Ideals and Factor Rings

Diana Mary George
Assistant Professor
Department of Mathematics
St. Mary's College
Thrissur-680020
Kerala

Ideal

A subring A of a ring R is called a (two-sided) ideal of R if for every $r \in R$ and every $a \in A$ both ra and ar are in A.

Theorem 1 (Ideal Test):

A nonempty subset A of a ring R is an ideal of R if

1. $a - b \in A$ whenever $a, b \in A$.

2. ra and ar are in A whenever $a \in A$ and $r \in R$.

EXAMPLE **1:**

For any ring R, {0} and R are ideals of R. The ideal {0}is called the trivial ideal.

EXAMPLE **2:**

For any positive integer n, the set nZ = {0, $\pm$n, $\pm$ 2n,…} is an ideal of Z.

EXAMPLE **3:**

Let R be a commutative ring with unity and let a ∈ R.
The set < a > = { ra | r ∈R} is an ideal of R called the principal ideal generated by a.

EXAMPLE 4:

Let R be a commutative ring with unity and let $a_1, a_2, \ldots, a_n \in$ R. Then I = < $a_1, a_2, \ldots, a_n$> ={$r_1 a_1, r_2 a_2, \ldots, r_n a_n$|r ∈ R} is an ideal of R called the ideal generated by $a_1, a_2, \ldots, a_n$.

Existence of Factor Rings

Let R be a ring and let A be a subring of R.
The set of cosets $\{ r + A \mid r \in R\}$ is a ring under the operations
$(s + A) + (t + A) = s + t + A$ and
$(s + A)(t + A) = st + A$ if and only if A is an ideal of R.

EXAMPLE **5:**

$Z/4Z = \{0 + 4Z, 1 + 4Z, 2 + 4Z, 3 + 4Z\}$.
To see how to add and multiply, consider $2 + 4Z$ and $3 + 4Z$.
$(2 + 4Z) + (3 + 4Z) = 5 + 4Z = 1 + 4 + 4Z = 1 + 4Z$,
$(2 + 4Z)(3 + 4Z) = 6 + 4Z = 2 + 4 + 4Z = 2 + 4Z$.
One can readily see that the two operations are essentially modulo 4 arithmetic.

EXAMPLE **9:**

$2Z/6Z = \{0 + 6Z, 2 + 6Z, 4 + 6Z\}$. Here the operations are essentially modulo 6 arithmetic. For example,
$(4 + 6Z) + (4 + 6Z) = 2 + 6Z$ and $(4 + 6Z)(4 + 6Z) = 4 + 6Z$.

EXAMPLE **10:**

Consider the factor ring of the Gaussian integers $R = Z[i]/\langle 2 - i \rangle$. The elements of R have the form $a + bi + \langle 2 - i \rangle$, where a and b are Similarly, all the elements of R can be written in the form $a + \langle 2 - i \rangle$ where a is an integer. We can show that every element of R is equal to one of the following cosets: $0 + \langle 2 - i \rangle$, $1 + \langle 2 - i \rangle$, $2 + \langle 2 - i \rangle$, $3 + \langle 2 - i \rangle$, $4 + \langle 2 - i \rangle$. In fact R is same as Z_5.

EXAMPLE **11:**

Let $\mathbf{R}[x]$ denote the ring of polynomials with real coefficients and let $< x^2+1>$ denote the principal ideal generated by x^2+1

$< x^2+1> = \{ f(x)(x^2+1) \mid f(x) \in \mathbf{R}[x]\}$.

Then $\mathbf{R}[x]/< x^2+1> = \{ g(x) + < x^2+1> \mid g(x) \in \mathbf{R}[x]\}$

If $g(x) \in \mathbf{R}[x]$, then $g(x) = q(x)(x^2+1) + r(x)$, where $q(x)$ is the quotient and $r(x)$ is the remainder upon dividing $g(x)$ by x^2+1.

In particular, $r(x) = 0$ or the degree of $r(x)$ is less than 2, so that $r(x) = ax + b$ for some a and b in $\mathbf{R}$. Thus,

$$g(x) +< x^2+1> = q(x)(x^2+1) + r(x) + < x^2+1> = r(x) + < x^2+1>$$
$$= ax + b +< x^2+1>$$

$$\therefore \mathbf{R}[x]/< x^2+1> =\{ax + b + < x^2+1> \mid a,b \in \mathbf{R} \}$$

Prime Ideals

A prime ideal A of a commutative ring R is a proper ideal of R such that a, b ∈ R and ab ∈ A imply a ∈ A or b ∈ A.

Maximal Ideals

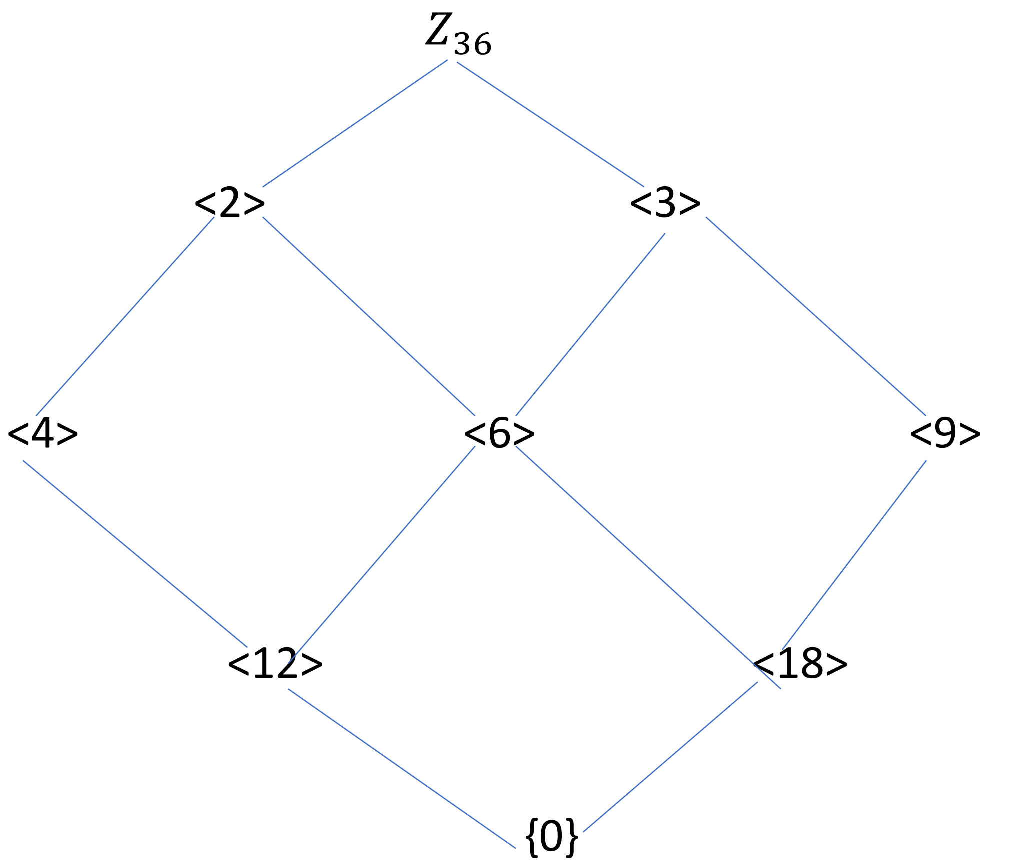
A maximal ideal of a commutative ring R is a proper ideal of R such that, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then B = A or B = R.

EXAMPLE 12

Let n be an integer greater than 1.
In the ring of integers, the ideal nZ is prime if and only if n is prime
{0} is also a prime ideal of Z.

EXAMPLE **13**

The lattice of ideals of Z_{36} shows that only < 2 > and <3> are maximal ideals



EXAMPLE **15:**

The ideal $< x^2+1 >$ is maximal in **R**[x].
To see this, assume that A is an ideal of **R**[x] that properly contains $< x^2+1 >$. We will prove that A = **R**[x] by showing that A contains some nonzero real number c. (This is the constant polynomial h(x) = c for all x.) Then $1 = (1/c)c \in A$ and therefore, A = **R**[x].
To this end, let $f(x) \in A$, but $f(x) \notin < x^2+1 >$.
Then $f(x) = q(x)(x^2+1) + r(x)$, where $r(x) \neq 0$ and the degree of r(x) is less than 2. It follows that r(x) = ax + b, where a and b are not both 0, and $ax + b = r(x) = f(x) - q(x)(x^2+1) \in A$
Thus, $a^2x^2 - b^2 = (ax + b)(ax - b) \in A$
So $0 \neq a^2+b^2 = (a^2x^2 + a^2) - (a^2x^2 - b^2) \in A$

Theorem 2

Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is an integral domain if and only if A is prime.

Theorem 3

Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is a field if and only if A is maximal.

EXAMPLE **17**

The ideal $\langle x \rangle$ is a prime ideal in $Z[x]$ but not a maximal ideal in $Z[x]$. To verify this, we begin with the observation that $\langle x \rangle = \{ f(x) \in Z[x] \mid f(0) = 0\}$ .Thus, if $g(x)h(x) \in \langle x \rangle$ then $g(0)h(0) = 0$. And since $g(0)$ and $h(0)$ are integers, we have $g(0) = 0$ or $h(0) = 0$.To see that $\langle x \rangle$ is not maximal, we simply note that $\langle x \rangle \subset \langle x,2 \rangle \subset Z[x]$

FACTORISATION OF POLYNOMIALS OVER A FIELD

Preliminaries

- Let R be a ring with unity $1 \neq 0$. An element u in R is a unit of R if it has a multiplicative inverse in R.
- If every non zero element of R is a unit then R is a division ring.
- A field is a commutative division ring.
- Let F be a field. Let F[x] denote set of all polynomials with indeterminate x of finite degree with coefficients from field F. F[x] is a ring.

DIVISION ALGORITHM IN F[x]

Let f(x)=$\sum_{i=0}^{n} a_i\, x^i$, g(x)=$\sum_{i=0}^{m} b_i x_i$ ∈ F[x] then there are unique polynomials q(x) and r(x) in F[x] such that f(x) =g(x)q(x)+r(x) where either r(x)=0 or the degree of r(x) ≤ degree of g(x)

FACTOR THEOREM

An element a∈ F is a zero of f(x) ∈ F[x] if and only if x-a is a factor of f(x) in F[x].

COROLLARY 1:

A nonzero polynomial $f(x) \in F[x]$ of degree n can have atmost n zeros in a field F.

COROLLARY 2:

If G is a finite subgroup of the multiplicative group $(F-\{0\}, *)$ of a field F, Then G is cyclic.

IRREDUCIBLE POLYNOMIALS

A nonconstant polynomial $f(x) \in F[x]$ is irreducible over F if $f(x)$ cannot be expressed as a product $g(x)h(x)$ of two poynomials $g(x)$ and $h(x)$ in $F[x]$ both of lower degree than the degree of $f(x)$.

THEOREM 1:

Let $f(x) \in F[x]$ be of degree 2 or 3. Then $f(x)$ is reducible over F if and only if it has a zero in F.

THEOREM 2:

If $f(x) \in \mathbb{Z}[x]$ then $f(x)$ factors into a product of two polynomials of lower degrees r and s in $\mathbb{Q}[x]$ if and only if it has such a factorization with polynomials of the same degrees r and s in $\mathbb{Z}[x]$.

COROLLARY 3:

If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is in $\mathbb{Z}[x]$ with $a_0 \neq 0$ and if $f(x)$ has a zero in $\mathbb{Q}$ then it has a zero m in $\mathbb{Z}$ and m must divide a_0.

EISENSTEIN CRITERION

Let $p \in \mathbb{Z}$ be a prime. Suppose that $f(x) = a_n x_n + a_{n-1}x^{n-1} + \cdots + a_0$ is in $\mathbb{Z}[x]$ and $a_n \neq 0\ mod\ p$ but a_i=0 mod p for all $i < n$ with $a_0 \neq 0\ mod\ p^2$. Then $f(x)$ is irreducible over $\mathbb{Q}$.

COROLLARY 4:

The polynomial

Φ_p(x)= $\frac{x^p - 1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$ for any prime p.

THEOREM 4:

Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides $r(x)s(x)$ for $r(x), s(x) \in F[x]$ then either $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$.

COROLLARY 5:

If $p(x)$ is irreducible in $F[x]$ and $p(x)$ divides the product $r_1(x)r_2(x) \ldots r_n(x)$ for $r_i(x) \in F[x]$ then $p(x)$ divides $r_i(x)$ atleast one i.

THEOREM 5:

If F is a field then every non constant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials the irreducible polynomials being unique except for order and for unit factors in F.


Thank you

Proof Existence :

The set of cosets forms a group under addition. The multiplication is well-defined if and only if A is an ideal of R. To do this, suppose that A is an ideal and let $s + A = s' + A$ and $t + A = t' + A$. Then we must show that $st + A = s't'+A$.

$s = s'+ a$ and $t = t' + b$, where $a, b \in A$.

Then $st = (s' + a)(t' + b) = s't' + at' + s'b + ab$ and so

$$st + A = s't' + at' + s'b + ab + A = s't' + A .$$

Thus multiplication is well-defined when A is an ideal.

On the other hand, suppose that A is a subring of R that is not an ideal of R. Then there exist elements $a \in A$ and $r \in R$ such that $ar \notin A$ or $ra \notin A$. For convenience, let $ar \notin A$. Consider the elements $a + A = 0 + A$ and $r + A$. Clearly, $(a + A)(r + A) = ar + A$ but $(0 + A)(r + A) = 0.r + A = A$. Since $ar + A \neq A$, the multiplication is not well-defined and the set of cosets is not a ring

Proof Theorem 2:

Suppose that R/A is an integral domain and $ab \in A$.
Then $(a + A)(b + A) = ab + A = A$, the zero element of the ring R/A.
So,either $a + A = A$ or $b + A = A$; that is, either $a \in A$ or $b \in A$.
Hence A is prime.
To prove the other half, we first observe that R/A is a commutative ring with unity for any proper ideal A.
We show that when A is prime, R/A has no zero-divisors. So, suppose that A is prime and $(a + A)(b + A) = 0 + A = A$.
Then $ab \in A$ and, therefore, $a \in A$ or $b \in A$.
Thus, one of $a + A$ or $b + A$ is the zero coset in R/A.

Proof Theorem 3:

Suppose that R/A is a field and B is an ideal of R that properly contains A. Let $b \in B$ but $b \notin A$. Then $b + A$ is a nonzero element of R/A and, therefore, there exists an element $c + A$ such that $(b + A)\ (c + A) = 1 + A$, the multiplicative identity of R/A. Since $b \in B$, we have $bc \in B$. Because $1 + A = (b + A)(c + A) = bc + A$, We have $1 - bc \in A \subset B$. So, $1 = (1 - bc) + bc \in B$. Therefore $B = R$. This proves that A is maximal.

Now suppose that A is maximal and let $b \in R$ but $b \notin A$. It suffices to show that $b + A$ has a multiplicative inverse. All other properties

for a field follow trivially. Consider $B = \{ br + a \mid r \in R, a \in A\}$. This is an ideal of R that properly contains A .Since A is maximal, we must have B = R. Thus, $1 \in B$, say, $1 = bc + a'$, where $a' \in A$.

Then $1 + A = bc + a' + A = bc + A = (b + A)(c + A)$.

When a commutative ring has a unity, it follows that a maximal ideal is a prime ideal.