2/17
Monday
week 5

Recall

Given a ring R and $a \in R$

$(a) = \{ax \mid x \in R\}$

Ex: What do the elements of $\mathbb{Z}[x]/(2)$ look like?

$$\mathbb{Z}[x] = \left\{ a_0 + a_1 x + \cdots + a_n x^n \;\middle|\; \underset{n \geq 0}{a_i \in \mathbb{Z}} \right\}$$

$$= \{0, 1, -1, 52, \ldots, x^2 - 10, 13x^{10072} + 10x^{101}, \ldots\}$$

$$(2) = \{\, 2f(x) \mid f(x) \in \mathbb{Z}[x] \,\}$$

$$= \{\, 2a_0 + 2a_1x + 2a_2x^2 + \cdots + 2a_nx^n \mid \overset{n\geq 0}{a_i \in \mathbb{Z}} \,\}$$

$$\mathbb{Z}[x]/(2) = \mathbb{Z}[x]/I$$

$$= \left\{ (a_0 + a_1x + \cdots + a_nx^n) + I \;\middle|\; \begin{matrix} a_i \in \{0,1\} \\ n \geq 0 \end{matrix} \right\}$$

$$\cong \mathbb{Z}_2[x]$$

Let $I = (2)$.

Pick $(5x^3 + 9x^2 - 2x + 7) + I \in \mathbb{Z}[x]/I$.

$$(5x^3 + 9x^2 - 2x + 7) + I = \left[(x^3 + x^2 + 1) + (4x^3 + 8x^2 - 2x + 6) \right] + I = (x^3 + x^2 + 1) + I$$

$2(2x^3 + 4x^2 - x + 3) \in (2) = I$

First iso thm (Another way)

$\pi : \mathbb{Z}[x] \to \mathbb{Z}_2[x]$

$\pi(a_0 + a_1x + \cdots + a_nx^n) = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n$

π is a homomorphism

$\ker(\pi) = (2) = I$

$\operatorname{im}(\pi) = \mathbb{Z}_2[x]$

$\mathbb{Z}[x]/I \cong \mathbb{Z}_2[x]$

8.1 – Euclidean domains

integral domain
commutative ring
$1 \neq 0$
no zero divisors

$\mathbb{Z}_+ = \{1, 2, 3, 4, \ldots\}$

Def: Let R be an integral domain. Any function $N : R \to \mathbb{Z}_+ \cup \{0\}$ with $N(0) = 0$ is called a norm on R.

Ex: $R = \mathbb{Z}$
$N(x) = |x|$

Ex: F is a field
$R = F[x]$

$$N(f(x)) = \begin{cases} 0, & f(x) \text{ is the zero poly.} \\ \deg(f), & \text{otherwise} \end{cases}$$

$N(x^3 - 5) = 3$, $N(0) = 0$, $N(1) = 0$

$(2) =$

Let

Pick

$(5x^3 +$

Def: An integral domain R is called a **Euclidean domain** if there is a norm N on R such that for any two elements $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ with

$$a = qb + r$$

and $r = 0$ or $N(r) < N(b)$.

Ex: $\mathbb{Z}$ is a Euclidean domain with $N(x) = |x|$.

Euclidean algorithm:

Given $a, b \in \mathbb{Z}$, $b \neq 0$, then there exist unique $q, r \in \mathbb{Z}$ with

$a = bq + r$ and $0 \leq r < |b|$

$0 \leq r$

$0 \leq |r| < |b|$

$0 \leq N(r) < N(b)$

Ex: $b = -5$, $a = 31$

$31 = (-6)(-5) + 1$

$q \quad b \quad + r$

$0 \leq |r| < |b|$

Ex: $b = -5$, $a = -31$

$-31 = (7)(-5) + 4$

$q \quad b \quad + r$

$0 \leq |r| < |b|$

Last time: Let F be a field.
Given $a(x), b(x) \in F[x]$, $b(x)$ is not the zero poly., then there exist $q(x), r(x) \in F[x]$

where

$$a(x) = b(x)q(x) + r(x)$$

and

$$r(x) = 0 \quad \text{or} \quad \deg(r(x)) < \deg(b(x)).$$

So, $F[x]$ is a Euclidean domain with $N(f) = \deg(f)$. Here $\deg(0) = 0$.

Prop: Every ideal in a Euclidean domain is principal.

I is principal if $I=(a)$ for some a.
$(a)=\{ar \mid r\in R\}$

Proof:

Let R be a Euclidean domain with norm N and I be an ideal of R.

If $I=\{0\}$, then $I=(0)=\{0\cdot r \mid r\in R\}$

Suppose $I\neq\{0\}$.

Let d be any nonzero element of I with minimal norm. [That is, $N(d)\leq N(x)$ for all $x\in I$, $x\neq 0$]

We claim that $I=(d)$.

Since I is an ideal and $d\in I$,

$(d)=\{dr \mid r\in R\}\subseteq I$

$d\in I$, $r\in R$ $\Rightarrow dr\in I$

So, $(d)\subseteq I$.

Ex: $R=\mathbb{Z}$, $N(x)=|x|$
$I=2\mathbb{Z}=\{\ldots,-4,-2,0,2,4,\ldots\}$
$d=2$ or $d=-2$

Ex: $R=F[x]$, $I=?$
$d=1$, $N(1)=0$ | $d=x^2+5$, $N(x^2+5)=2$

Why is $I \subseteq (d)$?

Let $a \in I$.

Since R is a Euclidean domain and $d \neq 0$ there exists $q, r \in R$ with $a = dq + r$ and $r = 0$ or $N(r) < N(d)$.

So, $r = \underbrace{a}_{\text{in } I} - \underbrace{dq}_{\substack{d \in I \\ q \in R}} \in I$. $\Rightarrow d \in I$

If $r \neq 0$, then we'd have $r \in I$ with $r \neq 0$ and $N(r) < N(d)$.

This would contradict the minimality of d.

So, $r = 0$.

Thus, $a = dq \in (d)$.

So, $I \subseteq (d)$.

Thus, $I = (d)$ is principal. ▨