lect 7
Sept. 30

Def A polynomial $p(x) \in F[x]$ is irreducible if $p(x)$ is not a constant polynomial ($\deg p \geq 1$) and does not factor nontrivially: if $p = fg$ for $f, g \in F[x]$, one of f or g is invertible ($f \in F^*$ or $g \in F^*$ a constant polynomial, not 0).

If $p = fg$ and f, g not constants $\Rightarrow \deg f < \deg p$ or $\deg g < \deg p$.

A polynomial is reducible if it is not irreducible.

Examples: 1) degree 1 polynomials are irreducible $ax+b$ $a \neq 0$

2) $p(x)$ is irreducible $\Leftrightarrow$ corresponding monic polynomial is irreducible

$p(x) = a_n x^n + \dots + a_0$

$a_n \underline{(x^n + a_{n-1} a_n^{-1} x^{n-1} + \dots + a_0 a_n^{-1})}$

$\uparrow$ invertible in F.

3) quadratic polynomial $p(x)$ is reducible

$\Updownarrow$

it has a linear factor in $F[x]$

$\Updownarrow$

$p(x)$ has a root in F

cubic $p(x)$ is reducible

$\Updownarrow$

has a root in F.

Examples: 1) $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ (no roots)

reducible in $\mathbb{R}[x]$ (roots $\pm\sqrt{2}$)

2) $x^2 + 4$ irreducible in $\mathbb{R}[x]$, reducible in $\mathbb{C}[x]$ roots $\pm 2i$

3) $\mathbb{F} = \mathbb{F}_2$ $x^2 + x + 1$ irreducible (no roots, $0^2 + 0 + 1 = 1$, $1^2 + 1 + 1 = 1$)

$x^2 + 1 = (x+1)^2$ reducible, $\underbrace{x^3 + 1, x^3 + x + 1, x^3 + x^2 + 1}_{?}$ irreducible or reducible in $\mathbb{F}_2[x]$?

Degree 4 and higher : may be reducible but have no roots in F

$$x^4 - 9 = (x^2-3)(x^2+3) \quad \text{no roots in } \mathbb{Q}$$

$$x^4+x^2+1 = (x^2+x+1)(x^2+x+1) \quad \text{in } \mathbb{F}_2, \text{ but no roots in } \mathbb{F}_2$$

Recall from lecture 4

Lemma (Euclid) If $p(x) \in F[x]$ is irreducible and $p(x) \mid q_1(x) \dots q_n(x)$ then $p(x) \mid q_j(x)$ for some j.

(it was stated in slightly greater generality, for $p(x)$ irreducible or constant).

This lemma implies

Theorem (Unique factorization in polynomial rings)
(see Friedman, "Factorization..." notes, Thm 2.13 on page 9)
Let $f \in F[x]$, f not constant. Then there exist irreducible polynomials $p_1, \dots p_k$, such that

$$f = p_1 p_2 \dots p_k.$$

f can be factored into a product of irreducible polynomials.

Factorization is unique up to permutation of factors and multiplying by units. If

$$f = p_1 \dots p_k = q_1 \dots q_\ell$$

then $\ell = k$ and, after reordering q's, if necessary,

$$q_i = c_i p_i \text{ for some } c_i \in F^*$$

Proof Existence

By induction on $\deg f$

$\deg f = 1$ f - linear $\Rightarrow$ irreducible $f = f$ ← one factor, p_1

Induction step: if true for $\deg f \le n-1$, consider f, $\deg f = n$.

If f is irreducible, done. $f = f$

If f is reducible, $f = gh$ $\deg g, \deg h < n$.

Factor g and h and multiply their factorizations to get a factorization for f

Uniqueness If $f = p_1 \cdots p_k = q_1 \cdots q_l$, p's, q's irreducible.

By induction on k

$k=1$ $f = p_1$ $p_1 = q_1 \cdots q_l$ contradiction with p_1 being irreducible unless $l=1$, $q_1 = p_1$

Inductive step: Use Euclid's lemma, $p_1 \mid q_1 \cdots q_l \Rightarrow p_1 \mid q_j$ some j.

q_j irreducible $\Rightarrow$ $q_j = c p_1$, $c \in F^*$ invertible

$$\underline{\underline{p_1}} \cdots p_k = c \underline{\underline{p_1}} (q_1 \cdots q_{j-1} q_{j+1} \cdots q_l)$$

use cancellation lemma (since $F[x]$ is an integral domain)

$$p_2 \cdots p_k = \underbrace{c\, q_1}_{} \cdots q_{j-1}$$

group together into irreducible cq_1

Can apply induction assumption now ($k-1$ terms on the left).

Prime and maximal ideals

(see Friedman, Ideals, section 2 and "Factorizations...", sect. 3)

Def An ideal $I \subset R$ is a prime ideal if $I \neq R$ and if $rs \in I$ then $r \in I$ or $s \in I$, for $r, s \in R$.

Prop R/I is an integral domain if and only if I is a prime ideal in R.

Proof R/I has zero divisors

$\Updownarrow$

$\exists$ $r+I$, $s+I$ are zero divisors $(r+I)(s+I) = I$, $r+I \neq I$, $s+I \neq I$
$r \notin I$, $s \notin I$

$\Updownarrow$

$\exists r,s$: $rs + I = I$, $r \notin I$, $s \notin I$

$\Updownarrow$

$\exists r,s$: $rs \in I$, $r \notin I$, $s \in I$.

Examples 1) $\{0\}$ is a prime ideal iff R is an integral domain

2) $(15) \subset \mathbb{Z}$ not a prime ideal, $5, 3 \in \mathbb{Z} \setminus (15)$, $5 \cdot 3 \in (15)$.

3) $(nm) \subset \mathbb{Z}$, $n, m > 1$ is not a prime ideal $n \cdot m \in (nm)$ but $n, m \notin (nm)$

4) $(x^2+x) \subset F[x]$ not a prime ideal $x, x+1$. $x(x+1) \in (x^2+x)$

Prime ideals in $\mathbb{Z}$: (0), $(p) = (-p)$ prime

Prime ideals in $F[x]$: (0), $(p(x))$ irreducible

<u>Theorem</u> (Correspondence theorem for rings)

$I \subset R$ proper ideal $\rightsquigarrow R/I$ quotient ring $\qquad R \xrightarrow{\alpha} R/I$ quotient map

There is a bijection between intermediate ideals J

$I \subset J \subset R$ and ideals $K \subset R/I$.

Intermediate ideals $I \subset J \subset R$ $\quad \overset{\text{bijection}}{\longleftrightarrow} \quad$ ideals of R/I $\quad K$

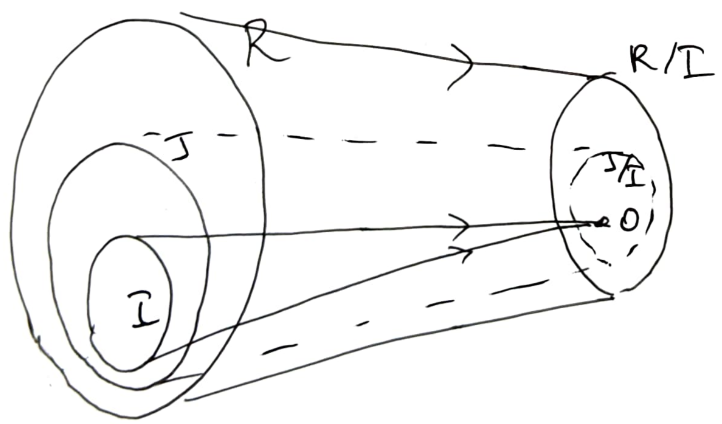
$$J \longmapsto J/I = \{a + I : a \in J\}$$

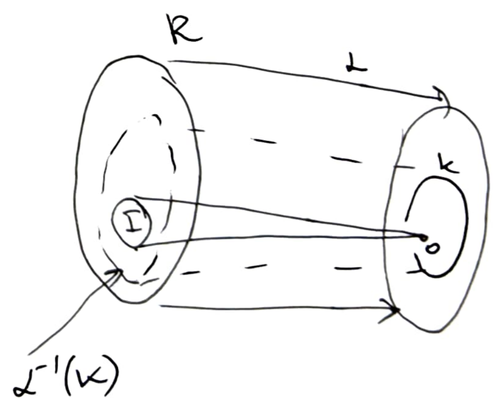
$$J/I = \alpha(J)$$

$$\{j \in R \mid \alpha(j) \in K\} \longleftarrow K$$

$\qquad = \alpha^{-1}(K)$

notation for inverse image of a set under a map α





<u>Exercise:</u> Prove Correspondence thm for rings. Compare with the correspondence theorem for groups.

[See ex. 3.8 in Rotman, p. 23].

__Def__ $I \subset R$ is a __maximal__ ideal if $I \neq R$ and for any ideal J, $I \subset J \subset R$, either $J = I$ or $J = R$

__Thm__ R/I is a field iff I is a maximal ideal.

Proof: see Friedman, prop 2.4 in "Ideals", or use correspondence theorem. If $\exists J$, $I \subset J \subset R$, $J \neq I, R$

$$\begin{array}{ccc} R & \xrightarrow{\alpha} & R/I \\ \cup & & \cup \\ J & \longrightarrow & \alpha(J) \end{array}$$

$\Rightarrow \alpha(J)$ is a proper ideal of R/I, $\alpha(J) \neq \{0+I\}$

$\alpha(J)$ ideal that is neither $\{0\}$ nor R/I

Recall that F is a field iff the only ideals of F are $\{0\}$ and F.

Any intermediate ideal J in R will produce an ideal in R/I other than $\{0\}, R/I$ and vice versa.

$K \subset R/I$ ideal, $K \neq 0, R/I$

$\alpha^{-1}(K) = \{a \mid \alpha(a) \in K\}$ is an intermediate ideal

$\square$

__Corollary__: A maximal ideal is a prime ideal

Holds, since any field is an integral domain.

Example 1) $\mathbb{Z}$ $\quad (0), (p)$, p - prime are prime ideals

(p), p - prime are maximal ideals

(0) is a prime but not a maximal ideal

2) $\mathbb{Z}[x]$ $\quad (x)$ is prime ideal $\quad \mathbb{Z}[x]/(x) \cong \mathbb{Z}$ integral domain

(x) is not maximal, $\mathbb{Z}$ not a field

what happens if we change from $\mathbb{Z}$ to a field F in this example?

Thm $\quad I \subset F[x]$ an ideal. TFAE:

(1) I is a maximal ideal

(2) I is a prime ideal and $I \neq \{0\}$

(3) there exists an irreducible polynomial p such that $I = (p)$

Proof (for more details see Friedman, Thm 3.1. in Factorizations section)

$(1) \Rightarrow (2)$ $\quad$ maximal implies prime; $(0) \subset F[x]$ is not maximal.

$(2) \Rightarrow (3)$ $\quad F[x]$ is a PID $\Rightarrow I = (p)$ some p. Want to show p is irreducible. Otherwise $p \in F$ a constant $\begin{cases} p \in F^* & (1) = F[x] \text{ not maximal} \\ p = 0 & (0) \text{ not maximal} \end{cases}$

or $p = fg$ $\quad \deg f, \deg g < \deg p$. $\Rightarrow fg \in (p)$, but $f \notin (p), g \notin (p)$ due to their degrees.

$(3) \Rightarrow (1)$ $\quad$ if $I = (p)$, p irreducible $\Rightarrow p$ not a unit, $(p) \neq 0, F[x]$

if $(p) \subset J \subset F[x]$ intermediate ideal, $J = (f)$, some f

$(p) \subset (f) \Rightarrow \; p = fq$, but p is irreducible $\Rightarrow J = F[x]$ or $J = (p)$.

Corollary Let $f \in F[x]$. Then $F[x]/(f)$ is a field iff f is irreducible.

Explanation: How to find the inverse of $g+(f) \in F[x]/(f)$? $g \notin (f)$

$\gcd(f,g)=1$ $1, f$ are the only factors of f.

$\Rightarrow 1 = af + bg$ some a, b.

$\Rightarrow bg = 1 - af$, $bg \in 1 + (f)$. $\Rightarrow$
b is the inverse of g in $F[x]/(f)$.

Get a large supply of fields that contain F, one for each irreducible polynomial. Can assume f monic

$c \in F^*$ $(cf) = (f) \Rightarrow F[x]/(fc) \simeq F[x]/(f)$.

$\deg f = 1$ $f = x + a$ $F[x]/(x+a) \simeq F$ exercise.

need irreducible polynomials of $\deg \geq 2$ for interesting examples

$\mathbb{R}[x]$, $f = x^2+1$ $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$ a field

$\mathbb{F}_2[x]/(x^3+x+1) \simeq \mathbb{F}_8$ field with 8 elements, see last lecture

$\mathbb{F}_2[x]/(x^2+x+1) \simeq \mathbb{F}_4$ 4-element field $\{0, 1, x, x+1\}$ $x(x+1) = 1$.
$x+1 = x^{-1}$ in $\mathbb{F}_4$.

irreducible, no roots in $\mathbb{F}_2$

relabel x into y

$E = \mathbb{F}_2[y]/(y^2+y+1)$ $\{0,1,y,y+1\}$.

E is a field, $E = \mathbb{F}_4$

polynomial $f(x) = x^2+x+1$ irreducible in $\mathbb{F}_2$

$f(x) = (x+y)(x+y+1)$ factors in E.

$(x+y)(x+y+1) = x^2 + (y+1)x + yx + y(y+1) = x^2+x+1$.

Made the field of constants larger, polynomial factors.

$f(x)$ - irreducible $\Rightarrow F[x]/(f(x))$ is a field

we use a different variable $E = F[y]/(f(y))$.

$$\begin{array}{ccc} F[x] & \subset & E[x] \\ \cup & & \cup \\ F & \subset & E \end{array}$$

constants y

Still free to use x.

In $F[x]$, no relations on powers of x

In E, relation on powers of y.

E is a <u>field</u>, since f is irreducible

evaluation homomorphism $E[x] \xrightarrow{ev_y} E$

x - formal variable

$y \in E$ "constant"

$f(x) \longmapsto f(y)$

$$\begin{tikzcd} F[x] \arrow[dr, "ev_y"] & \subset & E[x] \arrow[d, "ev_y"] \\ F & \subset & E \end{tikzcd}$$

$f(y)=0$ in E

$ev_y(f(x))=0$

$\Rightarrow y$ is a root of $f(x)$. $\Rightarrow f(x)$ factors nontrivially in E.

$x-y \mid f(x)$, $f(x) = (x-y)g(x)$ $g(x) \in E[x]$

coefficients in E

$f(x) = x^2+1$ irreducible in $\mathbb{R}[x]$

$E = \mathbb{R}[y]/(y^2+1)$ or $\mathbb{R}[i]/(i^2+1)$ secretly $i = \sqrt{-1}$
$y = \sqrt{-1}$.

y constant in E, $f(y) = y^2+1 = 0$ in E $\Rightarrow$ y a root of $f(x)$ in E.

$f(x) = (x-y)(x+y)$ factors in E.

We enlarge our field of constants from F to $\overset{E}{\overset{\shortparallel}{F[y]/(f(y))}}$

$f(x)$ must be irreducible in F, otherwise E is not a field.

now y is a root of $f(x)$ in E, $x-y \mid f(x)$
$f(y) = 0$.

$f(x) = (x-y)\,g(x)$.