Chapter 6.2 part 1

Ideals in a ring R - subrings with absorbtion property.

Th 6.10 The kernel of a ring homomorphism is an ideal

Th 6.2 Let R be a commutative ring with identity, and $c \in R$.

$(c) = \{cr \mid r \in R\}$ is an ideal | Terminology: principal ideal

notation for the principal ideal generated by $c \in R$

Question Is any ideal the kernel of a ring homomorphism?

R - a ring, $R \supseteq I$ - an ideal in R.

Is there a ring S and a ring homomorphism $R \to S$ such that the kernel is I?

Examples $\mathbb{Z} \supset (n) = \{na \mid a \in \mathbb{Z}\}$ $n \neq 0, \pm 1$

We constructed (Chapter 2) the ring $\mathbb{Z}_n$, and it is easy to check that

the map $\mathbb{Z} \longrightarrow \mathbb{Z}_n$ is a homomorphism of rings

$a \longmapsto [a]$

The kernel is $\{a \in \mathbb{Z} \mid [a] = [0]\} = \{a \in \mathbb{Z} \mid a \equiv 0 \ (\mathrm{mod}\ n)\} = \{nb \mid b \in \mathbb{Z}\} = (n)$

We constructed (Chapter 5) the ring $F[x]/(p)$ $\Big\}$ F - a field, $p \in F[x]$ - non-constant

It is easy to check that

the map $F[x] \longrightarrow F[x]/(p)$ is a homomorphism of rings

$f \longmapsto [f]$

The kernel is $(p) = \{ q p \mid q \in F[x] \} \subset F[x]$

principal ideal in $F[x]$ generated by $p \in F[x]$

<u>Strategy to attack the question</u>

We start with a ring R and an ideal $I \subseteq R$ } as $(n) \subset \mathbb{Z}$, $(p) \subset F[x]$

Define congruence modulo the ideal such that this is an equivalence relation on R.

Let R/I to be the set of equivalence classes. } $\mathbb{Z}_n = \mathbb{Z}/(n)$, $F[x]/(p)$

Make R/I a ring by introducing the operations of addition and multiplication in a way such that

the map $R \longrightarrow R/I$ is a ring homomorphism

$a \longmapsto$ the equivalence class which contains a

The kernel automatically is I - the class which contains 0_R

Outline of an implementation of this strategy (mostly Section 6.2)

Congruence

$\mathbb{Z} \supset (n) = \{cn \mid c \in \mathbb{Z}\}$ $a \equiv b \pmod{n}$ meaning $n \mid (a-b)$ meaning $\underline{a-b \in (n)}$

$F[x] \supset (p) = \{cp \mid c \in F[x]\}$ $f \equiv g \pmod{p}$ meaning $p \mid (f-g)$ meaning $\underline{f-g \in (p)}$

Def R - a ring, $I \subseteq R$ is an ideal in R

For $a, b \in R$ we say $a \equiv b \pmod{I}$ iff $\underline{a-b \in I}$

Th 6.4 The relation $\equiv$ on R is an equivalence relation

Notation R/I is the set of equivalence classes } similar to $F[x]/(p)$

Terminology equivalence class is called coset } congruence classes residue classes

Notation A coset is typically written as

$a + I$ - absolutely standard } $[a]$

I - the ideal

$a \in R$ - a representative (an element of the coset / equivalence class)

$\underline{a + I = \{a + i \mid i \in I\}} \in R/I$ $(a+i) - (a+j) = i - j \in I$ since $i, j \in I$

Operations

$$(a+I)+(b+I) = (a+b)+I \qquad [a]+[b]=[a+b]$$

$$(a+I)(b+I) = ab+I \qquad [a][b]=[ab]$$

Th 6.8 These operations are well-defined

The proof is based on Th 6.5 which states essentially the same

To summarize:

Th 6.9 Let I be an ideal in a ring R. Then

(1) R/I with the operations defined above is a ring

(2) If R is commutative, then so is R/I

(3) If R has an identity $1_R \in R$, then so does $R/I \ni 1_R + I$

The desired homomorphism

Th 6.12 Let I be an ideal in a ring R. Then the map

$$\pi : R \longrightarrow R/I \qquad r \longmapsto r+I$$

is a surjective homomorphism of rings

$$F[x] \to F[x]/(p) \qquad f \longmapsto [f]$$

Terminology R/I - quotion ring (factor ring)

Clearly, the kernel of π is the class of 0_R, namely the coset $0_R + I$

$$\underline{0_R + I} = \{0_R + i \mid i \in I\} = \{i \mid i \in I\} = \underline{I}$$

A combination of Th 6.10 and Th 6.12 can be stated as follows: