Introduction to Rings and Modules

Lecture 4, Wednesday April 19 2023

Ari Feiglin

4.1 The First Isomorphism Theorem

Theorem 4.1.1 (The First Isomorphism Theorem):

Suppose $f\colon R \longrightarrow S$ is a ring homomorphism, then there is a natural isomorphism

$$R/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$$

(in other words, $R/\mathrm{Ker}(f)$ and $\mathrm{Im}(f)$ are ring-isomorphic.)

Proof:

Let us take the group isomorphism between from $\mathrm{Im}(f)$ to $R/\mathrm{Ker}(f)$ (since they are also groups under their respective addition operations) $\varphi(b) = f^{-1}\{b\}$. Recall that if $f(a) = b$ then $\varphi(b) = a + \mathrm{Ker}(f)$. Now all we must show is that φ respects multiplication:

(1) $\varphi(1_S) = f^{-1}\{1_S\} = \{a \in R \mid f(a) = 1_S\} = 1_R + \mathrm{Ker}(f)$ which is the identity of the quotient group $R/\mathrm{Ker}(f)$.

(2) Now suppose $f(\alpha) = a$ and $f(\beta) = b$ then we must show that $\varphi(ab) = \varphi(a)\varphi(b)$, now since $\varphi(a)\varphi(b) = (\alpha + \mathrm{Ker}(f))(\beta + \mathrm{Ker}(f)) = \alpha\beta + \mathrm{Ker}(f)$. So we must show that this is equal to $\varphi(ab)$, which is equivalent to $f(\alpha\beta) = ab$, which is true since f is a ring homomorphism.

$\blacksquare$

Example 4.1.2:

Let us define $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}_n$ by $f(m) = [m]$, which we know is well-defined from group theory. f is obviously surjective and $\mathrm{Ker}(f) = n\mathbb{Z}$ so

$$Z_n = f(Z) \cong \mathbb{Z}/\mathrm{Ker}(f) = \mathbb{Z}/n\mathbb{Z}$$

So this classic equivalence is true for rings as well.

Definition 4.1.3:

Recall that Ra is the smallest left ideal containing a and aR is the smallest right ideal containing a. When R is commutative, $aR = Ra$ is the smallest (bidirectional) ideal containing a and is denoted (a). This is called the **ideal generated by a**.

Proposition 4.1.4:

If R is a ring and $f(x), g(x) \in R[x]$ such that the leading coefficient in $f(x)$ is 1 then there exists unique $q(x), r(x) \in R[x]$ such that $g(x) = q(x) \cdot f(x) + r(x)$ and the degree of $r(x)$ is less than that of $f(x)$.

Proof:

If the degree of g's is less than that of f's then we can take $r(x) = g(x)$ and $q(x) = 0$. Otherwise suppose

$$f(x) = \sum_{k=0}^{n} a_k x^k, \quad g(x) = \sum_{k=0}^{m} b_k x^k$$

where $a_n = 1$ and $n \leq m$. Then we have that $h(x) = g(x) - b_m x^{m-n} f(x)$ has degree $\leq m$ so proceeding inductively on m (the base case of $m = 0$ is trivial, as $g(x) = b$ and $f(x) = 1$ so $q(x) = b$ and $r(x) = 0$ satisfy) we have that $h(x) = q'(x)f(x) + r(x)$ where $r(x)$ has degree less than n. So

$$g(x) = \big(b_m x^{m-n} + q'(x)\big)f(x) + r(x)$$

as required.
If $q(x)f(x) + r(x) = q'(x)f(x) + r'(x)$ then $\big(q(x) - q'(x)\big)f(x) + \big(r(x) - r'(x)\big) = 0$ and since the degree of $r - r'$ is less than that of f's we must have that $q - q' = 0$ and so $r = r'$ as well so the decomposition is unique.

■

Example 4.1.5:

We claim that for a commutative ring R and any $a \in R$ we have

$$R[x] \big/ (x-a) \cong R$$

If $a = 0$ then by definition $(x) = \{x \cdot f(x) \mid f(x) \in R[x]\}$ which is the set of all polynomials without a free coefficient. Notice then that $f(x) - g(x) \in (x)$ if and only if they have the same free coefficient, so the quotient group intuitively should be the set of free coefficients, R.
To do this in general, we can look at the ring homomorphism $\mathrm{ev}_a \colon R[x] \longrightarrow R$ which is a homomorphism since R is commutative and whose kernel is

$$\mathrm{Ker}(\mathrm{ev}_a) = \{f \in R[x] \mid f(a) = 0\}$$

we claim that $\mathrm{Ker}(\mathrm{ev}_a) = (x-a)$. Suppose $f(x) \in (x-a)$ then $f(x) = (x-a)g(x)$ for $g(x) \in R[x]$ then $f(a) = 0$ so $f \in \mathrm{Ker}(\mathrm{ev}_a)$. And if $f \in \mathrm{Ker}(\mathrm{ev}_a)$ then we can divide f by $x - a$ due to our proposition above to get

$$f(x) = q(x)(x-a) + r$$

So $0 = r$ by plugging in $x = a$ (r is a scalar since the degree of f is 1) so we have that $f(x) = q(x)(x-a)$ and so $f(x) \in (x-a)$ as required.
So we have that

$$R[x] \big/ (x-a) = R[x] \big/ \mathrm{Ker}(\mathrm{ev}_a) \cong \mathrm{ev}_a(R[x]) = R$$

as required.

Proposition 4.1.6:

$$\mathbb{R}[x] \big/ (x^2+1) \cong \mathbb{C}$$

Proof:

We define $\varphi \colon \mathbb{R}[x] \longrightarrow \mathbb{C}$ where we evaluate the input polynomial at i, in other words $\varphi = \mathrm{ev}_i \circ \iota$ where $\iota \colon \mathbb{R} \longrightarrow \mathbb{C}$ is the inclusion homomorphism $\iota(x) = x$. ι is trivially a homomorphism and the composition of homomorphisms is a homomorphism. φ is surjective since $\varphi(a+bx) = a+bi$. Now we must prove $\mathrm{Ker}(\varphi) = (x^2+1)$. Suppose $f(x) \in (x^1+1)$ so $f(x) = g(x)(x^1+1)$ so $\varphi(f) = g(i) \cdot 0 = 0$ so $(x^1+1) \subseteq \mathrm{Ker}(\varphi)$. If $f(x) \in \mathrm{Ker}(\varphi)$ then by above $f(x)$ can be written as

$$f(x) = q(x)(x^2+1) + ax + b$$

Since $f(i) = 0$ we must have that $ai+b = 0$ which means $a = b = 0$ since they are real so we have that $f(x) = q(x)(x^1+1)$ so $f(x) \in (x^2+1)$. So we have that

$$\mathbb{R}[x] \big/ (x^2+1) = \mathbb{R}[x] \big/ \mathrm{Ker}(\varphi) \cong \varphi(\mathbb{R}[x]) = \mathbb{C}$$

■

Definition 4.1.7:

Similar to before, if R is commutative and I and J are ideals we define

$$IJ = \left\{ \sum_{n=1}^{N} i_n j_n \,\middle|\, i_n \in I, j_n \in J \right\}$$

This is obviously an ideal. We could generalize this and require I be a left ideal and J be a right ideal. Similarly $I + J = \{i + j \mid i \in I, j \in J\}$ is a (left or right) ideal if I and J are (left or right; but the same direction) ideals.

Definition 4.1.8:

Let R be a ring and I and J be (left or right) ideals. If $I + J = R$ then I and J are called **comaximal ideals**.

Theorem 4.1.9 (The Chinese Remainder Theorem):

Let R be a commutative ring and $I, J \trianglelefteq R$ be comaximal ideals. Then

$$R/IJ \cong R/I \times R/J$$

Proof:

We will focus on the homomorphism:

$$f\colon R \longrightarrow R/I \times R/J, \quad f(a) = (a + I, a + J)$$

in order to use the first isomorphism theorem, we must show that f is surjective and its kernel is IJ.
Since $R = I + J$ (they are comaximal), $1_R \in I + J$ so $1_R = i + j$ so

$$f(j) = (j + I, j + J) = (1_R + I, J) = \left(1_{R/I}, 0_{R/J}\right)$$

and similarly

$$f(i) = \left(0_{R/I}, 1_{R/J}\right)$$

so let $(a + I, b + J) \in R/I \times R/J$ then

$$f(aj + bi)f(a)f(j) + f(b)f(i) = (a + I, a + J)(1, 0) + (b + I, b + J)(0, 1) = (a + I, b + J)$$

so f is indeed surjective.
Now $a \in \mathrm{Ker}(f)$ if and only if

$$(a + I, a + J) = (I, J)$$

which is only if $a \in I \cap J$, so $\mathrm{Ker}(f) = I \cap J$. Now since for $i_n \in I$ and $j_n \in J$, $i_n j_n \in I \cap J$ since I and J are ideals so $IJ \subseteq I \cap J$. And if $a \in I \cap J$ then $a = 1_R \cdot a = (i + j)a = ia + ja$ since $a \in J$, $ia \in IJ$ and $a \in I$ so $ja \in IJ$ so $a = ia + ja \in IJ$. Thus $IJ = I \cap J$.o So $\mathrm{Ker}(f) = IJ$ as required.
Thus

$$R/IJ = R/\mathrm{Ker}(f) \cong f(R) = R/I \times R/J$$

■