Chapter 6.3 part 2

Section 6.3

Generalizations (to an arbitrary commutative ring R with identity) of Th 2.8 and Th 5.10

Recall Th 2.8 & Th 5.10

$p \in \mathbb{Z}$ - integer or $p \in F[x]$ - non-constant polynomial (F is a field)

The following three conditions are equivalent:

(1) p is prime ⦚ p is irreducible

(2) $\mathbb{Z}_p = \mathbb{Z}/(p)$ is a field ⦚ $F[x]/(p)$ is a field

(3) $\mathbb{Z}_p = \mathbb{Z}/(p)$ is an integral domain ⦚ $F[x]/(p)$ is an integral domain

Both $\mathbb{Z}$ and $F[x]$ belong to a certain special class of rings.

For more general ring, such a theorem is not true.

<u>R is a commutative ring with identity</u>

We want to find a condition on an ideal $I \subseteq R$ which is an analog of being prime/irreducible for the generator if the ideal was principal.

There are 2 ways to do that.

(1') **Def** An ideal $P \subset R$ $(P \neq R)$ is said to be *prime* if $bc \in P$ implies $b \in P$ or $c \in P$ (or both)

irreducible $p \in F[x]$

Clearly, for a prime $p \in \mathbb{Z}$, the ideal (p) is prime.

Indeed, $bc \in (p)$ means $p | bc$ $\overset{\mathbb{Z}\ \text{Th 1.5}}{\underset{F[x]\ \text{Th 4.12 (b)}}{\text{implies}}}$ $p | b$ or $p | c$ (or both)

that is $b \in (p)$ or $c \in (c)$ (or both)

Th 6.14 [Equivalence of (1) and (3)]

An ideal $P \subset R$ is prime iff R/p is an integral domain

Ex 7 shows that R/p for a prime ideal P is not necessarily a field.

$R = \mathbb{Z}[x]$ $\quad P = (x)$

(1) P is a prime ideal

(2) $\mathbb{Z}[x]/(x)$ is not a field

Pf (1) Assume $ab \in (x)$ $\qquad$ Wanted: $a \in (x)$ or $b \in (x)$

$ab = xf \quad a, b, x, f \in \mathbb{Z}[x]$

Pick $x = 0$

$a(0)\, b(0) = 0$ $\qquad$ $a(0)$ and $b(0)$ are the constant terms of the polynomials a and b correspondingly

That implies $a(0) = 0$ or $b(0) = 0$

For a polynomial $c_0 + \dots + c_n x^n$, zero constant term implies either the polynomial is zero, or the polynomial is $x(c_1 + \dots + c_n x^{n-1})$

In either case, $c_0 + \dots + c_n x^n \in (x)$ provided $c_0 = 0$

That is either $a \in (x)$ or $b \in (x)$. The ideal $P = (x)$ is prime.

② $\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$ - not a field

Diet $f : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$

$a \longmapsto a(0) \leftarrow$ the constant term of a.

- homomorphism (from the definition of the operations of addition and multiplication on $\mathbb{Z}[x]$)
- $\ker f = (x)$
- surjective
- use the First Isomorphism Theorem to conclude

$$\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$$

(2) <u>Def</u> An ideal $M \subset R$ $(M \neq R)$ is said to be <u>maximal</u> if whenever $J \subset R$ is an ideal such that $M \subseteq J \subseteq R$, then $J = M$ or $J = R$ (not both).

No ideal J such that
$$M \subsetneq J \subsetneq R$$

For a prime $p \in \mathbb{Z}$, the ideal (p) is maximal.

Indeed let $(p) \subseteq J \subseteq \mathbb{Z}$.

Assume that $\underline{(p) \neq J}$: there exists $m \in J$, $m \notin (p)$
$p \nmid m$

$p \nmid m$, p is prime imply that $(p, m) = 1$ means $ap + bm = 1$ for some $a, b \in \mathbb{Z}$.

$$\left.\begin{array}{l} (p) \subseteq J \text{ implies } ap \in J \\ m \in J \text{ implies } bm \in J \end{array}\right\} \text{imply } ap + bm \in J, \text{ thus } 1 \in J \text{ implies } J = \mathbb{Z}$$

by the absorbtion property of J

Prop
If an ideal $I \subseteq R$ is such that there is a unit $u \in R$ which is an element of I, then $\underline{I = R}$.

Pf $u^{-1}u = 1_R$ and $u^{-1}u \in I$ by the absorbtion property of I. Thus $1_R \in I$. Again by the absorbtion property of I, for any $r \in R$, $r = r 1_R \in I$.

Th 6.15 [Equivalence of (1) and (2)]

Let M be an ideal in R.

M is maximal iff R/M is a field.

Cor 6.16 Every maximal ideal is prime.

Pf - Combine Th 6.15, Th 6.14, and the fact that every field is an integral domain

Example not every prime ideal is maximal

$R = \mathbb{Z}[x]$, $I = (x)$

$\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$ is an integral domain but not a field

From Th 6.14: (x) is a prime ideal in $\mathbb{Z}[x]$

From Th 6.15: (x) is not maximal in $\mathbb{Z}[x]$

For example (a lengthier argument)

$(x) \subset (2, x) \subset \mathbb{Z}[x]$