14 Ideals and Factor Rings

Def A subring I of R is called a (two-sided) ideal of R if for every $r \in R$ and every $a \in I$ both ra and ar are in I

Theorem (Ideal Test)

A nonempty subset I of a ring R is an ideal of R if

1. $a-b \in I$ for any $a, b \in I$
2. $ra \in I$ and $ar \in I$ for any $a \in I$ and $r \in R$

Proof:

Clear from the definition of an ideal and the subring test

Ex For any ring R, $\{0\}$ and R are ideals of R

$\{0\}$ is called the trivial ideal

Ex For any $n \in \mathbb{Z}^+$ the set $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$ (show this)

Ex Let R be a commutative ring with unity and let $a \in R$

The set $\langle a \rangle = \{ra \mid r \in R\}$ is an ideal called the principal ideal generated by a.

Ex Let R be a commutative ring with unity and let $a_1, a_2, \ldots, a_n \in R$. Then

$$\langle a_1, a_2, \ldots, a_n \rangle = \{ r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \mid r_i \in R \}$$

is an ideal of R (show this) called the ideal generated by $a_1, a_2, \ldots, a_n$

Ex Let I be the subset of $\mathbb{Z}[x]$ of all polynomials with even constant term. Then I is an ideal of $\mathbb{Z}[x]$ and $I = \langle x, 2 \rangle$

Theorem

Let R be a ring and let I be a subring of R. The set of cosets $R/I = \{r+I \mid r \in R\}$ is a ring under the operations

$(s+I)+(t+I) = s+t+I$

$(s+I)(t+I) = st+I$

iff I is an ideal of R

Proof

($\Leftarrow$) Suppose I is an ideal of R

Since R is an abelian group under addition, therefore I is a normal subgroup of R and R/I is an abelian group. We must show that multiplication is well-defined on R/I

Once we show this, it will be clear that multiplication is associative and that multiplication is distributive over addition

We now show multiplication is well-defined.

Suppose $s+I = s'+I$
$t+I = t'+I$

where $s, s', t, t' \in R$

Then $s = s'+a$ and $t = t'+b$

where $a, b \in I$

$st = (s'+a)(t'+b) = s't'+at'+s'b+ab$

Since I is an ideal, therefore

$at', s'b, ab \in I$

So we get

$(s+I)(t+I) = st+I = s't'+I = (s'+I)(t'+I)$

So multiplication is well-defined

($\Longrightarrow$) Suppose I is not an ideal of R

Then there exist $a \in I$, $r \in R$ such that $ar \notin I$ or $ra \notin I$

Suppose $ra \notin I$ (the proof for the other case is similar)

$a + I = 0 + I$

$(r + I)(a + I) = ra + I$

$(r + I)(0 + I) = r0 + I = 0 + I$

But $ra + I \neq 0 + I$

because $ra \notin I$

so multiplication

is not well-defined

Ex $8\mathbb{Z}$ is an ideal of $\mathbb{Z}$ so $\mathbb{Z}/8\mathbb{Z}$ is a ring

$$(2+8\mathbb{Z})+(6+8\mathbb{Z}) = 0+8\mathbb{Z}$$

$$(2+8\mathbb{Z})(6+8\mathbb{Z}) = 4+8\mathbb{Z}$$

Ex $6\mathbb{Z}$ is and ideal of $2\mathbb{Z}$ so $2\mathbb{Z}/6\mathbb{Z} = \{0+6\mathbb{Z}, 2+6\mathbb{Z}, 4+6\mathbb{Z}\}$ is a ring

$$(4+6\mathbb{Z})+(4+6\mathbb{Z}) = 2+6\mathbb{Z}$$

$$(4+6\mathbb{Z})(4+6\mathbb{Z}) = 4+6\mathbb{Z}$$