MTH302: INTEGERS, POLYNOMIALS AND MATRICES
LECTURE 3

VARADHARAJ R. SRINIVASAN

*K*eywords: Boolean ring, opposite ring, direct products, characteristic of a ring.

1. OPPOSITE RING AND BOOLEAN RING

Opposite ring: Let $(R, +, \cdot)$ be a ring. On R, define addition and multiplication as follows: $a \dotplus b = a + b$ and $a * b = b \cdot a$. Then $R^0 := (R, \dotplus, *)$ forms a ring called the *opposite ring*[1] of R. Clearly, $(R^0)^0 = R$.

Idempotents: Let R be a ring. An element $a \in R$ is called an *idempotent* of R if $a^2 = a$. The elements 0 and 1 (if 1 exists) are called the *trivial idempotents*.

Boolean Ring: A ring R is called a *Boolean* ring if every element of R is an idempotent.

2. DIRECT PRODUCTS

Let R and S be rings. Form the Cartesian product $R \times S := \{(r, s) \mid r \in R, s \in S\}$. Then $R \times S$ forms a ring, which we call the *direct product* of rings R and S, under the following operation:

Addition: $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$
Multiplication: $(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$.

The additive identity is $(0, 0)$, the additive inverse of (r, s) is $(-r, -s)$. If R and S are rings with 1 then multiplicative identity $1_{R\times S} = (1_R, 1_S)$. If $I = \{1, 2, \cdots, n\}$ and $R_1, \cdots, R_n$ are rings then the product

$$\prod_{i=1}^{n} R_i = \{(r_1, \cdots, r_n) \mid r_i \in R_i\}$$

is a ring under the *coordinate-wise addition* $(r_1, \cdots, r_n) + (s_1, \cdots, s_n) = (r_1 + s_1, \cdots, r_n + s_n)$ and *coordinate-wise multiplication* $(r_1, \cdots, r_n) \cdot (s_1, \cdots, s_n) = (r_1 \cdot s_1, \cdots, r_n \cdot s_n)$.

In general, for a nonempty set I and a family of rings $\{R_\alpha \mid \alpha \in I\}$, we define direct product as follows: Let

$$\prod_{\alpha \in I} R_\alpha = \{f : I \to \cup_{\alpha \in I} R_\alpha \mid f \text{ is a function such that } f(\alpha) \in R_\alpha\}.$$

Addition: $(f + g)(\alpha) = f(\alpha) + g(\alpha)$.
Multiplication: $(f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha)$.

[1] Addition operation remains the same and the order of multiplication is reversed.

It is easy to show that $\prod_{\alpha \in I} R_\alpha$ is a ring. An element $f \in \prod_{\alpha \in I} R_\alpha$ will be denoted by (r_α) if $f(\alpha) = r_\alpha$ for all $\alpha \in I$.

Direct Sum: Let $\{R_\alpha \mid \alpha \in I\}$ be a family of rings. The subset

$$\bigoplus_{i \in I} R_i := \{(r_\alpha) \in \prod_{\alpha \in I} R_\alpha \,\Big|\, r_\alpha = 0 \text{ for all but finitely many } \alpha\}$$

forms a subring of $\prod_{\alpha \in I} R_\alpha$ and is called the *direct sum* of the family of rings $\{R_\alpha \mid \alpha \in I\}$.

If I is an infinite set then direct sum and direct product of a family of rings need not be equal (as sets).

Example.

(1) Let $F = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $I = \{1, 2, \cdots, n\}$ and for each i, $R_i = F$ be the ring of real numbers. Then $F^n = \prod_{i=1}^n R_i$ is a ring under the coordinate-wise addition and multiplication.

3. Characteristic of a Ring

Characteristic of a Ring: Let $n \in \mathbb{N}$. A ring R is said to of characteristic n, denoted by $char(R) = n$, if n is the least positive integer such that $na = 0$ for all $a \in R$. If no such n exists for a ring R then R is said to be of characteristic 0.

Remark 3.1. If R is a ring with 1 then $char(R) = n$ if and only if $n1 = 0$.

Examples.

(1) The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are of characteristic 0.
(2) The ring $\mathbb{Z}_n$ is of characteristic n.
(3) Let R be a Boolean ring having at least two elements. Then $a + a = (a + a)^2 = a^2 + a + a + a^2 = a + a + a + a$. Thus $2a = a + a = 0$ for all $a \in R$ and this implies $char(R) = 2$.

Theorem 3.2. *If R is an integral domain of characteristic $n \neq 0$ then n is a prime number.*

Proof. Suppose that n is not prime and write $n = pm$ for $2 \leq p, m \leq n - 1$. There are elements $a, b \in R$ such that $pa \neq 0$ and $mb \neq 0$ (why?). Since R is an integral domain, $(pa) \cdot (mb) \neq 0$. Now, $n(a \cdot b) = (pm)(a \cdot b) = (pa) \cdot (mb) \neq 0$. This contradicts the fact that $char(R) = n$. □

Theorem 3.3. *Suppose that R is a ring with 1 such that the set of all nonunits in R forms a subgroup of $(R, +)$. Then $char(R) = 0$ or $char(R)$ is a power of a prime number.*

Proof. Let $char(R) \neq 0$ and suppose that there are two distinct prime numbers p, q dividing $n = char(R)$. Then $n = pqm$ for some $2 \leq m \leq n - 1$. We know that $p1_R \neq 0$, $qm1_R \neq 0$ and $pm1_R \neq 0$ (why?). Since $0 = n1_R = pqm1_R$, we obtain

$$\begin{aligned} 0 &= (p1_R) \cdot (qm1_R) \\ &= (q1_R) \cdot (pm1_R). \end{aligned}$$

Thus $p1_R$ and $q1_R$, being zero-divisors, are nonunits. Since the set of all nonunits forms a subgroup of $(R, +)$, we have $l(p1_R) + k(q1_R)$ is a nonunit for any $l, k \in \mathbb{Z}$.

Choose integers l, k such that $pl + qk = 1$ (why such l, k exist?). Then $1_R = 11_R = (pl + qk)1_R = l(p1_R) + k(q1_R)$ becomes a nonunit, which is absurd! Thus n has only one prime divisor, which makes $n = p^t$ for some $t \in \mathbb{N}$. $\square$