3.3 Lecture 12: Factor Rings

Suppose that R is a ring and that I is a (two-sided) ideal of R. Then we can use R and I to create a new ring, called "the factor ring of R modulo I". This ring is denoted R/I (read "R mod I"), and its elements are certain subsets of R associated to I. The most well known examples are the rings $\mathbb{Z}/n\mathbb{Z}$, created from the ring $\mathbb{Z}$ of integers and its ideals.

Definition 41. *Let R be a ring and let I be a (two-sided) ideal of R. If $a \in R$, the* coset *of I in R determined by a is defined by*

$$a + I = \{a + r : r \in I\}.$$

So $a + I$ is a subset of R; it consists of all those elements of R that differ from a by an element of I. Note that $a + I$ does not generally have algebraic structure in its own right, it is typically not closed under the addition or multiplication of R.

We will show that the set of cosets of I in R is itself a ring, with addition and multiplication defined in terms of the operations of R.

NOTES

1. $a + I$ is a coset of the subgroup $(I, +)$ of the additive group of R.
2. Suppose $R = \mathbb{Z}$ and $I = \langle 5 \rangle = 5\mathbb{Z}$. Then

   $$2 + I = \{2 + 5n,\ n \in \mathbb{Z}\} = \{\dots, -3, 2, 7, 12, \dots\}.$$

   This is the congruence class of 2 modulo 5. So in $\mathbb{Z}$, the cosets of $n\mathbb{Z}$ in Z are the congruence classes modulo n - there is a finite number n of them and each has exactly one representative in the range $0, \dots, n-1$ (this is guaranteed by the division algorithm in $\mathbb{Z}$).
3. Let F be a field and let I be an ideal in $F[X]$. Then $I = \langle f(X) \rangle$ for some polynomial $f(X)$, by Lemma 40. If $g(X) \in F[X]$ then the coset $g(X) + I$ contains all those polynomials that differ from $g(X)$ by a multiple of $f(X)$.

   If F is infinite then the number of cosets of I in $F[X]$ is infinite but each has exactly one representative of degree less than that of $f(X)$. This is its remainder on division by $f(X)$.

   If F is finite (e.g. $F = \mathbb{Z}/p\mathbb{Z}$ for some prime p), then the number of cosets of I in $F[X]$is finite.

Lemma 42. *Let a and b be elements of a ring R in which I is a two-sided ideal. Then*

(i) If $a - b \in I$, $a + I = b + I$.

(ii) If $a - b \notin I$, the cosets $a + I$ and $b + I$ are disjoint subsets of R.

Proof: (i): Suppose $a - b \in I$ and let $x \in a + I$. Then $x = a + m$ for some $m \in I$ and we can write

$$x = a - b + b + m = b + (a - b) + m.$$

Since $a - b \in I$ and $m \in I$ this means $(a - b) + m \in I$ and so $x \in b + I$. Thus $a + I \subseteq b + I$.

Now $a - b$ belongs to I and so $b - a = -(a - b)$ does also. It then follows from the above argument that $b + I \subseteq a + I$. Thus $a + I = b + I$.

(ii) Suppose $a - b \notin I$ and let $c \in (a + I) \cap (b + I)$. Then

$$c = a + m_1 = b + m_2$$

where $m_1, m_2 \in I$. It follows that $a - b = m_2 - m_1$ which is a contradiction since $a - b \notin I$. □

Lemma 42 shows that the different cosets of I in R are disjoint subsets of R. We note that their union is all of R since every element a of R belongs to *some* coset of I in R : $a \in a + I$. The set of cosets of I in R is denoted R/I. We can define addition and multiplication in R/I as follows.

Let $a + I,\ b + I$ be cosets of I in R. We define their *sum* by

$$(a + I) + (b + I) = (a + b) + I.$$

Claim: This addition is well-defined.

What does this mean? Why would it not be "well-defined"?

What the claim is concerned with is the following : if $a + I = a_1 + I$ and $b + I = b_1 + I$, how do we know that $(a + b) + I = (a_1 + b_1) + I$? How do we know that the coset sum $(a + I) + (b + I)$ as defined above does not depend on the choice a and b of representatives of these cosets to be added in R?

PROOF OF CLAIM: Suppose

$$a + I = a_1 + I \text{ and } b + I = b_1 + I$$

for elements a_1, b_1 of R. Then $a - a_1 \in I$ and $b - b_1 \in I$, by Lemma 42. Hence $(a - a_1) + (b - b_1) = (a + b) - (a_1 + b_1)$ belongs to I. Thus

$$(a + b) + I = (a_1 + b_1) + I,$$

by Lemma 42 again.

Multiplication in R/I is defined by

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

for cosets $a + I$ and $b + I$ of I in R.

Claim: Multiplication is well-defined in R/I
(i.e. the coset $ab + I$ does not depend on the choice of representatives of $a + I$ and $b + I$).

PROOF OF CLAIM: Suppose that

$$a + I = a_1 + I \text{ and } b + I = b_1 + I$$

for elements a_1, b_1 of R. Then $a - a_1 \in I$ and $b - b_1 \in I$, by Lemma 42. We need to show that

$$ab + I = a_1 b_1 + I.$$

By Lemma 42, this means showing that $ab - a_1 b_1 \in I$. To see this observe that

$$\begin{aligned} ab - a_1 b_1 &= ab - a_1 b + a_1 b - a_1 b_1 \\ &= (a - a_1)b + a_1(b - b_1). \end{aligned}$$

Now since I is a two-sided ideal we know that $(a - a_1)b \in I$ and $a(b - b_1) \in I$. Thus

$$(a - a_1)b + a_1(b - b_1) = ab - a_1 b_1 \in I,$$

and this proves the claim. □

That addition and multiplication in R/I satisfy the ring axioms now follows from the fact that these axioms are satisfied in R. The ring R/I, with addition and multiplication defined as above, is called the *factor ring* "R modulo "I". Its zero element is I $(= 0_R + I)$ and its multiplicative identity is $1_R + I$.

NOTES:

1. The ring R/I has some properties in common with R. For example

- R/I is commutative if R is commutative.
- If u is a unit in R with inverse u^{-1}, then $u + I$ is a unit in R/I, with inverse $u^{-1} + I$.

2. However, R/I can be structurally quite different from R. For example, R/I can contain zero-divisors, even if R does not. It is also possible for R/I to be a field if R is not.

In the next section we will look at conditions on I under which R/I is an integral domain or a field, for a commutative ring R.