Notes - Commutative Rings

George McNinch

2025-01-15

See [Stewart, chapter 16] [1] for general results about commutative rings.

[1] As noted in the course syllabus, Tisch library has an entry for this item here; click to find online access to the text *Galois Theory*, Ian Stewart. (CRC Press, 4th edition 2022).

Commutative rings

In the lecture today, we define the notion of a *ring*:

Definition A ring R is an additive abelian group together with an operation of multiplication $R \times R \to R$ given by $(a, b) \mapsto a \cdot b$ such that the following axioms hold:

- multiplication is *associative*

We say that the ring R is *commutative* if the operation of multiplication is commutative; i.e. if $ab = ba$ for all $a, b \in R$.

And we say that R has identity if multiplication has an identity

Commutative rings

In the lecture today, we define the notion of a *ring*:

Definition A ring R is an additive abelian group together with an operation of multiplication $R \times R \to R$ given by $(a, b) \mapsto a \cdot b$ such that the following axioms hold:

- multiplication is *associative*
- multiplication *distributes* over addition: for every $a, b, c \in R$ we have [2]

  $$a(b + c) = ab + ac$$

  and

  $$(b + c)a = ba + ca$$

We say that the ring R is *commutative* if the operation of multiplication is commutative; i.e. if $ab = ba$ for all $a, b \in R$.

And we say that R has identity if multiplication has an identity

Commutative rings

In the lecture today, we define the notion of a *ring*:

Definition A ring R is an additive abelian group together with an operation of multiplication $R \times R \to R$ given by $(a, b) \mapsto a \cdot b$ such that the following axioms hold:

- multiplication is *associative*
- multiplication *distributes* over addition: for every $a, b, c \in R$ we have [2]

  $$a(b + c) = ab + ac$$

  and

  $$(b + c)a = ba + ca$$

We say that the ring R is *commutative* if the operation of multiplication is commutative; i.e. if $ab = ba$ for all $a, b \in R$.

And we say that R has identity if multiplication has an identity

Commutative rings

In the lecture today, we define the notion of a *ring*:

Definition A ring R is an additive abelian group together with an operation of multiplication $R \times R \to R$ given by $(a, b) \mapsto a \cdot b$ such that the following axioms hold:

- multiplication is *associative*
- multiplication *distributes* over addition: for every $a, b, c \in R$ we have [2]

$$a(b + c) = ab + ac$$

and

$$(b + c)a = ba + ca$$

We say that the ring R is *commutative* if the operation of multiplication is commutative; i.e. if $ab = ba$ for all $a, b \in R$.

And we say that R has identity if multiplication has an identity

Polynomial rings

If R is a commutative ring, the collection of all polynomials in the variable T having coefficients in R is denoted $R[T]$.

Notice that the set of *monomials* $S = \{T^i \mid i \in \mathbb{N}\}$ has the following properties:

- every element of $R[T]$ is an R-linear combination of elements of S. This just amounts to the statement that every polynomial $f(T) \in R[T]$ has the form

  $$f(T) = \sum_{i=0}^{N} a_i T^i$$

  for a suitable $N \geq 0$ and suitable coefficients $a_i \in R$.

Polynomial rings

If R is a commutative ring, the collection of all polynomials in the variable T having coefficients in R is denoted $R[T]$.

Notice that the set of *monomials* $S = \{T^i \mid i \in \mathbb{N}\}$ has the following properties:

- every element of $R[T]$ is an R-linear combination of elements of S. This just amounts to the statement that every polynomial $f(T) \in R[T]$ has the form
$$f(T) = \sum_{i=0}^{N} a_i T^i$$
for a suitable $N \geq 0$ and suitable coefficients $a_i \in R$.

- the elements of S are linearly independent
i.e. if
$$\sum_{i=0}^{N} a_i T^i = 0 \quad \text{for} \quad a_i \in R,$$