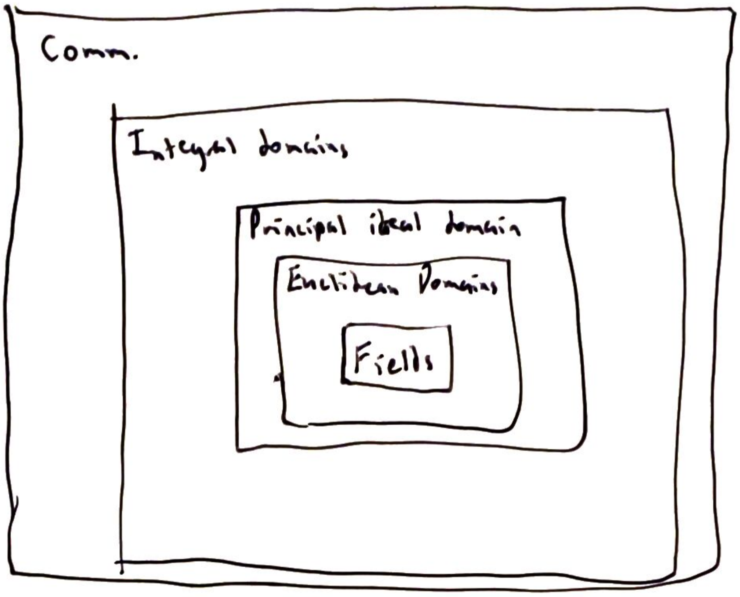
Week 6

Irreducibility and Factoring

Rings so far:



Principal ideal domains (PIDs):

Integral domains in which all ideals are principal, i.e. of the form $I=(d)$ for some $d\in R$

Ex: $\mathbb{Z}$

nonexample: $\mathbb{Z}[x]$

Euclidean domains: Integral domains for which there exists a Euclidean function $f: R\setminus\{0\} \to \mathbb{Z}_{\geq 0}$ such that for every $a,b\in R$, with $b\neq 0$ there are $q,r\in R$ with $a=qb+r$ and either $r=0$ or $f(r)<f(b)$

Ex: $\mathbb{Z}$, $\mathbb{Q}[x]$

non-example: $\mathbb{Z}[x]$

Proposition: Every Euclidean domain is a PID

proof: Suppose R is a Euclidean domain with Euclidean function $f:R\setminus\{0\}\to\mathbb{Z}_{\geq 0}$

Suppose $I\subseteq R$ is an ideal

If $I=\{0\}$, then $I=(0)$

Suppose I is nonzero. Look at $S=\{f(i): i\in I\setminus\{0\}\}$

There is a minimum in S, so take $d\in I$ with the minimum size

Claim: $I=(d)$

little proof: $(d)\subseteq I$ b/c $d\in I$ and I ideal

To show $I \subseteq (d)$, take any $i \in I$

wts: $i = qd$ for some $q \in R$ ($\Leftrightarrow$ $i \in (d)$)

By the division algorithm there are some $q, r \in R$ with

$i = qd + r$ and either $r = 0$ or $f(r) < f(d)$

If $r \neq 0$ then $r = i - qd \in I$ but $f(r) < f(d)$ violating minimality of $f(d)$.

So $i = qd \Rightarrow i \in (d)$

Then $I \subseteq (d)$ and thus $I = (d)$

So R is a PID

<u>Primes</u>: In an integral domain R:

An element $p \in R$ is prime if the ideal generated $(p) \subseteq R$ is a prime ideal

Observation: p is prime as an element $\Leftrightarrow$ (p) is a prime ideal

$\Leftrightarrow$ if $ab \in I \Rightarrow a \in I$ or $b \in I$

$\Leftrightarrow$ $ab = kp$ for some $k \in \mathbb{Z} \Rightarrow a = mp$ or $b = np$ $m, n \in \mathbb{Z}$

$\Leftrightarrow$ if $p \mid ab \Rightarrow p \mid a$ or $p \mid b$

<u>Irreducibility</u>: In any commutative ring R

<u>Def</u>: A nonzero, nonunit $r \in R$ is <u>reducible in R</u> if

$r = st$ for some nonunits $s, t \in R$

Otherwise r is called irreducible in R

Warning: Suppose $r \in R \subseteq S$ with R, S integral domains

then the reducibility of r depends on whether you're viewing $r \in R$ or $r \in S$

Reasons: 1. more elements in $S \Rightarrow$ more potential factors

2. more units in $S \Rightarrow$ elements $s, t \in R$ that were nonunits in R might be units in S

<u>Examples</u>: 1. $\mathbb{Z} \subseteq \mathbb{Q}$

2 is irreducible in $\mathbb{Z}$

2 is a unit in $\mathbb{Q}$ ($\Rightarrow$ neither reducible or irreducible in $\mathbb{Q}$)

2. $\mathbb{Z}[x] \subseteq \mathbb{Q}[x] \subseteq \mathbb{R}[x] \subseteq \mathbb{C}[x]$

$f(x) = 2x$ is reducible in $\mathbb{Z}[x]$

nonunits

$f(x) = 2x$ is irreducible in $\mathbb{Q}[x]$
$\uparrow$ unit

$g(x) = x^2 - 2$ is irreducible in $\mathbb{Z}[x]$

$g(x) = x^2 - 2$ is still irreducible in $\mathbb{Q}[x]$

$g(x) = x^2 - 2$ is reducible in $\mathbb{R}[x]$

What is the relationship between prime and irreducible in R?

A: (Proposition) In an integral domain R, every nonzero prime element is irreducible

proof: Suppose $p \in R \setminus \{0\}$ is prime (p is not a unit)

Suppose $p = st$ for some s, t. Then $p \mid s$ or $p \mid t$

WLOG: suppose $p \mid s$

so $s = kp \Rightarrow p = st = kpt$ (in domain, $p \neq 0$)

so $kt = 1 \Rightarrow t$ is a unit

Def: A unique factorization domain (UFD) is an integral domain R in which every nonzero nonunit can be written as a product $r = p_1 p_2 \cdots p_n$ where all p_i are irreducible in R, uniquely up to reordering and multiplication by units

Example (1):

$f(x) = 2x^2 - 8$ in $\mathbb{Z}[x]$

Factor in $\mathbb{Q}[x]$ $\quad f(x) = (2x-4)(x+2) = \underbrace{2}_{\text{unit in } \mathbb{Q}}(x-2)(x+2)$

both irreducible in $\mathbb{Q}[x]$

In $\mathbb{Z}[x]$ $\quad f(x) = \underbrace{(2x-4)}_{\text{reducible in } \mathbb{Z}}(x+2) = 2(x-2)(x+2)$

irreducible factors in $\mathbb{Z}[x]$

Gauss' Lemma: Suppose $p(x) \in \mathbb{Z}[x]$

Suppose $p(x) = A(x)B(x)$ for some nonconstant polynomials in $\mathbb{Q}[x]$

then there are $r, s \in \mathbb{Q}$ such that $rA(x), sB(x) \in \mathbb{Z}[x]$

and $p(x) = (rA(x))(sB(x))$

Corollary: 1) If $p(x)$ is reducible in $\mathbb{Q}[x]$ then its reducible in $\mathbb{Z}[x]$

2) If coeff. of $p(x)$ have gcd(1) then

$p(x)$ irred. in $\mathbb{Z}[x] \iff p(x)$ irred. in $\mathbb{Q}[x]$

proof: Suppose $p(x) = A(x)B(x)$

write $A(x) = \frac{c_0}{d_0} + \frac{c_1}{d_1}x + \dots + \frac{c_n}{d_n}x^n$

$B(x) = \frac{e_0}{f_0} + \frac{e_1}{f_1}x + \dots + \frac{e_m}{f_m}x^m$

where $c_i, d_i, e_i, f_i \in \mathbb{Z}$ and $d_i \neq 0 \neq f_i$

clear denominators with $d = d_0 d_1 \cdots d_n f_0 \cdots f_m$

then $dp(x) = \underbrace{(d_0 \cdots d_n A(x))}_{a(x) \in \mathbb{Z}[x]} \underbrace{(f_0 \cdots f_m B(x))}_{b(x) \in \mathbb{Z}[x]}$

want to cancel d from the left somehow

Fix: factor d in $\mathbb{Z}$

$d = p_1 p_2 \cdots p_k$ where p_i are primes in $\mathbb{Z}$

then $p_1 p_2 \cdots p_k\, p(x) = a(x) b(x)$

<u>Observation</u> $\mathbb{Z}[x] / (p_i)_{\mathbb{Z}[x]} \simeq \underbrace{\mathbb{Z}/(p_i)}_{\text{integral domain}}[x] \Rightarrow \mathbb{Z}/(p_i)[x]$ is an integral domain

so $\mathbb{Z}[x] / (p_i)\mathbb{Z}[x]$ is an integral domain

$\hookrightarrow$ p_i is prime in $\mathbb{Z}[x]$

WLOG: $p_1 \mid a(x) \Rightarrow a(x) = p_1 \alpha(x)$

$p_1 p_2 \cdots p_k\, p(x) = (\cancel{p_1} \alpha(x)) b(x)$

Repeat until $p(x) = \varsigma(x) \xi(x)$

for $\varsigma(x), \xi(x) \in \mathbb{Z}[x]$ ■

<u>Rational Roots Theorem</u>

Suppose $p(x) = c_0 + c_1 x + \dots + c_n x^n \in \mathbb{Z}[x]$ $c_n \neq 0$

If $\alpha = \frac{r}{s} \in \mathbb{Q}$ with $\gcd(r,s) = 1$, then $p(\alpha) = 0 \Rightarrow r \mid c_0$ & $s \mid c_n$

proof: Suppose $p(\alpha) = 0$ $p(\frac{r}{s}) = c_0 + c_1 \frac{r}{s} + \dots + c_n (\frac{r}{s})^n \underset{=0}{\in} \mathbb{Q}$

$\Rightarrow c_0 s^n + c_1 r s^{n-1} + \dots + c_n r^n = 0$ in $\mathbb{Z}$

$c_0 s^n = -c_1 r s^{n-1} - \dots - c_n r^n = r(-c_1 s^{n-1} - \dots - c_n r^{n-1})$ in $\mathbb{Z}$

so $r \mid c_0 s^n \Rightarrow r \mid c_0$

similarly, $c_n r^n = -c_0 s^n - c_1 r s^{n-1} - \dots - c_{n-1} r^{n-1} s$
$= s(-c_0 s^{n-1} - c_1 r s^{n-2} - \dots - c_{n-1} r^{n-1})$

so $s \mid c_n$

Example ①: $x^3 - 2x^2 + x - 1$

roots in $\mathbb{Q}$? $\alpha = \frac{r}{s}$ where $r \mid 1$, $s \mid 1$

$\Rightarrow r = \pm 1$, $s = \pm 1$ $\quad \alpha = \pm 1$

$f(1) \neq 0$ $\quad f(-1) \neq 0$ so no roots

Example ② (sad): $f(x) = 24x^4 + 2x^2 - 60$

roots $\alpha = \frac{r}{s} \Rightarrow r \mid (-60)$ $\quad s \mid 24$,

$r = \pm 1, 2, 3, 4, 5, 6, \dots$

$s = \pm 1, 2, 3, 4, \dots$

Q: Why look at roots?

The factor theorem: For a polynomial $f(x) \in F[x]$ with F a field, $\alpha \in F$ is a root of $f(x) \Leftrightarrow f(x) = (x-\alpha) g(x)$ in $F[x]$

Danger: If $\deg(f(x)) \leq 3$, then $f(x)$ irreducible in $F[x] \Leftrightarrow f(x)$ has no roots in $F[x]$

but if $\deg(f(x)) \geq 4$, then $f(x)$ has no linear factors in F $\Leftrightarrow$ $f(x)$ has no roots in F

proof: For any $\alpha \in F$, just divide $f(x)$ by $x - \alpha$

$f(x) = (x-\alpha) q(x) + r(x)$

where either $r(x) = 0$ or $\deg(r(x)) < \deg(x-\alpha) = 1 \Rightarrow r$ is const.

$f(\alpha) = (\alpha - \alpha) q(\alpha) + r_0 = 0$ if $r = 0$
$= r_0$ if $r \neq 0$

Factoring and irreducibility

so far: 1) Gauss' lemma: nonconstant factors of $f(x) \in \mathbb{Z}[x]$

$\updownarrow$

nonconstant factor of $f(x) \in \mathbb{Q}[x]$

2) Rational roots theorem: recipe for potential rational roots

$\hookrightarrow$ find linear factors in $\mathbb{Q}[x]$

$\hookrightarrow$ linear factors in $\mathbb{Z}[x]$

Brute force

HW #8a $f(x) = x^4 - 2x^3 + 2x^2 + x + 4$

linear factors? Use rational root theorem

A rational root $\alpha = \frac{r}{s}$ would satisfy $r \mid 4$ and $s \mid 1$

$r = \pm 1, \pm 2, \pm 4$ $s = \pm 1$

so $\alpha = 1, 2, 4$ $(\pm)$ test ... none are roots

no linear factors

quadratic factors?

Suppose it factored $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ in $\mathbb{Z}[x]$

$x^4 - 2x^3 + 2x^2 + x + 4 = x^4 + (a+c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd = 0$

$\Rightarrow$ ① $a + c = -2 \Rightarrow c = -2 - a$

② $ac + b + d = 2$

③ $ad + bc = 1$ in $\mathbb{Z}$

④ $bd = 4$

Notice ④ $bd = 4 \Rightarrow (b, d) = (1,4) (-1,-4), (2,2), (-2,-2), (4,1), (-4,-1)$

Tedious work ... found a solution

$a = 1$, $b = 1$, $c = -3$, $d = 4$

$f(x) = (x^2 + x + 1)(x^2 - 3x + 4)$

Polynomials in $\mathbb{Z}_p[x]$

Example ② Find irreducibles in $\mathbb{Z}_2[x]$

linear polynomials: $\boxed{x}$, $\boxed{x+1}$

quadratic polynomials: $x \cdot x = x^2$ $x(x+1) = x^2 + x$ $(x+1)(x+1) = x^2 + 1$

so $\boxed{x^2 + x + 1}$

cubic polynomials: $x \cdot x \cdot x = x^3$ $x \cdot x \cdot (x+1) = x^3 + x^2$ $x \cdot (x+1) \cdot (x+1) = x^3 + x$

$(x+1)(x+1)(x+1) = x^3 + x^2 + x + 1$ $x(x^2 + x + 1) = x^3 + x^2 + x$ $(x+1)(x^2 + x + 1) = x^3 + 1$

so what's left is $\boxed{x^3 + x^2 + 1}$ $\boxed{x^3 + x + 1}$

Test irreducibility in $\mathbb{Z}[x]$ by looking mod p

Idea: suppose $f(x) = c_n x^n + \dots + c_0$ in $\mathbb{Z}[x]$

Suppose p is prime and <u>doesn't</u> divide c_n

Suppose f(x) factored into nonconstant polynomials

$$f(x) = (d_m x^m + \dots + d_0)(e_k x^k + \dots + e_0)$$

then $d_m e_k = c_n$ and $p \nmid c_n$ so $p \nmid d_m$ and $p \nmid e_k$

this will also give factors in $\mathbb{Z}_p[x]$

we found

$$x^4 - 2x^3 + 2x^2 + x + 4 = (x^2+x+1)(x^2-3x+4)$$

mod 2: $x^4 + x = (x^2+x+1)(x^2+x)$

mod 3: $x^4 + -2x^3 + 2x^2 + x + 1 = (x^2+x+1)(x^2+1)$

If f(x) does not factor mod p then it does not factor in $\mathbb{Z}[x]$ into nonconstant polynomials

Ex (3) (lame)

$x^2 + 3x + 45$

Just need to check for linear factors

↳ could use R.R.T. or quadratic formula

look mod 2 $x^2 + x + 1$ is irreducible → we done

mod 3: x^2 is reducible (no useful info)

Ex (4) $f(x) = x^4 + 1$ in $\mathbb{Z}[x]$

Facts 1: irreducible in $\mathbb{Z}[x]$

2: f(x) is reducible mod p for every prime p

e.g. $p=2$ $x^4 + 1 = (x+1)^4$

<u>Eisenstein's criterion</u>

Suppose $f(x) = c_n x^n + \dots + c_1 x + c_0 \in \mathbb{Z}[x]$

suppose p is a prime such that

1) $p \nmid c_n$

2) $p \mid c_0, p \mid c_1, \dots, p \mid c_{n-1}$

3) $p^2 \nmid c_0$

Then f(x) cannot be factored into nonconstant polynomials in $\mathbb{Z}[x]$

(if gcd of all factors is 1, then its irreducible)

Ex (5) $f(x) = x^4 + 10x + 5$ in $\mathbb{Z}[x]$

$p=5$ divides 5 and 10 $\quad 5^2 \nmid 5$

$\xrightarrow[\text{Eisenstein}]{} f(x)$ is irreducible in $\mathbb{Z}[x]$

Ex (6) (Sneaky) $\quad \Phi_p = x^{p-1} + x^{p-2} + \dots + x + 1 = \dfrac{x^p - 1}{x-1}$ (cyclotomic polynomial)

look at $\quad \Phi_p(x+1) = f(x)$

$$= \frac{(x+1)^p - 1}{x+1-1} = \frac{x^p + \binom{p}{1}x^{p-1} + \dots + \binom{p}{p-1}x}{x}$$

$$= x^{p-1} + \underbrace{\binom{p}{1}x^{p-2} + \dots + \binom{p}{p-2}x + \binom{p}{p-1}}_{p \text{ divides all of these}}$$

Eisenstein: f is irreducible

so $f(x-1) = \Phi_p(x)$ is irreducible