Course 11: 10.05.2021

2.6 The characteristic of a ring

Throughout this section, R will be a commutative ring with identity $1 \neq 0$. Then $(R, +)$ is an abelian group and we may talk about the order of an element $a \in R$. Recall that $a \in R$ has finite order if $\exists n \in \mathbb{N}^*$ such that $n \cdot a = 0$. If a has finite order, then:

$$ord(a) = min\{k \in \mathbb{N}^* \mid k \cdot a = 0\}.$$

Otherwise, we write $ord(a) = \infty$.

Definition 2.6.1 The order of the identity element 1 of R in the group $(R, +)$ is called the *characteristic* of R, and is denoted by $char(R)$.

Remark 2.6.2 (1) $char(R) = n \in \mathbb{N}^* \Leftrightarrow [n \cdot 1 = 0$ and $\forall m \in \mathbb{N}^*$ such that $m \cdot 1 = 0$ we have $n \leq m]$.

(2) Using a result from Group Theory, if $char(R) = n \in \mathbb{N}^*$ and $m \in \mathbb{Z}$, then:

$$m \cdot 1 = 0 \Leftrightarrow n|m \Leftrightarrow m \in n\mathbb{Z}.$$

(3) If $char(R) = n \in \mathbb{N}^*$, then $n \cdot a = 0$ for every $a \in R$. Indeed, we have:

$$n \cdot a = n \cdot (1 \cdot a) = (n \cdot 1) \cdot a = 0 \cdot a = 0.$$

(4) $char(R) = \infty \Leftrightarrow$ the elements $m \cdot 1$ with $m \in \mathbb{Z}$ are distinct.

Example 2.6.3 (a) $char(\mathbb{Z}) = char(\mathbb{Q}) = char(\mathbb{R}) = char(\mathbb{C}) = \infty$.

(b) Let $n \in \mathbb{N}$, $n \geq 2$. Then $char(\mathbb{Z}_n) = char(\mathbb{Z}_n[X]) = n$.

Theorem 2.6.4 *Let $a \in R^*$ be an element which is not a zero divisor in R. Then $char(R)$ is the order of a in the group $(R, +)$.*

Proof. If $ord(a) = \infty$, then $m \cdot a \neq 0$ for every $m \in \mathbb{N}^*$. We have:

$$m \cdot a \neq 0 \Leftrightarrow m \cdot (1 \cdot a) \neq 0 \Leftrightarrow (m \cdot 1) \cdot a \neq 0 \Leftrightarrow m \cdot 1 \neq 0.$$

Hence $char(R) = ord(1) = \infty$.

If $ord(a) = m \in \mathbb{N}^*$, then $m \cdot a = 0$. We have:

$$m \cdot a = 0 \Leftrightarrow m \cdot (1 \cdot a) \Leftrightarrow (m \cdot 1) \cdot a = 0 \Leftrightarrow m \cdot 1 = 0.$$

Hence $char(R) = ord(1)$ is finite, say $char(R) = n$, and we have $n \leq m$. But by Remark 2.6.2 (3), we also have $n \cdot a = 0$. Then it follows that $m \leq n$, because $ord(a) = m$. Hence we have $n = m$, and so $char(R) = ord(a)$.

Theorem 2.6.5 *Assume that R has no zero divisor. Then $char(R)$ is either a prime number or infinite.*

Proof. If $char(R) = \infty$, then we are done. Suppose that $char(R) = n = m \cdot k$ for some natural numbers $m, k > 1$. We have:

$$char(R) = n \Rightarrow n \cdot 1 = 0 \Rightarrow (m \cdot k) \cdot 1 = 0 \Rightarrow (m \cdot 1) \cdot (k \cdot 1) = 0.$$

But R has no zero divisor, hence we have $m \cdot 1 = 0$ or $k \cdot 1 = 0$. This contradicts the fact that $char(R) = n$. Hence $char(R) = n$ is a prime number.

Corollary 2.6.6 *Assume that R is an integral domain or a field. Then $char(R)$ is either a prime number or infinite.*

Theorem 2.6.7 *There exists a unique unitary ring homomorphism $f : \mathbb{Z} \to R$, which is defined by $f(m) = m \cdot 1'$ for every $m \in \mathbb{Z}$, where $1'$ denotes the identity element of R.*

If $char(R) = \infty$, then f is injective. If $char(R) = n \in \mathbb{N}^*$, then $Ker\, f = n\mathbb{Z}$.

Proof. We first show that if f does exist, then it is unique. So, suppose that $f : \mathbb{Z} \to R$ is a unitary ring homomorphism. Then $f(0) = 0' = 0 \cdot 1'$, where $0'$ is the zero element of R. For every $k \in \mathbb{N}^*$, we have:

$$f(k) = f(\underbrace{1 + \cdots + 1}_{k \text{ times}}) = \underbrace{f(1) + \cdots + f(1)}_{k \text{ times}} = \underbrace{1' + \cdots + 1'}_{k \text{ times}} = k \cdot 1',$$

$$f(-k) = -f(k) = -(k \cdot 1') = (-k) \cdot 1'.$$

Hence $f(m) = m \cdot 1'$ for every $m \in \mathbb{Z}$.

Now we show that the function f defined in the statement of the theorem is a unitary ring homomorphism. For every $m, n \in \mathbb{Z}$, we have:

$$f(m + n) = (m + n) \cdot 1' = m \cdot 1' + n \cdot 1' = f(m) + f(n),$$

$$f(m \cdot n) = (m \cdot n) \cdot 1' = (m \cdot 1') \cdot (n \cdot 1') = f(m) \cdot f(n)$$

and $f(1) = 1 \cdot 1' = 1'$. Hence f is a unitary ring homomorphism.

Assume that $char(R) = \infty$. If $f(m) = f(n)$, then $m \cdot 1' = n \cdot 1'$, which implies that $m = n$ by Remark 2.6.2 (4). Hence f is injective.

Assume that $char(R) = n \in \mathbb{N}^*$. Then we have:

$$Ker\, f = \{m \in \mathbb{Z} \mid f(m) = 0'\} = \{m \in \mathbb{Z} \mid m \cdot 1' = 0'\} = n\mathbb{Z}$$

by Remark 2.6.2 (2).

Corollary 2.6.8 *(i) Assume that $char(R) = \infty$. Then R has a subring isomorphic to $\mathbb{Z}$, and so $\mathbb{Z}$ is the smallest unitary ring with infinite characteristic.*

(ii) Assume that $char(R) = n \in \mathbb{N}^*$. Then R has a subring isomorphic to $\mathbb{Z}_n$, and so $\mathbb{Z}_n$ is the smallest unitary ring with characteristic n.

Proof. By Theorem 2.6.7, there exists a unique unitary ring homomorphism $f : \mathbb{Z} \to R$. By the first isomorphism theorem for rings, we have $\mathbb{Z}/Ker\, f \cong Im\, f$ and $Im\, f$ is a subring of R.

(i) If $char(R) = \infty$, then f is injective by Theorem 2.6.7, and so $Ker\, f = \{0\}$. Hence

$$\mathbb{Z} \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}/Ker\, f \cong Im\, f,$$

and so R has the subring $Im\, f$ isomorphic to $\mathbb{Z}$.

(ii) If $char(R) = n \in \mathbb{R}^*$, then $Ker\, f = n\mathbb{Z}$ by Theorem 2.6.7. Hence

$$\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/Ker\, f \cong Im\, f,$$

and so R has the subring $Im\, f$ isomorphic to $\mathbb{Z}_n$.

2.7 Polynomial rings

Throughout this section, R will be a commutative ring with identity.

Consider the set $R^{\mathbb{N}}$ of all functions with domain $\mathbb{N}$ and codomain R. For each $i \in \mathbb{N}$ and each $f \in R^{\mathbb{N}}$, we denote $a_i = f(i)$. Thus, $R^{\mathbb{N}}$ can be seen as the set of all sequences of elements of R.

Let $f = (a_0, a_1, \dots, a_n, \dots)$, $g = (b_0, b_1, \dots, b_n, \dots) \in R^{\mathbb{N}}$. Clearly,

$$f = g \iff a_i = b_i\,,\ \forall i \in \mathbb{N}\,.$$

We are going to define a ring structure on $R^{\mathbb{N}}$. For every $f = (a_0, a_1, \dots, a_n, \dots)$, $g = (b_0, b_1, \dots, b_n, \dots) \in R^{\mathbb{N}}$, we define the addition and the multiplication by:

$$f + g = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, \dots)\,,$$

$$f \cdot g = (c_0, c_1, \dots, c_n, \dots)\,,$$

where

$$c_n = \sum_{i=0}^{n} a_i b_{n-i}\,.$$

Definition 2.7.1 Let $f = (a_0, a_1, \dots, a_n, \dots) \in R^{\mathbb{N}}$. The set of natural numbers

$$supp(f) = \{i \in \mathbb{N} \mid a_i \neq 0\}$$

is called the *support* of f.

We denote

$$R^{(\mathbb{N})} = \{f \in R^{\mathbb{N}} \mid supp(f) \text{ is finite}\}.$$

Theorem 2.7.2 *(i)* $(R^{\mathbb{N}}, +, \cdot)$ *is a commutative ring with identity, called the* ring of formal series with coefficients in R.

(ii) $R^{(\mathbb{N})}$ *is a subring of* $R^{\mathbb{N}}$*, called the* ring of polynomials with coefficients in R.

(iii) The function $\varphi : R \to R^{(\mathbb{N})}$ *defined by* $\varphi(a) = (a, 0, \dots)$, $\forall a \in R$, *is an injective unitary ring homomorphism.*

Proof. (i) It is easy to check that $(R^{\mathbb{N}}, +)$ is an abelian group. The identity is $(0, 0, \dots)$ and the symmetric of $f = (a_0, a_1, \dots, a_n, \dots) \in R^{\mathbb{N}}$ is $-f = (-a_0, -a_1, \dots, -a_n, \dots) \in R^{\mathbb{N}}$.

Also, $(R^{\mathbb{N}}, \cdot)$ is a commutative monoid, where the identity element is $(1, 0, \dots)$.

Finally, let us check the distributive law, that is, $\forall f, g, h \in R^{\mathbb{N}}$,

$$f \cdot (g + h) = f \cdot g + f \cdot h\,.$$

Let $f = (a_0, a_1, \dots)$, $g = (b_0, b_1, \dots)$, $h = (c_0, c_1, \dots) \in R^{\mathbb{N}}$. Then $f \cdot (g+h) = (d_0, d_1, \dots, d_n, \dots)$, where

$$\begin{aligned} d_n &= \sum_{i=0}^{n} a_i \cdot (b_{n-i} + c_{n-i}) \\ &= \sum_{i=0}^{n} (a_i \cdot b_{n-i} + a_i \cdot c_{n-i}) \\ &= \sum_{i=0}^{n} a_i \cdot b_{n-i} + \sum_{i=0}^{n} a_i \cdot c_{n-i}\,. \end{aligned}$$

Using the definition of multiplication for $f \cdot g$ and $f \cdot h$, it follows that $f \cdot (g + h) = f \cdot g + f \cdot h$.

(ii) We have $(0, 0, \dots) \in R^{(\mathbb{N})} \neq \emptyset$. Let $f = (a_0, a_1, \dots), g = (b_0, b_1, \dots) \in R^{(\mathbb{N})}$.

If $f = 0$ or $g = 0$, then we clearly have $f - g, f \cdot g \in R^{(\mathbb{N})}$.

Next suppose that $f \neq 0$ and $g \neq 0$. Then $\exists m, n \in \mathbb{N}$ such that $f = (a_0, a_1, \dots, a_n, 0, \dots)$ with $a_n \neq 0$ and $g = (b_0, b_1, \dots, b_m, 0, \dots)$ with $b_m \neq 0$. Then $a_i - b_i = 0$ for $i > max(m, n)$, hence

$$supp(f - g) \subseteq \{0, 1, \dots, max(m, n)\}$$

is finite, and so $f - g \in R^{(\mathbb{N})}$. Also, we have $f \cdot g = (c_0, c_1, \dots, c_{m+n}, 0, \dots)$, where $c_{m+n} = a_n \cdot b_m$. Hence

$$supp(f \cdot g) \subseteq \{0, 1, \dots, m + n\}$$

is finite, and so $f \cdot g \in R^{(\mathbb{N})}$. Hence $R^{(\mathbb{N})}$ is a subring of $R^{\mathbb{N}}$.

(iii) The function φ is clearly injective. We have $\varphi(1) = (1, 0, \dots)$. Moreover, $\forall a, b \in R$ we have

$$\varphi(a + b) = (a + b, 0, \dots) = (a, 0, \dots) + (b, 0, \dots) = \varphi(a) + \varphi(b)\,,$$

$$\varphi(a \cdot b) = (a \cdot b, 0, \dots) = (a, 0, \dots) \cdot (b, 0, \dots) = \varphi(a) \cdot \varphi(b)\,.$$

Therefore, φ is an injective unitary ring homomorphism.

Remark 2.7.3 Since φ is injective, we have $Ker\,\varphi = \{0\}$, and so $R \cong R/\{0\} \cong R/Ker\,\varphi \cong Im\,\varphi$ by the first isomorphism theorem for rings. Hence we may identify an element $a \in R$ with its image $\varphi(a) \in R^{(\mathbb{N})}$.

Definition 2.7.4 The element $X = (0, 1, 0, \dots)$ of $R^{(\mathbb{N})}$ is called the *indeterminate*.

For every $n \in \mathbb{N}$ we have:

$$X^n = (\underbrace{0, \dots, 0}_{n \text{ times}}, 1, 0, \dots)$$

by the definition of multiplication.

Lemma 2.7.5 *Every non-zero $f \in R^{(\mathbb{N})}$ can be uniquely written in the form*

$$f = a_0 + a_1 X + \cdots + a_n X^n ,$$

called the algebraic form *of f, where $a_0, \ldots, a_n \in R$ and $a_n \neq 0$.*

Proof. Since $f \in R^{(\mathbb{N})}$ is non-zero, $f = (a_0, a_1, \ldots, a_n, 0, \ldots)$ for some $a_0, \ldots, a_n \in R$ such that $a_n \neq 0$. By identifying each a_i with $\varphi(a_i)$ (see Remark 2.7.3), we have:

$$\begin{aligned} f &= (a_0, 0, \ldots) + (0, a_1, 0, \ldots) + \cdots + (0, \ldots, 0, a_n, 0, \ldots) \\ &= a_0(1, 0, \ldots) + a_1(0, 1, 0, \ldots) + \cdots + a_n(0, \ldots, 0, 1, 0, \ldots) \\ &= a_0 + a_1 X + \cdots + a_n X^n. \end{aligned}$$

Now suppose that we also have $f = b_0 + b_1 X + \cdots + b_m X^m$, where $b_0, \ldots, b_m \in R$ and $b_m \neq 0$. It follows that $f = (a_0, a_1, \ldots, a_n, 0, \ldots) = (b_0, b_1, \ldots, b_m, 0, \ldots)$. Hence we must have $m = n$ and $a_i = b_i$ for every $i \in \{1, \ldots, n\}$. Hence f has a unique representation in algebraic form.

Definition 2.7.6 The ring $R^{\mathbb{N}}$ is also denoted by $R[[X]]$ and called the *ring of formal power series over R*. The ring $R^{(\mathbb{N})}$ is also denoted by $R[X]$ and called the *polynomial ring over R*.