable but $\mathbb{Q}$ is countable.

Degree: $[F:K]$ = size of a K-basis of F.

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

Building fields by adding roots.

K - field $p(x)$ - irred nonconst poly in $K[x]$

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

$\Rightarrow (p)$ is a prime ideal

$\Rightarrow (p)$ is maximal.

An elt of F has the form $f(x)+I$ where $I=(p(x))$. Can assume $\deg f < \deg p$ since if $f = a_n x^n + \cdots + a_0$ and $p = b_m x^m + \cdots + b_0$ with $n \geq m$ then

$$f(x)+I = f(x) - \frac{a_n}{b_m} p(x) + I$$
$$= \frac{a_n a_{n-1}}{b_m} x^{n-1} + \cdots + I$$

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

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

<u>Ex</u>: $K = \mathbb{R}$, $p = x^2+1$ which is irred since it has no roots.

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

Q: What is an $\mathbb{R}$ basis for F? A. $\{1, x\}$

In general $[F = K[x]/(p(x)) : K] = \deg p(x)$
since $1, x, \ldots, x^{\deg p - 1}$ is a K-basis for F.

Now $F = \mathbb{R}[x]/(x^2+1)$ is isom to $\mathbb{C}$

via

$$1 \longleftrightarrow 1$$
$$x \longleftrightarrow i$$

or

$$1 \longleftrightarrow 1$$
$$x \longleftrightarrow -i$$

Further examples, e.g. $\mathbb{Q}(\sqrt{2})$ as time allows. Or $\mathbb{Q}(\zeta_3 = e^{2\pi i/3})$, so $\zeta_3^3 = 1$, though $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$.