LECTURE 16 22.03.2024

More on quotient rings

Let R be a ring and I be an ideal of R. The quotient ring is then given by $R/I = \{r+I : r \in R\}$. Also, there is a natural map $f : R \to R/I : r \mapsto r+I$.

What are the ideals of R/I ?

Let us consider the following two sets:

$A = \{J : J \text{ is an ideal of } R \text{ containing } I\}$

$B = \{K/I : K/I \text{ is an ideal of } R/I\}$

Claim: There is a one-one correspondence between these two sets, A and B.

Proof idea: (i) From A to B.

Take any $J \in A$. Define $F(J) = \{f(j) : j \in J\}$.

Of course $F(J) \subseteq R/I$. Let's see whether $F(J)$ forms an ideal of R/I.

(i) $F(J)$ forms a subgroup of R/I under addition.

- Let $a', b' \in F(J)$. Then there are $a, b \in J$ s.t. $f(a) = a'$ and $f(b) = b'$. Then, $a' + b' = f(a) + f(b) = f(a+b)$. Since $a+b \in J$, $a'+b' \in F(J)$.
- Associativity follows from the associativity of $+$ in the ring R.
- Identity element is I (check!)
- Inverse of $a' = f(a) = a+I$ is $-a+I$ (As, $-a$ is in J for all $a \in J$, J being an ideal of R).

(ii) Take any $r+I \in R/I$ and $a+I \in F(J)$. To show that $(r+I).(a+I) \in F(J)$, that is, $r.a + I \in F(J)$.

Since, $a+I \in F(J)$, $a \in J$ and so $r.a \in J$, so $r.a + I \in F(J)$.

Thus, $F(J)$ forms an ideal of R/I.

(2) From B to A

Let J' be an ideal of R/I. We need to find an ideal J of R containing I, s.t. $J' = J/I$. Let us define J as follows: $J = \{ j : j + I \in J' \}$, that is, $J = f^{-1}(J') = \{ a \in R : f(a) \in J' \}$.

(i) Does J contain I?

Take any $a \in I$. To show that $a \in J$, that is $f(a) \in J'$. Now, $f(a) = a + I = I$.

Now, I is the zero element of R/I and J' is an ideal of R/I. So, $I \in J'$.

Then, $f(a) \in J'$ and so, $a \in f^{-1}(J') = J$.

Hence, $I \subseteq J$.

(2) J is an ideal of R.

T.P. (i) J is a subgroup of R under addition.

(ii) Take $r \in R$, $a \in J$. Then $r.a \in J$.

Proof is done in the

This gives us the one-one correspondence between A and B.

An application of this correspondence

Let R be ring and I be an ideal of R. We have the quotient ring R/I. We also have a surjective homomorphism from R to R/I. Similarly, we have a surjective homomorphism from R/I to $\dfrac{R/I}{J/I}$, where J is an ideal of R containing I. Consider:

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[dr, "g := f' \circ f"'] & R/I \arrow[d, "f'"] \\ & \dfrac{R/I}{J/I} \end{tikzcd}$$

Let $g = f' \circ f$. Then g gives a surjective homomorphism from R to $R/I \big/ J/I$.

Then we have :

$$R/\ker g \cong R/I \big/ J/I$$

<u>What is $\ker g$?</u>

H.W. Check that $\ker g = J$.

We then have :

$$\boxed{R/J \cong R/I \big/ J/I}$$

<u>We happens if a quotient ring R/I is a field (another application)?</u>

Suppose R/I is a field. Then it has only two ideals I and R/I. It follows that there is no proper ideal J of R s.t. $I \subsetneq J \subsetneq R$. Such an ideal is said to be a maximal ideal of R. Also, it follows that if I is a maximal ideal of R, then the only possible ideals of R/I are I and R/I. Then R/I forms a field. Thus we have proved the following theorem:

Theorem: Let R be a ring and I be an ideal of R. Then R/I is a field iff I is a maximal ideal of R.

Adjoining elements to a ring.

Let R be a ring and let α be some element. Our target is to find a ring R', say which contains R and α and is the smallest such ring.

Consider $R' = R[\alpha]$.

$$= \{ r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_n\alpha^n : r_i \in R \text{ for each } i, n \geq 0 \}.$$

H.W. Check that $R[\alpha]$ forms a ring and it is the smallest ring containing R and α.

Examples.

1. if $\alpha \in R$, then $R[\alpha] = R$.
2. if α is not a root of any polynomial over R, then $R[\alpha] \cong R[x]$.
3. if α is a root of a monic polynomial of minimal degree, n, say over R then what can we say about $R[\alpha]$?

We claim that:

$$R[\alpha] = \{ r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_{n-1}\alpha^{n-1} : r_i \in R \text{ for all } i, \ 0 \leq i \leq n-1 \}.$$

This is true because: for some polynomial $f(x)$ over R, we have $f(\alpha) = 0$, that is

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0.$$

So, $\alpha^n = -(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1})$

Thus we have $R[\alpha]$ as above.

In particular we have:

$$R[\alpha] \cong R^n \quad \text{(as abelian groups)}.$$

Example:

- $R = \mathbb{Z}$, $\alpha = i$, consider the monic polynomial x^2+1 over $\mathbb{Z}$.

So, $\mathbb{Z}[i] = \{ z_0 + z_1 i : z_0, z_1 \in \mathbb{Z} \}$

$$\cong \mathbb{Z}^2 \quad \text{(as abelian groups)}.$$

Back to $R[\alpha]$

Continuing our discussion on $R[\alpha]$ where α is a root of a monic polynomial of minimal degree n, say, we can consider the ideal generated by $f(x)$, $(f(x))$. Now, any $h(x) \in R[x]$

can be written as $h(x) = q(x) \cdot f(x) + r(x)$, where $\text{degree}(r) < \text{degree}(f)$.

So, we can consider the quotient ring $R[x] / (f(x)) \cong R[\alpha]$ (as rings).

H.W. (i) Show $R[\alpha] \cong R^n$ (as abelian groups)

(ii) Show $R[x] / (f(x)) \cong R[\alpha]$ (as rings)

[α is a root of the monic polynomial $f(x)$, say, of minimal degree n, say.]

Example (continuing):

$\mathbb{Z}[i] \underset{\text{[as ring]}}{\cong} \mathbb{Z}[x] / (x^2+1) \underset{\text{[as abelian group]}}{\cong} \mathbb{Z}^2$, where

i is a root of the monic polynomial x^2+1 over $\mathbb{Z}$.