Lecture 6:

Ideals (6.1–6.2):

Ex: We have seen before that

$$I = \{0, \pm 3, \pm 6, \pm 9, \dots\}$$

is a subring of $\mathbb{Z}$. Furthermore I has the following property:

$$a \in \mathbb{Z},\ b \in I \Rightarrow ab \in I$$

It also follows that

$$r \equiv s \pmod 3 \Leftrightarrow r - s \in I$$

Def (ideal): A subring I of R with the property

$$r \in R,\ a \in I \Rightarrow ra \in I \text{ and } ar \in I$$

is called an *ideal*.

Note: If R is commutative, then $ra \in I$ is sufficient.

Ex: $\{0_R\}$ and R are always ideals of R (trivial)

Ex: $\mathbb{Z}$ is a subring of $\mathbb{Q}$ but not an ideal.

E.g. $\underset{\in \mathbb{Q}}{\frac{1}{2}} \cdot \underset{\in \mathbb{Z}}{1} = \frac{1}{2} \notin \mathbb{Z}$.

Ex: $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$ subring of $M_2(\mathbb{R})$ (check!)

We see that

$$\begin{pmatrix} c & d \\ e & f \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ca+db & 0 \\ ea+fb & 0 \end{pmatrix} \in I,$$

but

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} c & d \\ e & f \end{pmatrix} = \begin{pmatrix} ac & ad \\ bc & bd \end{pmatrix} \notin I$$

I is not ideal (but is a left ideal though).

Theorem: Let $I \neq \emptyset$ be a subset of ring R. Then

$$I \text{ ideal} \Leftrightarrow \begin{cases} ① & a, b \in I \Rightarrow a - b \in I \\ ② & r \in R,\ a \in I \Rightarrow ra \in I,\ ar \in I \end{cases}$$

Proof: Almost immediate consequence of theorem for test of a subring. □

Theorem: If R is a commutative ring with identity and $c \in R$, then

$$I = \{rc;\ r \in R\} \text{ is an ideal.}$$

Proof: Theorem above: ① $r_1 c, r_2 c \in I \Rightarrow$

$\Rightarrow r_1 c - r_2 c = (r_1 - r_2)c \in I$

② $r_1 \in R,\ rc \in I \Rightarrow$

$\Rightarrow r_1(rc) = (r_1 r)c \in I$

and $(rc)r_1 \underset{\text{commutative}}{=} (r_1 r)c \in I$ □

Def: The ideal above is denoted (c) and is called the principal ideal generated by c.

Note: Since R has identity, it follows that $c \in (c)$.

Ex: $I = \{0, \pm 3, \pm 6, \pm 9, \dots\} \subseteq \mathbb{Z} \Rightarrow I = (3)$.

Note: Every ideal in $\mathbb{Z}$ is principal (exercise 38).

($\mathbb{Z}$ is an example of a so called principal ideal domain)

Ex*) $I = \{a_n x^n + \dots + a_1 x + a_0;\ a_0 \text{ is even}\} \subseteq \mathbb{Z}[x]$

is an ideal (check!). Is it principal?

Assume $I = (p(x))$. Then, since $2 = 2x^0 \in I$, it follows that $2 = q_1(x)p(x)$ for some $q_1(x) \in \mathbb{Z}[x]$. We then must have $p(x) = \pm 2$. On the other hand, since also $x = x + 0 \in I$, it follows that

$$x = q_2(x)p(x) = q_2(x) \cdot (\pm 2) \text{ for some } q_2(x) \in \mathbb{Z}[x].$$

Impossible! $\Rightarrow I$ not principal. □

Note: F field $\Rightarrow$ every ideal in $F[x]$ is principal (exercise 44)

Theorem: Let R be a commutative ring with identity, and let $c_1, c_2, \dots, c_n \in R$. Then

$$I = \{r_1 c_1 + r_2 c_2 + \dots + r_n c_n;\ r_i \in R\}$$

is an ideal.

Proof: Exercise

Def: The ideal above is said to be generated by $c_1, c_2, \dots, c_n$ and is written $(c_1, c_2, \dots, c_n)$.

For this reason the ideal is said to be finitely generated.

Ex: In Example *) above we have $I = (x, 2)$.

Def (Congruence): Let I be an ideal in R, and let $a, b \in R$.

$$a \equiv b \pmod I \overset{\text{def.}}{\Leftrightarrow} a - b \in I.$$

Note: Compare first example. Agrees with congruence in $\mathbb{Z}$ (and in $F[x]$).

It can be proven that $\equiv$ above is an equivalence relation on R, so we can construct equivalence classes $[a]$, $a \in R$, just as in $\mathbb{Z}$ and $F[x]$.

For congruence modulo ideals we will not use the notation $[a]$, but instead

$$a + I = \{b \in R;\ b \equiv a \pmod I\}.$$

We usually call the class $a + I$ a coset of I.

(Reason for notation: $b \equiv a \pmod I \Leftrightarrow b - a \in I$

$\Leftrightarrow b - a = i \Leftrightarrow b = a + i$ for some $i \in I$.)

Notation: $R/I = \{a + I,\ a \in R\}$,

i.e. R/I is the set of all cosets.

Ex: Consider the ideal

$$I = \{a_n x^n + \dots + a_1 x + a_0 \mid a_0 \text{ even}\} \subseteq \mathbb{Z}[x].$$

Assume $f(x) = b_m x^m + \dots + b_0 \in \mathbb{Z}[x]$.

Two cases:

(1) $2 \mid b_0 \Rightarrow f(x) \in I \Rightarrow f(x) + I = 0 + I$

(2) $2 \nmid b_0 \Rightarrow 2 \mid b_0 - 1 \Rightarrow f(x) - 1 \in I$

$\Rightarrow f(x) + I = 1 + I$

Conclusion $\mathbb{Z}[x]/I = \{0 + I, 1 + I\}$. □

We now introduce operations $+$ and $\cdot$ on R/I:

Def: $(a+I) + (b+I) = (a+b) + I$

$(a+I)\cdot(b+I) = (ab) + I$

Note: Operations can be proved to be well-defined.

Note2: To be able to define multiplication we really need that I is an ideal, not just an ordinary subring:

$$(a+i_1)(b+i_2) = ab + \underbrace{ai_2 + i_1 b + i_1 i_2}_{\text{we want this to belong to } I\,!}$$

Note3: Operations above agree with $\mathbb{Z}_n$ and $F[x]/(p(x))$ before.

> **Theorem:** (1) R/I with operations above is a ring.
> (2) R commutative $\Rightarrow R/I$ commutative
> (3) R has identity $1_R \Rightarrow R/I$ has identity $1_R + I$

Def: We say that R/I is the quotient ring or factor ring of R by I.

(We "factor out" I to obtain R/I.)

Note: I "large" $\Rightarrow R/I$ "small"

I "small" $\Rightarrow R/I$ "large"

Def (kernel): Let $f: R \to S$ be a homomorphism of rings. Then the set

$$K = \{ r \in R \,;\, f(r) = 0_S \}$$

is called the kernel of f and is written $\ker f$.

> **Theorem:** $\ker f$ is an ideal in R.

Proof: We make the "test" for ideals (prev. theorem).

$\ker f \neq \emptyset$, since $f(0_R) = 0_S$.

(1) $a, b \in \ker f \Rightarrow f(a-b) \underset{f \text{ hom.}}{=} f(a) - f(b) = 0_S - 0_S = 0_S$

$\Rightarrow a - b \in \ker f$

(2) $r \in R, a \in \ker f \Rightarrow f(ra) \underset{f \text{ hom.}}{=} f(r)f(a) = f(r)\cdot 0_S = 0_S$

$\Rightarrow ra \in \ker f$

Similarly $ar \in \ker f$. □

> **Theorem:** Let $f: R \to S$ be a homomorphism. Then
> f is injective $\Leftrightarrow \ker f = \{0_R\}$.

Proof: $\Rightarrow$) Let $a \in \ker f$. Then

$f(a) = 0_S = f(0_R) \underset{f \text{ injective}}{\Rightarrow} a = 0_R$

Conclusion $\ker f = \{0_R\}$.

$\Leftarrow$) $f(a) = f(b) \Rightarrow f(a-b) \underset{f \text{ hom.}}{=} f(a) - f(b) = 0_S$

$\Rightarrow a - b \in \ker f \underset{\ker f = \{0_R\}}{\Rightarrow} a - b = 0_R \Rightarrow a = b$

Conclusion f is injective. □

We can define a natural homomorphism

$$\pi : R \to R/I,$$

by $\pi(r) = r + I$. (A projection.)

> **Theorem:** π is a surjective homomorphism with $\ker \pi = I$.

Proof: Exercise.

> **Theorem (First isomorphism theorem):** If $f: R \to S$ is a surjective homomorphism, then
> $$R/\ker f \cong S.$$

Proof: We use the notation $K = \ker f$.

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\pi"'] & S \\ R/K \arrow[ur, dashed, "\varphi"'] & \end{tikzcd} \qquad (f = \varphi \circ \pi)$$

We define a mapping $\varphi : R/K \to S$ by

$$\boxed{\varphi(r + K) = f(r).}$$

Show that φ is an isomorphism:

- φ well-defined: $a + K = b + K \Rightarrow$
  $\Rightarrow a - b \in K \Rightarrow f(a-b) = 0_S \Rightarrow f(a) - f(b) = 0_S \Rightarrow$
  $\Rightarrow f(a) = f(b) \Rightarrow \varphi(a+K) = \varphi(b+K)$
- φ homomorphism: $\varphi((a+K)+(b+K)) = \varphi((a+b)+K) =$
  $= f(a+b) = f(a) + f(b) = \varphi(a+K) + \varphi(b+K)$
  and $\varphi((a+K)(b+K)) = \varphi((ab)+K) = f(ab) =$
  $= f(a)f(b) = \varphi(a+K)\varphi(b+K)$
- φ injective: $\varphi(a+K) = \varphi(b+K) \Rightarrow f(a) = f(b)$
  $\Rightarrow f(a) - f(b) = f(a-b) = 0_S \Rightarrow a - b \in K \Rightarrow$
  $\Rightarrow a + K = b + K$
- φ surjective: Follows from f surjective. □

Note: In case f not surjective, we instead have

$$R/\ker f \cong f(R) \quad \text{(subring of } S\text{)}.$$

Note2: $f(R)$ is called the image of f and is often written $\operatorname{im} f$.

Ex: Consider the homomorphism $f: \mathbb{Z} \to \mathbb{Z}_n$ defined by $f(a) = [a]$. Clearly f is surjective, and $f(a) = [0] \Leftrightarrow a = k \cdot n$ so $\ker f = (n)$.

F. Iso. Th $\Rightarrow$ $\mathbb{Z}_n \cong \mathbb{Z}/(n)$.

Ex: $\{\text{polynomials with constant term} = 0\} \subseteq \mathbb{Z}[x]$ is the same as the ideal (x) (check!)

Define $f: \mathbb{Z}[x] \to \mathbb{Z}$ by $f(a_n x^n + \cdots + a_0) = a_0$.
It follows that f is a surjective homomorphism (check!) and that $\ker f = (x)$.

F. Iso. Th. $\Rightarrow$ $\mathbb{Z} \cong \mathbb{Z}[x]/(x)$.