IDHAYA COLLEGE FOR WOMEN, KUMBAKONAM

DEPARTMENT OF MATHEMATICS

SUBJECT NAME	**:**	**ABSTRACT ALGEBRA**
SUBJECT CODE	**:**	**16SCCMM12**
CLASS	**:**	**III B.Sc., MATHEMATICS**
SEMESTER	**:**	**VI**
TOPICS COVERED	**:**	**UNIT V**
STAFF NAME	**:**	**Dr. T. RAJESWARI**

Unit v

Maximal and Prime Ideal

Definition 1 Maximal ideal

Let R be a ring. An ideal $M \neq R$ is said to be a maximal ideal of R if whenever U is an ideal of R such that $M \subset U \subset R$ then either $U = M$ or $U = R$. That is, there is no proper ideal of R properly containing M.

Example 2 (2) is a maximal ideal in Z.

For, let U be an ideal properly containing (2).

Therefore U contains an odd integer say, $2n + 1$.

Therefore $1 = (2n + 1) - 2n \in U$. Therefore $U = Z$.Thus there is no proper ideal of Z properly containing (2)

Hence (2) is a maximal ideal of Z.

Definition 3 Let R be a commutative ring. An ideal $P \neq R$ is called a prime ideal if $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$

Example 4 Let R be an integral domain. (0) is a prime ideal of R.

For, $ab \in (0) \Rightarrow ab = 0$

$\Rightarrow a = 0$ or $b = 0$(Since R is an I.D)

$\Rightarrow a \in (0)$ or $b \in (0)$

Definition 5 Let R and $R^{'}$ be rings. A function $f : R \to R^{'}$ is called a homomorphism if

i $f(a + b) = f(a) + f(b)$ and

ii $f(ab) = f(a)f(b)$ for all $a, b \in R$

Example 6 Let $f : RXR \to R$ given by $f(x, y) = x$ is a ring homomorphism.

For,

$$\begin{aligned} f(a,b)+f(c,d) &= f((a+c,b+d) \\ &= a+c \\ &= f(a,b)+f(c,d) \end{aligned}$$

Also, $f(a,b)+f(c,d)=f(ac,bd)=f(a,b)f(c,d)$

Definition 7 The kernel K of a homomorphism f of a ring R to a ring $R^{'}$ is defined by

$\{a/a \in R$ and $f(a)=0\}$

Definition 8 Let R be a commutative ring without zero-divisors. R is called an Euclidean domain or an Euclidean ring if for every non-zero element $a \in R$ there is defined a non-negative integer $d(a)$ satisfying the following conditions

- (i) For any two non-zero elements $a, b \in R, d(a) \leq d(ab)$
- (ii) For any two non-zero elements $a, b \in R$, there exist $a, r \in R$ such that $a = qb + r$ where either $r = 0$ or $d(r) < d(b)$

Example 9 Z is an Euclidean domain where $d(a) = |a|$

Proof

$d(ab) = |ab| = |a||b| \geq |a| = d(a)$.

Let a, b be two non-zero elements of Z. Let q be the quotient and r be the remainder when a is divided by b.

Then $a = qb + r$ and $0 \leq r < |b|$

Hence Z is an Euclidean domain.

Example 10 Two elements a and b of an Euclidean domain R are said to be relatively prime if their g.c.d is unit in R.

Theorem 11 Let R be any commutative ring with identity. Let P be an ideal of R. Then P is a prime ideal iff R/P is an integral domain

Proof

Let P be a prime ideal.

Since R is a commutative ring with identity R/P is also commutative ring with identity.

Now,

$$\begin{aligned}(P+a)(P+b) &= P+0\\ &\Rightarrow P+ab=P\\ &\Rightarrow ab\in P\end{aligned}$$

$\Rightarrow a\in P$ or $b\in P$ (since P is a prime ideal)

$\Rightarrow P+a=P$ or $P+b=P$

Thus R/P has no zero divisors.

Therefore R/P is integral domain.

Conversely,

suppose R/P is an integral domain.

We have to prove P is a prime ideal of R.

Let $ab\in P$. Then $P+ab=P$.

Therefore $(P+a)(P+b)=P$.

Therefore $P+a=P$ or $P+b=P$.(since R/P has no zero divisors).

Therefore $a\in P$ or $b\in P$.

Thus P is a prime ideal of R.

Hence Let R be any commutative ring with identity. Let P be an ideal of R. Then P is a prime ideal iff R/P is an integral domain

Theorem 12 The Fundamental theorem of ring homomorphism

Statement

Let R and $R^{'}$ be rings and $f : R \to R^{'}$ be an epimorphism. Let K be the kernel of f. Then $R/K \simeq R^{'}$

Proof

Define $\varphi R/K \to R^{'}$ by $\varphi(K+a) = f(a)$.

(i) φ is well defined, for let $K+b = K+a$.

Then $b \in K+a$.

Therefore $b = k+a$ where $k \in K$

Therefore $f(a) = f(k+a) = f(k)+f(a) = 0+f(a) = f(a)$

Therefore $\varphi(K+b) = f(b) = f(a) = \varphi(K+a)$

(ii)φ is 1-1.

For,

$$\begin{aligned}
\varphi(K+a) = \varphi(K+b) \Rightarrow f(a) &= f(b) \\
&\Rightarrow f(a) - f(b) = 0 \\
&\Rightarrow f(a) + f(-b) = 0 \\
&\Rightarrow f(a-b) = 0 \\
&\Rightarrow a-b \in K \\
&\Rightarrow a \in K+b \\
&\Rightarrow K+a = K+b \\
\varphi(K+a) = \varphi(K+b) &\Rightarrow K+a = K+b
\end{aligned}$$

(iii)φ is onto

For, let $a^{'} \in R^{'}$

Since f is onto, there exists $a^{'} \in R$ such that $f(a) = a^{'}$.

Hence $f(a) = a^{'}$.

Hence $\varphi(K+a) = f(a) = a^{'}$

(iv) φ is homomorphism.

For,

$$\begin{aligned}
\varphi[(K+a)(K+b)] &= \varphi[K+(a+b)] \\
&= f(a+b) \\
&= f(a)+f(b), since f is a homomorphism \\
&= \varphi(K+a)+\varphi(K+b) \\
\varphi[(K+a)(K+b)] &= \varphi(K+ab) \\
&= f(ab) \\
&= f(a)f(b) since f is homomorphism
\end{aligned}$$

$\varphi(K+a)\varphi(K+b)$

Hence φ is an isomorphism.

Hence $R/K \simeq R^{'}$

Theorem 13 Let R be a ring and I be a subgroup of $(R,+)$. The multiplication in R/I given by $(I+a)(I+b) = I+ab$ is well defined iff I is an ideal of R

Proof

Let I be an ideal R.

To prove multiplication is well defined, let $I+a_1 = I+a$ and $I+b+1 = I+b$

Then $a_1 \in I+a$ and $b_1 \in I+b$

Therefore $a_1 = i_1+a$ and $b_1 = i_2+b$ where $i_1, i_2 \in I$

Hence $a_1b_1 = (i_1+a)(i_2+b) = i_1i_2+i_1b+ai_2+ab$

Now since I is an ideal we have $i_1i_2, i_1b, ai_2 \in I$

Hence $a_1b_1 = i_3$ where $i_3 = i_1i_2+i_1b+ai_2 \in I$

Therefore $a_1b_1 \in I + ab$

Hence $I + ab = I + a_1b_1$ Conversely,

Suppose that the multiplication in R/I given by $(I+a)(I+b) = I+ab$ is well defined.

To prove that I is an ideal of R.

Let $i \in I$ and $r \in R$. We have to prove that $ir, ri \in I$

Now,

$$\begin{aligned} I + ir &= (I+i)(I+r) \\ &= (I+0)(I+r) \\ &= I + or \\ &= 0 \end{aligned}$$

Therefore $ir \in I$

Similarly,

$$\begin{aligned} I + ri &= (I+r)(I+i) \\ &= (I+r)(I+0) \\ &= I + r0 \\ &= 0 \end{aligned}$$

Therefore $ri \in I$

Hence I is and ideal.

Hence Let R be a ring and I be a subgroup of $(R,+)$. The multiplication in R/I given by $(I+a)(I+b) = I+ab$ is well defined iff I is an ideal of R

Definition 14 Let R be any ring and I be an ideal of R. Well-defined binary operations in R/I given by $(I+a)+(I+b) = I+(a+b)$ and $(I+a)(I+b) = I+ab$. The ring R/I is called quotient ring of R modulo I.

Example 15 The subset $I = \{0, 3\}$ of Z_6 is an ideal.

Solution

$Z_6/I = \{I, I+1, I+2\}$ is a ring isomorphic to Z_3.

Here Z_6 is not an integral domain but the quotient ring Z_6/I is an integral domain.

Theorem 16 Let R be an Euclidean domain and I be an ideal of R. Then there exists an element $a \in I$ such that $I = aR$. (i.e.,) Every ideal of an Euclidean domain is a principal ideal.

Proof

If $I \neq 0$, then we take $a = 0$. Hence we assume that $I \neq 0$.

Let$a \in I$ be a non-zero element such that $d(a)$ is minimum.

Now, we claim that $I = aR$

Let $x \in I$. Then there exist $q, r \in R$ such that $x = qa + r$ where $r = 0$ or $d(r) < d(a)$.

Now $a \in I \Rightarrow qa \in I$

Also $s \in I$. Hence $r = x - qa \in I$.

Now, suppose $r \neq 0$. Then $d(r) < d(a)$ which is contradiction to the choice of a and hence $r = 0$.

Therefore $x = qa$ and hence $I = aR$

Theorem 17 Any Euclidean domain R has an identity element.

Since R is an ideal of R, there exists $c \in R$ such that $R = cR$.

Therefore Every element of R is a multiple of c.

In particular $c = ec$ for some $e \in R$.

Now, let $x \in R$. Then $x = cy$ for some $y \in R$

Therefore

$$\begin{aligned} ex &= e(cy) \\ &= (ec)y \\ &= cy \\ &= x \\ ex &= x \end{aligned}$$

Therefore e is the required identity element.

Hence Any Euclidean domain R has an identity element.

Theorem 18 Let a be a non-zero element of an Euclidean domain R. Then a is unit in R iff $d(a) = d(1)$

Proof

Suppose a is a unit in R.

Therefore $d(a) = d(aa^{-1})$

$= d(1)$

Therefore $d(a) = d(1)$.

Conversely,

Let $d(a) = d(1)$

Suppose a in not a unit in R.

Then $d(1.a) > d(1)$

Therefore $d(a) > d(1)$ which is contradiction.

Therefore a is a unit.

Hence let a be a non-zero element of an Euclidean domain R. Then a is unit in R iff $d(a) = d(1)$

Theorem 19 Let R be an Euclidean domain. Let $a, b, c \in R$. Then $a|bc$ and $(a, b) = 1 \Rightarrow a|c$

Proof

Let R be an Euclidean domain.

Let $a, b, c \in R$.

We have to prove $a|bc$ and $(a, b) = 1 \Rightarrow a|c$

Since $(a, b) = 1$, there exist $s, y \in R$ such that $ax + by = 1$.

Therefore $acx + bcy = c$.

Now, $a|acx$.

Also $a|bc \Rightarrow a|bcy$.

Therefore $a|(acx + bcy)$.

Hence $a|c$.

Theorem 20 Let R be an Euclidean domain R. Let a and b two non-zero elements of R.Then

- (i) b is not a unit in $R \Rightarrow d(a) < d(ab)$

- (ii) b is a unit in $R \Rightarrow d(a) = d(ab)$

Proof

(i) Suppose b is not a unit in R.

By definition of Euclidean domain there exist elements $q, r \in R$ such that $a = q(ab) + r$——(1)

where either $r = 0$ or $d(r) < d()ab$.

Now, suppose $r = 0$ then $a = q(ab)$

Therefore $a - q(ab) = 0 \Rightarrow a(1 - qb) = 0$

Now, R has no zero-divisors and $a \neq 0$.

Therefore $1 - qb = 0$. Hence $qb = 1$.

Therefore b is a unit in R which is a contradiction.

Therefore $r \neq 0$. Hence $d(a) < d(ab)$ ———(2)

Now $r = a(1 - qb)$ by (1)

Therefore $d(r) = d[a(1 - qb)] \geq d(a)$————(3)

Therefore $d(a) \leq d(r) < d(ab)$

(ii) Suppose b is a unit in R.

Now, $d(a) \leq d(ab)$.

Also, $d(a) = d[(ab)b^{-1}] \geq d(ab)$.

Therefore $d(a) \leq d(ab)$. Therefore $d(a) = d(ab)$