

Math 310 Class Notes 3: A Preview to Modern Algebra

Definition 1. A set R with two binary operations $+$ and \cdot is called a ring if

- (1) $+$ is commutative and associative.
- (2) R has an additive identity, denoted as usual by 0 . That is, $a+0 = a$ for all $a \in R$.
- (3) Each $a \in R$ has an additive inverse. That is, for any $a \in R$, there is an element $b \in R$ such that $a+b = 0$. As usual, we denote b by $-a$.
- (4) \cdot is associative.
- (5) The distributive law is true. That is, for all $a, b, c \in R$, $a \cdot (b+c) = a \cdot b + a \cdot c$, and $(a+b) \cdot c = a \cdot c + b \cdot c$.

Note that in the definition, \cdot need not be commutative. Moreover, R need not have a multiplicative identity.

Definition 2. If in the ring R , the binary operation \cdot is commutative, then R is called a commutative ring. On the other hand, if R has a multiplicative identity, denoted as usual by 1 , that is $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$, then R is called a ring with identity.

For example, \mathbb{Z} and \mathbb{Z}_m for $m \in \mathbb{N}$ are commutative rings with identity. $2\mathbb{Z}$, the set of even integers, is a commutative ring without identity. The set M_n of n -by- n matrices whose entries are integers is a non-commutative ring with identity, whereas the set of n -by- n matrices whose entries are even integers is a non-commutative ring without identity. As a last example, the set of all real polynomials in one variable x is a commutative ring with identity.

Definition 3. F is a field if

- (i) $(F, +, \cdot)$ is a commutative ring with identity.
- (ii) Each nonzero element has a multiplicative inverse. That is, for any $a \neq 0$, there is an element $b \in F$ such that $a \cdot b = 1$. As usual, b is denoted by a^{-1} .

For example, \mathbb{Q} , \mathbb{R} and \mathbb{Z}_p , where p is a prime, are all fields. \mathbb{Z} and \mathbb{Z}_m , where m is not a prime, are not fields. As a last example, the set of all real rational functions in one variable x , of the form $p(x)/q(x)$, where $p(x)$ and $q(x) \neq 0$ are real polynomials in x , is a field.

Proposition 4. Let R be a ring. Then

- (I) $-(-a) = a$.
- (II) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$.
- (III) $(-a) \cdot (-b) = a \cdot b$.

Proof. (I) follows because $-(-a)$ is the additive inverse to $-a$, which is just a .

(II) follows because $a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$, so that $a \cdot (-b)$ is the additive inverse to $a \cdot b$. Hence, $a \cdot (-b) = -(a \cdot b)$. The same reasoning yields $(-a) \cdot b = -(a \cdot b)$.

Note that we have used the fact that $a \cdot 0 = 0$ for all $a \in R$. This is true because $0 + 0 = 0$ by (2) above, so that

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Let b be the additive inverse to $a \cdot 0$. Adding b to the above equation, we obtain

$$0 = b + a \cdot 0 = (b + a \cdot 0) + a \cdot 0 = 0 + a \cdot 0 = a \cdot 0.$$

For (III), we use (II) repeatedly as follows.

$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b,$$

where the last equality is gotten by (I). □