Rings

KYB

Thrn, it's a Fact

mathrnfact@gmail.com

January 13, 2021

Overview

Rings

Definition

1. A ring R is a set with two binary operations $+$ and $\times$ satisfying the following axtioms:
   i $(R, +)$ is an abelian group,
   ii $\times$ is associative,
   iii the distributive laws hold in R, i.e. for all $a, b, c \in R$

$$(a+b) \times c = (a \times c) + (b \times c),$$
$$a \times (b+c) = (a \times b) + (a \times c).$$

2. R is commutative ring if $\times$ is commutative.
3. R is said to be have an identity if there is an element $1 \in R$ with

$$1 \times a = a \times 1 = a \text{ for all } a \in R.$$

Definition

1. A ring R with $1 \neq 0$ is called a division ring (or skew field) if every nonzero element $a \in R$ has a multiplicative inverse.
2. A commutative division ring is called a field.

Definition

Let R be a ring.

1. A nonzero element $a \in R$ is called a zero divisor if there is a nonzero $b \in R$ such that either $ab = 0$ or $ba = 0$.
2. Assume R has an identity $1 \neq 0$. An element u of R is called a unit in R if u has an multiplicative inverse in R.
3. The set of units in R is denoted $R^{\times}$.
4. If R has no zero divisor, R is called an integral domain.

Subrings

Definition

A subring of the ring R is a subgroup of R that is closed under multiplication.

Example

1. $\mathbb{Z}$ is a subring of $\mathbb{Q}$, and $\mathbb{Q}$ if a subring of $\mathbb{R}$ and $\mathbb{R}$ is a subring of $\mathbb{C}$.
2. $n\mathbb{Z}$ is a subring of $\mathbb{Z}$.
3. Let R be a ring with $1 \neq 0$. Then $R \times R$ forms a ring in a natrual way with identity $(1, 1)$

$$
\begin{aligned}
(a_1, a_2) + (b_1, b_2) &= (a_1 + b_1, a_2 + b_2) \\
(a_1, a_2) \times (b_1, b_2) &= (a_1 b_1, a_2 b_2) \\
(a, b) \times (1, 1) &= (1, 1) \times (a, b) = (a, b).
\end{aligned}
$$

Then $R \times \{0\}$ is a subring of $R \times R$ with identity $(1, 0)$.

Example (Polynomial Rings)

Fix a commutative ring R with identity. Let x be an indeterminate. We call $p(x)$ is a polynomial if

$$p(x) = a_n x^n + \cdots + a_1 x + a_0$$

where $n \geq 0$ and $a_i \in R$. If $a_n \neq 0$,

- $\deg p = n$
- $a_n x^n$ is called the leading term
- a_n is called the leading coefficient
- if $a_n = 1$, $p(x)$ is called monic.

We can give $+$ and $\times$ in familiar ways. Then the set of all polynomial $R[x]$ forms a ring.

Example (Matrix Rings)

Fix an arbitrary ring R and let n be a positive integer. Let $M_n(R)$ be the set of all $n \times n$ matrices with entries from R. The $M_n(R)$ forms a ring.

Ring Homomorphism

Definition

Let R and S be rings.

1. A ring homomorphism f is a map $f : R \to S$ satisfying
   (i) $f(a+b) = f(a) + f(b)$,
   (ii) $f(ab) = f(a)f(b)$.
2. $\mathrm{Ker} f = \{x \in R : f(x) = 0\}$ and $\mathrm{Im}\, f = \{f(x) : x \in R\}$.
3. If f is bijective, f is called an isomorphism.

Proposition

Let $f : R \to S$ be a ring homomorphism.

1. $\mathrm{Im}\, f$ is a subring of S.
2. $\mathrm{Ker} f$ is a subring of R. Furthermore, if $\alpha \in \mathrm{Ker} f$, then $r\alpha, \alpha r \in \mathrm{Ker} f$ for all $r \in R$.

Remark

Note that a ring is a additive abelian group. So $R/\mathrm{Ker} f$ is a quotient additive group. Now we want to give a multiplication on $R/\mathrm{Ker} f$ by

$$(x + \mathrm{Ker} f) \times (y + \mathrm{Ker} f) = (xy) + \mathrm{Ker} f.$$

This is well-defined because

$$\begin{aligned}(x + \mathrm{Ker} f) \times (y + \mathrm{Ker} f) &= xy + \mathrm{Ker} f y + x \mathrm{Ker} f + \mathrm{Ker} f \mathrm{Ker} f \\ &\subset xy + \mathrm{Ker} f + \mathrm{Ker} f + \mathrm{Ker} f = (xy) + \mathrm{Ker} f.\end{aligned}$$

So $R/\mathrm{Ker} f$ is a ring.

Ideals

Definition

Let R be a ring, and let I be a subset of R and $r \in R$.

1. $rI = \{ra : a \in I\}$ and $Ir = \{ar : a \in I\}$.
2. A subset I of R is a left ideal (resp. right ideal) of R is
   (i) I is a subring of R,
   (ii) I is closed under left (resp. right) multiplication by element from R, i.e.
   $$rI \subset I \text{ (resp. } Ir \subset I) \text{ , for all } r \in R.$$
3. A subset I that is both a left ideal and a right ideal is called an ideal of R.

Example

$\mathrm{Ker} f$ is an ideal of R.

Proposition

Let R be a ring and let I be an ideal of R. Then the quotient group R/I is a ring under the binary operations:

$$(r+I)+(s+I)=(r+s)+I$$
$$(r+I)\times(s+I)=(rs)+I.$$

Conversely, if I is any subgroup such that the above operations are well defined, then I is an ideal of R.
In this case, R/I is called the quotient ring of R by I.

Theorem (The first Isomorphism Theorem for Rings)

Let $f : R \to S$ *be a ring homomorphism. Then* $R/\mathrm{Ker}\, f \cong \mathrm{Im}\, f$.

Definition

Let I and J be ideals of R.

1. $I + J = \{a + b : a \in I, b \in J\}$.
2. $IJ = \{\sum_{i=1}^{n} a_i b_i, a_i \in I, b_i \in J\}$.
3. $I^n = II^{n-1}$.

From now on, a ring has a identity $1 \neq 0$.

Proposition

Let I be an ideal of R.

1. $I = R$ iff I contains a unit.
2. Assume R is commutative. Then R is a field iff its only ideals are 0 and R.

Corollary

If R is a field, then any nonzero ring homomorphism from R into another ring is an injection. In this sense, a field is unique.

Definition

An ideal M in an arbitrary ring S is called a maximal ideal if

1. $M \neq S$
2. if $M \subset I \subset S$ is an ideal, then either $I = M$ or $I = S$.

Proposition

In a ring with identity every proper ideal is contained in a maximal ideal.

Proposition

Assume R is commutative. The ideal M is a maximal ideal iff R/M is a field.

Definition

Assume R is commutative. An ideal P is called a prime ideal if

1. $P \neq R$,
2. if $ab \in P$, then either $a \in P$ or $b \in P$.

Proposition

Assume R is commutative. Then the ideal P is a prime ideal in R iff R/P is an integral domain.

Corollary

Assume R is commutative. Every maximal ideal of R is a prime ideal.

The End