MATH146 - 2025-01-15

GEORGE MCNINCH

Contents

1. Commutative Rings

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

1.1. Definitions.

Definition 1.1.1. 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, i.e. if there is an element $1_R \in R$ such that $a \cdot 1_R = 1_R \cdot a = a$ for every $a \in R$. [3]

In the course, we will consider (almost?) exclusively rings which are commutative and have identity.

Here are some examples of commutative rings:

Problem 1.1.2. (a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
(b) if X is a set and if R is a commutative ring, the set X^R of all R-valued functions on X can be viewed as a commutative ring in a natural way.

Date: 2025-01-26 14:00:10 EST (george@valhalla).

[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).

[2] We often just denote multiplication by juxtaposition: i.e. we may write ab instead of $a \cdot b$ for $a, b \in R$

[3] Usually we write 1 for 1_R. The idea is that 1_R is the multiplicative identity of R. For example, the identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the multiplicative identity 1_R of the matrix ring $R = \mathrm{Mat}_2(\mathbb{R})$.

1.2. **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:

(M1) 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 $a_i \in R$.

(M2) the elements of S are linearly independent i.e. if

$$\sum_{i=0}^{N} a_i T^i = 0 \quad \text{for} \quad a_i \in R,$$

then $a_i = 0$ for every i.

Polynomials in $R[T]$ can be added in a natural way. (This is just like adding vectors in a vector space).

And there is a product operation on polynomials, as follows:

if $f(T) = \displaystyle\sum_{i=0}^{N} a_i T^i$ and $g(T) = \displaystyle\sum_{i=0}^{M} b_i T^i$ then

$$f(T) \cdot g(T) = \sum_{i=0}^{N+M} c_i T^i \quad \text{where} \quad c_i = \sum_{s+t=i} a_s b_t.$$

Proposition 1.2.1. *$R[T]$ is a commutative ring with identity.*