Chapter 13: Basic ring theory

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Spring 2014

Introduction

Definition

A ring is an additive (abelian) group R with an additional binary operation (multiplication), satisfying the distributive law:

$$x(y+z) = xy + xz \qquad \text{and} \qquad (y+z)x = yx + zx \quad \forall x, y, z \in R\,.$$

Remarks

- There need not be multiplicative inverses.
- Multiplication need not be commutative (it may happen that $xy \neq yx$).

A few more terms

If $xy = yx$ for all $x, y \in R$, then R is commutative.

If R has a multiplicative identity $1 = 1_R \neq 0$, we say that "R has identity" or "unity", or "R is a ring with 1."

A subring of R is a subset $S \subseteq R$ that is also a ring.

Introduction

Examples

1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are all commutative rings with 1.
2. $\mathbb{Z}_n$ is a commutative ring with 1.
3. For any ring R with 1, the set $M_n(R)$ of $n \times n$ matrices over R is a ring. It has identity $1_{M_n(R)} = I_n$ iff R has 1.
4. For any ring R, the set of functions $F = \{f \colon R \to R\}$ is a ring by defining

$$(f+g)(r) = f(r) + g(r) \qquad (fg)(r) = f(r)g(r)\,.$$

5. The set $S = 2\mathbb{Z}$ is a subring of $\mathbb{Z}$ but it does *not* have 1.
6. $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{R} \right\}$ is a subring of $R = M_2(\mathbb{R})$. However, note that

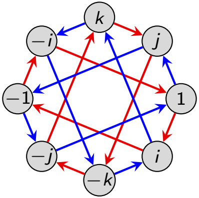
$$1_R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \text{but} \qquad 1_S = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

7. If R is a ring and x a variable, then the set

$$R[x] = \{a_n x^n + \cdots a_1 x + a_0 \mid a_i \in R\}$$

is called the polynomial ring over R.

Another example: the quaternions



Recall the (unit) quaternion group:

$$Q_4 = \langle i,j,k \mid i^2 = j^2 = k^2 = -1,\ ij = k\rangle.$$

Allowing addition makes them into a ring $\mathbb{H}$, called the quaternions, or Hamiltonians:

$$\mathbb{H} = \{a + bi + cj + dk \mid a,b,c,d \in \mathbb{R}\}.$$

The set $\mathbb{H}$ is isomorphic to a subring of $M_n(\mathbb{R})$, the real-valued 4×4 matrices:

$$\mathbb{H} = \left\{ \begin{bmatrix} a & -b & -c & -d \\ -b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix} : a,b,c,d \in \mathbb{R} \right\} \subseteq M_4(\mathbb{R}).$$

Formally, we have an embedding $\phi\colon \mathbb{H} \hookrightarrow M_4(\mathbb{R})$ where

$$\phi(i) = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad \phi(j) = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \quad \phi(k) = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

We say that $\mathbb{H}$ is represented by a set of matrices.

Units and zero divisors

Definition

Let R be a ring with 1. A unit is any $x \in R$ that has a multiplicative inverse. Let $U(R)$ be the set (a multiplicative group) of units of R.

An element $x \in R$ is a left zero divisor if $xy = 0$ for some $y \neq 0$. (Right zero divisors are defined analogously.)

Examples

1. Let $R = \mathbb{Z}$. The units are $U(R) = \{-1, 1\}$. There are no (nonzero) zero divisors.
2. Let $R = \mathbb{Z}_{10}$. Then 7 is a unit (and $7^{-1} = 3$) because $7 \cdot 3 = 1$. However, 2 is not a unit.
3. Let $R = \mathbb{Z}_n$. A nonzero $k \in \mathbb{Z}_n$ is a unit if $\gcd(n, k) = 1$, and a zero divisor if $\gcd(n, k) \geq 2$.
4. The ring $R = M_2(\mathbb{R})$ has zero divisors, such as:

$$\begin{bmatrix} 1 & -2 \\ -2 & 4 \end{bmatrix} \begin{bmatrix} 6 & 2 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

   The groups of units of $M_2(\mathbb{R})$ are the invertible matrices.

Group rings

Let R be a commutative ring (usually, $\mathbb{Z}$, $\mathbb{R}$, or $\mathbb{C}$) and G a finite (multiplicative) group. We can define the group ring RG as

$$RG := \{a_1 g_1 + \cdots + a_n g_n \mid a_i \in R,\ g_i \in G\},$$

where multiplication is defined in the "obvious" way.

For example, let $R = \mathbb{Z}$ and $G = D_4 = \langle r, f \mid r^4 = f^2 = rfrf = 1\rangle$, and consider the elements $x = r + r^2 - 3f$ and $y = -5r^2 + rf$ in $\mathbb{Z}D_4$. Their sum is

$$x + y = r - 4r^2 - 3f + rf,$$

and their product is

$$\begin{aligned} xy &= (r + r^2 - 3f)(-5r^2 + rf) = r(-5r^2 + rf) + r^2(-5r^2 + rf) - 3f(-5r^2 + rf) \\ &= -5r^3 + r^2 f - 5r^4 + r^3 f + 15fr^2 - 3frf = -5 - 8r^3 + 16r^2 f + r^3 f. \end{aligned}$$

Remarks

- The (real) Hamiltonians $\mathbb{H}$ is *not* the same ring as $\mathbb{R}Q_4$.
- If $|G| > 1$, then RG always has zero divisors, because if $|g| = k > 1$, then:

$$(1 - g)(1 + g + \cdots + g^{k-1}) = 1 - g^k = 1 - 1 = 0.$$

- RG contains a subring isomorphic to R, and the group of units $U(RG)$ contains a subgroup isomorphic to G.

Types of rings

Definition

If all nonzero elements of R have a multiplicative inverse, then R is a division ring. (Think: "field without commutativity".)

An integral domain is a commutative ring with 1 and with no (nonzero) zero divisors. (Think: "field without inverses".)

A field is just a commutative division ring. Moreover:

$$\text{fields} \subsetneq \text{division rings}$$

$$\text{fields} \subsetneq \text{integral domains} \subsetneq \text{all rings}$$

Examples

- Rings that are not integral domains: $\mathbb{Z}_n$ (composite n), $2\mathbb{Z}$, $M_n(\mathbb{R})$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{H}$.
- Integral domains that are not fields (or even division rings): $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{R}[[x]]$ (formal power series).
- Division ring but not a field: $\mathbb{H}$.

Cancellation

When doing basic algebra, we often take for granted basic properties such as cancellation: $ax = ay \implies x = y$. However, *this need not hold in all rings!*

Examples where cancellation fails

- In $\mathbb{Z}_6$, note that $2 = 2 \cdot 1 = 2 \cdot 4$, but $1 \neq 4$.
- In $M_2(\mathbb{R})$, note that $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 4 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$.

However, everything works fine as long as there aren't any (nonzero) zero divisors.

Proposition

Let R be an integral domain and $a \neq 0$. If $ax = ay$ for some $x, y \in R$, then $x = y$.

Proof

If $ax = ay$, then $ax - ay = a(x - y) = 0$.

Since $a \neq 0$ and R has no (nonzero) zero divisors, then $x - y = 0$. $\square$

Finite integral domains

Lemma (HW)

If R is an integral domain and $0 \neq a \in R$ and $k \in \mathbb{N}$, then $a^k \neq 0$. $\square$

Theorem

Every finite integral domain is a field.

Proof

Suppose R is a finite integral domain and $0 \neq a \in R$. It suffices to show that a has a multiplicative inverse.

Consider the infinite sequence $a, a^2, a^3, a^4, \ldots$, which must repeat.

Find $i > j$ with $a^i = a^j$, which means that

$$0 = a^i - a^j = a^j(a^{i-j} - 1).$$

Since R is an integral domain and $a^j \neq 0$, then $a^{i-j} = 1$.

Thus, $a \cdot a^{i-j-1} = 1$. $\square$

Ideals

In the theory of groups, we can quotient out by a subgroup if and only if it is a normal subgroup. The analogue of this for rings are (two-sided) ideals.

Definition

A subring $I \subseteq R$ is a left ideal if

$$rx \in I \qquad \text{for all } r \in R \text{ and } x \in I.$$

Right ideals, and two-sided ideals are defined similarly.

If R is commutative, then all left (or right) ideals are two-sided.

We use the term ideal and two-sided ideal synonymously, and write $I \trianglelefteq R$.

Examples

- $n\mathbb{Z} \trianglelefteq \mathbb{Z}$.
- If $R = M_2(\mathbb{R})$, then $I = \left\{ \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} : a, c \in \mathbb{R} \right\}$ is a left, but *not* a right ideal of R.
- The set $\mathrm{Sym}_n(\mathbb{R})$ of symmetric $n \times n$ matrices is a subring of $M_n(\mathbb{R})$, but *not* an ideal.

Ideals

Remark

If an ideal I of R contains 1, then $I = R$.

Proof

Suppose $1 \in I$, and take an arbitrary $r \in R$.

Then $r1 \in I$, and so $r1 = r \in I$. Therefore, $I = R$. $\square$

It is not hard to modify the above result to show that if I contains *any* unit, then $I = R$. (HW)

Let's compare the concept of a normal subgroup to that of an ideal:

- normal subgroups are characterized by being invariant under conjugation:

$$H \leq G \text{ is normal iff } ghg^{-1} \in H \text{ for all } g \in G,\ h \in H.$$

- (left) ideals of rings are characterized by being invariant under (left) multiplication:

$$I \subseteq R \text{ is a (left) ideal iff } ri \in I \text{ for all } r \in R,\ i \in I.$$

Ideals generated by sets

Definition

The left ideal generated by a set $X \subset R$ is defined as:

$$(X) := \bigcap \big\{ I : \ I \text{ is a left ideal s.t. } X \subseteq I \subseteq R \big\}.$$

This is the smallest left ideal containing X.

There are analogous definitions by replacing "left" with "right" or "two-sided".

Recall the two ways to define the subgroup $\langle X \rangle$ generated by a subset $X \subseteq G$:

- "*Bottom up*": As the set of all finite products of elements in X;
- "*Top down*": As the intersection of all subgroups containing X.

Proposition (HW)

Let R be a ring *with unity*. The (left, right, two-sided) ideal generated by $X \subseteq R$ is:

- Left: $\{r_1x_1 + \cdots + r_nx_n : n \in \mathbb{N},\ r_i \in R,\ x_i \in X\}$,
- Right: $\{x_1r_1 + \cdots + x_nr_n : n \in \mathbb{N},\ r_i \in R,\ x_i \in X\}$,
- Two-sided: $\{r_1x_1s_1 + \cdots + r_nx_ns_n : n \in \mathbb{N},\ r_i, s_i \in R,\ x_i \in X\}$.

Ideals and quotients

Since an ideal I of R is an additive subgroup (and hence normal), then:

- $R/I = \{x + I \mid x \in R\}$ is the set of cosets of I in R;
- R/I is a quotient group; with the binary operation (addition) defined as

$$(x + I) + (y + I) := x + y + I.$$

It turns out that if I is also a two-sided ideal, then we can make R/I into a ring.

Proposition

If $I \subseteq R$ is a (two-sided) ideal, then R/I is a ring (called a quotient ring), where multiplication is defined by

$$(x + I)(y + I) := xy + I\,.$$

Proof

We need to show this is well-defined. Suppose $x + I = r + I$ and $y + I = s + I$. This means that $x - r \in I$ and $y - s \in I$.

It suffices to show that $xy + I = rs + I$, or equivalently, $xy - rs \in I$:

$$xy - rs = xy - ry + ry - rs = (x - r)y + r(y - s) \in I\,.$$

Finite fields

We've already seen that $\mathbb{Z}_p$ is a field if p is prime, and that finite integral domains are fields. But *what do these "other" finite fields look like?*

Let $R = \mathbb{Z}_2[x]$ be the polynomial ring over the field $\mathbb{Z}_2$. (Note: we can ignore all negative signs.)

The polynomial $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$ because it does not have a root. (Note that $f(0) = f(1) = 1 \neq 0$.)

Consider the ideal $I = (x^2 + x + 1)$, the set of multiples of $x^2 + x + 1$.

In the quotient ring R/I, we have the relation $x^2 + x + 1 = 0$, or equivalently, $x^2 = -x - 1 = x + 1$.

The quotient has only 4 elements:

$$0 + I\,, \qquad 1 + I\,, \qquad x + I\,, \qquad (x + 1) + I\,.$$

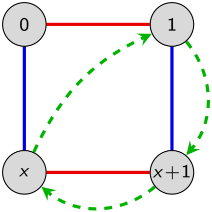
As with the quotient group (or ring) $\mathbb{Z}/n\mathbb{Z}$, we usually drop the "I", and just write

$$R/I = \mathbb{Z}_2[x]/(x^2 + x + 1) \cong \{0,\ 1,\ x,\ x + 1\}\,.$$

It is easy to check that this is a field!

Finite fields

Here is a Cayley diagram, and the operation tables for $R/I = \mathbb{Z}_2[x]/(x^2+x+1)$:



$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

Theorem

There exists a finite field $\mathbb{F}_q$ of order q, which is unique up to isomorphism, iff $q = p^n$ for some prime p. If $n > 1$, then this field is isomorphic to the quotient ring

$$\mathbb{Z}_p[x]/(f)\,,$$

where f is *any* irreducible polynomial of degree n.

Much of the error correcting techniques in coding theory are built using mathematics over $\mathbb{F}_{2^8} = \mathbb{F}_{256}$. This is what allows your CD to play despite scratches.

Homomorphisms: groups vs. rings (spoilers!)

Many of the big ideas from group homomorphisms carry over to ring homomorphisms.

Group theory

- The quotient group G/N exists iff N is a normal subgroup.
- A homomorphism is a structure-preserving map: $f(x * y) = f(x) * f(y)$.
- The kernel of a homomorphism is a normal subgroup: $\operatorname{Ker}\phi \trianglelefteq G$.
- For every normal subgroup $N \trianglelefteq G$, there is a natural quotient homomorphism $\phi \colon G \to G/N$, $\phi(g) = gN$.
- There are four standard isomorphism theorems for groups.

Ring theory

- The quotient ring R/I exists iff I is a two-sided ideal.
- A homomorphism is a structure-preserving map: $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$.
- The kernel of a homomorphism is a two-sided ideal: $\operatorname{Ker}\phi \trianglelefteq R$.
- For every two-sided ideal $I \trianglelefteq R$, there is a natural quotient homomorphism $\phi \colon R \to R/I$, $\phi(r) = r + I$.
- There are four standard isomorphism theorems for rings.

Ring homomorphisms

Definition

A ring homomorphism is a function $f \colon R \to S$ satisfying

$$f(x+y) = f(x) + f(y) \qquad \text{and} \qquad f(xy) = f(x)f(y) \quad \text{for all } x, y \in R.$$

A ring isomorphism is a homomorphism that is bijective.

The kernel $f \colon R \to S$ is the set $\operatorname{Ker} f := \{x \in R : f(x) = 0\}$.

Examples

1. The function $\phi \colon \mathbb{Z} \to \mathbb{Z}_n$ that sends $k \mapsto k \pmod{n}$ is a ring homomorphism with $\operatorname{Ker}(\phi) = n\mathbb{Z}$.
2. For a fixed real number $\alpha \in \mathbb{R}$, the "evaluation function"

$$\phi \colon \mathbb{R}[x] \longrightarrow \mathbb{R}\,, \qquad \phi \colon p(x) \longmapsto p(\alpha)$$

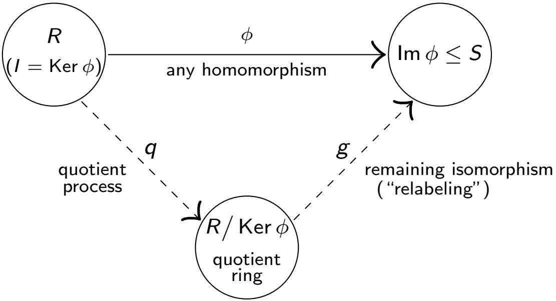
   is a homomorphism. The kernel consists of all polynomials that have α as a root.
3. The following is a homomorphism, for the ideal $I = (x^2 + x + 1)$ in $\mathbb{Z}_2[x]$:

$$\phi \colon \mathbb{Z}_2[x] \longrightarrow \mathbb{Z}_2[x]/I, \qquad f(x) \longmapsto f(x) + I\,.$$

The isomorphism theorems for rings

Fundamental homomorphism theorem

If $\phi\colon R \to S$ is a ring homomorphism, then $\operatorname{Ker}\phi$ is an ideal and $\operatorname{Im}(\phi) \cong R/\operatorname{Ker}(\phi)$.



Proof (HW)

The statement holds for the underlying additive group R. Thus, it remains to show that $\operatorname{Ker}\phi$ is a (two-sided) ideal, and the following map is a ring homomorphism:

$$g\colon R/I \longrightarrow \operatorname{Im}\phi\,, \qquad\qquad g(x+I) = \phi(x)\,.$$

The second isomorphism theorem for rings

Diamond isomorphism theorem

Suppose S is a subring and I an ideal of R. Then

(i) The sum $S+I=\{s+i \mid s\in S,\ i\in I\}$ is a subring of R and the intersection $S\cap I$ is an ideal of S.

(ii) The following quotient rings are isomorphic:

$$(S+I)/I \cong S/(S\cap I)\,.$$

$$\begin{tikzcd}[column sep=small]
 & R \arrow[d, dash] & \\
 & S+I \arrow[dl, dash] \arrow[dr, dash] & \\
S \arrow[dr, dash] & & I \arrow[dl, dash] \\
 & S\cap I &
\end{tikzcd}$$

Proof (sketch)

$S+I$ is an additive subgroup, and it's closed under multiplication because

$$s_1,s_2\in S,\ i_1,i_2\in I \quad\Longrightarrow\quad (s_1+i_1)(s_2+i_2)=\underbrace{s_1s_2}_{\in S}+\underbrace{s_1i_2+i_1s_2+i_1i_2}_{\in I}\in S+I.$$

Showing $S\cap I$ is an ideal of S is straightforward (homework exercise).

We already know that $(S+I)/I\cong S/(S\cap I)$ as additive groups.

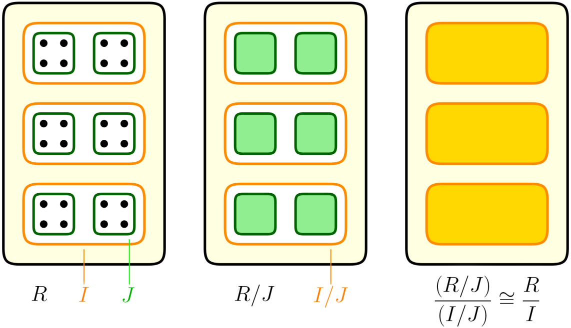
One explicit isomorphism is $\phi\colon s+(S\cap I)\mapsto s+I$. It is easy to check that $\phi\colon 1\mapsto 1$ and ϕ preserves products. $\square$

The third isomorphism theorem for rings

Freshman theorem

Suppose R is a ring with ideals $J \subseteq I$. Then I/J is an ideal of R/J and

$$(R/J)/(I/J) \cong R/I\,.$$

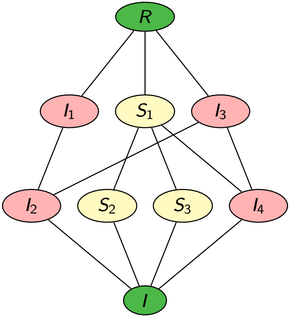


(Thanks to Zach Teitler of Boise State for the concept and graphic!)

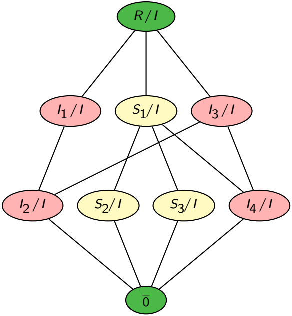
The fourth isomorphism theorem for rings

Correspondence theorem

Let I be an ideal of R. There is a bijective correspondence between subrings (& ideals) of R/I and subrings (& ideals) of R that contain I. In particular, every ideal of R/I has the form J/I, for some ideal J satisfying $I \subseteq J \subseteq R$.



subrings & ideals that contain I



subrings & ideals of R/I

Maximal ideals

Definition

An ideal I of R is maximal if $I \neq R$ and if $I \subseteq J \subseteq R$ holds for some ideal J, then $J = I$ or $J = R$.

A ring R is simple if its only (two-sided) ideals are 0 and R.

Examples

1. If $n \neq 0$, then the ideal $M = (n)$ of $R = \mathbb{Z}$ is maximal if and only if n is prime.
2. Let $R = \mathbb{Q}[x]$ be the set of all polynomials over $\mathbb{Q}$. The ideal $M = (x)$ consisting of all polynomials with constant term zero is a maximal ideal.

   Elements in the quotient ring $\mathbb{Q}[x]/(x)$ have the form $f(x) + M = a_0 + M$.
3. Let $R = \mathbb{Z}_2[x]$, the polynomials over $\mathbb{Z}_2$. The ideal $M = (x^2 + x + 1)$ is maximal, and $R/M \cong \mathbb{F}_4$, the (unique) finite field of order 4.

In all three examples above, the quotient R/M is a field.

Maximal ideals

Theorem

Let R be a commutative ring with 1. The following are equivalent for an ideal $I \subseteq R$.

(i) I is a maximal ideal;

(ii) R/I is simple;

(iii) R/I is a field.

Proof

The equivalence (i)$\Leftrightarrow$(ii) is immediate from the Correspondence Theorem.

For (ii)$\Leftrightarrow$(iii), we'll show that an *arbitrary* ring R is simple iff R is a field.

"$\Rightarrow$": Assume R is simple. Then $(a) = R$ for any nonzero $a \in R$.

Thus, $1 \in (a)$, so $1 = ba$ for some $b \in R$, so $a \in U(R)$ and R is a field. ✓

"$\Leftarrow$": Let $I \subseteq R$ be a nonzero ideal of a field R. Take any nonzero $a \in I$.

Then $a^{-1}a \in I$, and so $1 \in I$, which means $I = R$. ✓ $\square$

Prime ideals

Definition

Let R be a commutative ring. An ideal $P \subset R$ is prime if $ab \in P$ implies either $a \in P$ or $b \in P$.

Note that $p \in \mathbb{N}$ is a prime number iff $p = ab$ implies either $a = p$ or $b = p$.

Examples

1. The ideal (n) of $\mathbb{Z}$ is a prime ideal iff n is a prime number (possibly $n = 0$).
2. In the polynomial ring $\mathbb{Z}[x]$, the ideal $I = (2, x)$ is a prime ideal. It consists of all polynomials whose constant coefficient is even.

Theorem

An ideal $P \subseteq R$ is prime iff R/P is an integral domain.

The proof is straightforward (HW). Since fields are integral domains, the following is immediate:

Corollary

In a commutative ring, every maximal ideal is prime.