Last time: solvability. Today: fields!

II fields

§1. Reminder about ring of polynomials
§2. Field extensions

III §2 Polynomials
Fix a ring $R$.

Def: A power series over $R$, in variable $x$, is a formal expression
\[ f = \sum_{n=0}^{\infty} a_n x^n, \quad \text{where} \quad (a_n)_{n=0}^{\infty} \subset R \]

\[ g = \sum_{n=0}^{\infty} b_n x^n \]
is another such, so $R[x]$ is the set:

\[
rf \overset{\text{def}}{=} \sum_{n=0}^{\infty} (ra_n)x^n \quad \quad fg \overset{\text{def}}{=} \sum_{n=0}^{\infty} (\sum a_i b_n) x^n \\
f + g \overset{\text{def}}{=} \sum_{n=0}^{\infty} (a_n + b_n) x^n \quad \quad l = 0 \quad m + n = l
\]

Ex: This endows the set $R[[x]]$ of power series with the structure of an $R$-algebra (\( = \) ring + $R$-module, "arithmetic works as expected") compatibly.

Def: A polynomial is a power series with finitely many non-zero coefficients. Write $R[x] \subset R[[x]]$ for the set of polynomials.
**Ex:** \( \mathbb{R}[x] \) is a subalgebra.

**Def:** The degree \( \deg f \in \mathbb{R}[x] \) is \( \deg f = \max \{ n \mid a_n \neq 0 \} \)

the leading coefficient of \( f \) is \( a_{\deg f} \)

**call \( f \) monic if its leading coeff is 1.**

**Lemma:** \( \mathbb{R} \) is an integral domain then

1. \( \deg (fg) = \deg f + \deg g \)
2. \( \deg (f+g) = \max \{ \deg f, \deg g \} \) (\( = \) if \( \deg f = \deg g \))
3. \( \) if \( \deg f, \deg g \leq 0 \) then \( \deg (f+g) = 0. \) \( \mathbb{R}\mathbb{C} \) is an integral domain

4. \( fg = 1 \Rightarrow \deg f = \deg g = 0 \) and \( f, g \in \mathbb{R}^* \)

**Not:** \( \mathbb{R} \) is a field, \( f, g \in \mathbb{R}[x], f \neq 0, \) then \( \exists! g, r \in \mathbb{R}[x] \) with \( \deg r < \deg f \) st \( g = qf + r. \)

\( \) division with remainder.

**Ex:** enough that the leading coeff of \( f \) be invertible

\( \Rightarrow \) \( \mathbb{R}[x] \) is a Euclidean domain \( \Rightarrow \) PID \( \Rightarrow \) UFD

An ideal \( I \subset \mathbb{R}[x] \) has the form \( I = (m) \) when \( m \in \mathbb{F} \) is the monic poly of least degree, \( I \) is prime

if \( I \) maximal \( \Rightarrow m \) is irreducible

(int. domain)

**Recall:** \( \mathbb{R} \) nice, \( \mathbb{R} \) is a field if can write \( f = gh \)

with \( g, h \in \mathbb{R}^* \) i.e. \( g, h \) not assoc. to \( f \) (in form of \( \mathbb{R}\mathbb{C} \))
I is prime if \( \{ f, g \in \mathbb{I} \rightarrow fg \in \mathbb{I} \} \) \( \Rightarrow \mathbb{R}/\mathbb{I} \) is an integral domain \( \Rightarrow \mathbb{R}/\mathbb{I} \) is a field

(no ideals in \( \mathbb{R}/\mathbb{I} \) other than \( \mathbb{I} \))

In a PID prime \( \Rightarrow \) maximal; (converse always true)

prime \( \Rightarrow \) irreducible  

if \( f \mid gh \)  

the \( f \mid a \) or \( f \mid b \)  

if \( f \mid gh \)  

the \( f \mid a \) or \( f \mid b \)  

if \( f \mid gh \)  

when \( g \) or \( h \) is a scalar

---

A bit of number theory.

Need a supply of irreducible polynomials.

**HW:** if \( f \in F[x], \deg f \leq 2 \), then \( f \) irreducible has no root in \( F \).

(+ "rational root thin")

**Thm:** (Gauss's lemma): let \( f \in \mathbb{Z}[x] \) be irreducible. Then \( f \) is irreducible in \( \mathbb{Q}[x] \) as well.

**Pf:** suppose \( f \) is reducible in \( \mathbb{Z}[x] \), say \( f = gh \) for some \( g, h \in \mathbb{Z}[x], \deg g, h \geq 1 \).

Then there exists \( a \in \mathbb{Z}_2 \), s.t. \( af = gh \) with \( g, h \in \mathbb{Z}[x] \) ("clearing denominators"). Suppose \( af = gh \) and let a minimal \( a \in \mathbb{Z}_2 \), the \( f = gh \), impossible.

Otherwise, there is a prime \( p \) \( \not| \) polynomial.

Reduce everything mod \( p \): write \( \overline{g} \) for \( g \) in \( \mathbb{Z}_p[\mathbb{Z}_2[x]] \) whose coefficients are the reduction mod \( p \) of the coeff. of \( g \).
Then \( \overline{a_f} = \overline{0} \) since \( p|a \)
so \( \overline{g}/\overline{h} = \overline{0} \)
but \( \mathbb{Z}/p\mathbb{Z} \) is a field, so \( \mathbb{Z}/p\mathbb{Z}[x] \) is an int. domain.
So either \( \overline{g} = \overline{0} \), or \( \overline{h} = \overline{0} \). Wlog \( \overline{g} = \overline{0} \), i.e. every coeff \( \overline{a} \) is divisible by \( p \). But then:
\[
\frac{a}{p} \cdot f = \frac{g}{p} \cdot h
\]
with \( \frac{a}{p} \in \mathbb{Z}/p \), \( p|g \), \( \overline{\frac{a}{p}} \notin \mathbb{Z}/p \mathbb{Z}[x] \).
Impossible.

This (Eisenstein's criterion) let \( f \in \mathbb{Z}[x] \), \( f = a_n x^n + \cdots + a_1 x + a_0 \).
Suppose \( p \) prime s.t. \( p \nmid a_n \), \( p \mid a_i \) for \( i < n \).
Then \( f \) is irreducible in \( \mathbb{Z}[x] \).

**Proof:**
Suppose \( f = gh \) (d.e. \( \deg g, \deg h \) d.e. \( f \)).
Reduce everything mod \( p \), and \( f = \overline{f} \).
Now \( \overline{f} : \overline{a_n} \cdot \overline{x}^n \).
Since \( \mathbb{Z}/p\mathbb{Z}[x] \) is a UFD, must have \( \overline{g} = \overline{r} \cdot \overline{x}^r \), \( \overline{h} = \overline{s} \cdot \overline{x}^s \)
where \( r + s = d \). Therefore \( g = \sum_{k=0}^{r} r_k \cdot x^k \), \( h = \sum_{k=0}^{s} s_k \cdot x^k \).
(d.e. \( \deg g = r \), \( \deg h = s \), and \( \deg g + \deg h = \deg f = d = r + s \))
so \( \deg g = r \), \( \deg h = s \)

where \( p \mid \deg g \), \( p \nmid \deg h \) if \( \deg g = r \).
But if \( f = gh \) then \( a_0 = b_0 c_0 \) \( \implies r, s \geq 1 \) so \( p \nmid \deg g \)

\[ p^2 \mid a_0 \]
Example: The \( p \text{-th} \) cyclotomic polynomial is
\[
\Phi_p(x) = \frac{x^p - 1}{x - 1}
\]
(rmk: \( \Phi_p(1) = 0 \) but \( \Phi_p(\zeta) \neq 0 \) for \( \zeta \neq 1 \))
i.e. \( \zeta \) is an element of \( \mathbb{F}_p \) in a field.

Claim: \( \Phi_p(x) \) is irreducible in \( \mathbb{Z}[x] \)

**Pf:** Map \( \mathbb{Z}[x] \to \mathbb{Z}[y] \) is a ring hom isom (reverse is \( y \mapsto x - 1 \))

So enough to check \( \Phi_p(y + 1) \) is irreduc.

\[
\Phi_p(y + 1) = \frac{\prod (y + 1)^p - y}{(y + 1)^p - 1} = \frac{\prod (y + 1)^p - y}{(y + 1)^p - 1} = \sum_{i=0}^{p-1} (\frac{P_i}{1})y^i + 1
\]

\[
= \sum_{i=0}^{p-1} (\frac{P_i}{1})y^i + y^p + \sum_{i=0}^{p-2} (\frac{P_i}{1})y^i
\]

This is Eisenstein: monic \( \frac{p}{1} \) not \( \text{div} \) by \( p^3 \) (w/o \( p \) in denom)

Fact: if \( f \in \mathbb{Q}[x] \) is irreducible then the roots of \( f \) are distinct.

Roots of unity in \( \mathbb{C} \) are the elements \( \exp \frac{2\pi i}{n} \), \((\phi, n) = 1\)

Def: \( \Phi_n(x) = \prod (x - \exp \frac{2\pi i}{n}) \)

\( a \in \mathbb{Z}/n\mathbb{Z} \)
Thus $\Psi_h(x) \in \mathbb{D}$, indeed.

Better: $\Psi_h(x) = \frac{x^t - 1}{\prod_{\text{all } \ell \in \mathbb{D}} \Psi_h(\ell)}$ - same thin

[if all then $\Psi_h(\ell) | x^d - 1 | x^t - 1$]

Aside

Def: A field $F$ is algebraically closed if every polynomial in $F[x]$ has a root in $F$.

F.T. of Algebra: $\overline{F}$ is algebraically closed

if $F, K$ contain $\overline{F}$, are algebraically closed, are uncountable then $F \times K \approx |F| \cdot |K| = |F|^2$

$\mathbb{Q}_p$ is another completion of $\mathbb{Q}$, so $\overline{\mathbb{Q}_p} = \mathbb{C}$ ($\text{field of } p\text{-adic numbers}$)

To study systems of equations, associate wedge $(\mathbb{C}$, $\mathbb{Q}$)

+ matrices "Frobenius", acts on it $^t$

Eigenvalues of matrix are important:

Fact: Generally, eigenvalues don't depend on $t$ (after ideal) with $\mathbb{C}$