UNIT-3.

Rings:

* A nonempty set R together with two binary operations denoted by '+' and '.' and called addition, multiplication which satisfy the following axioms is called a ring.

  * $(R, +)$ is an abelian group.

Eg: * $(2\mathbb{Z}, +, \cdot)$ is a ring

  * $(\mathbb{Z}, +, \cdot)$; $(\mathbb{Q}, +, \cdot)$ are all rings

4.2 Elementary Properties of rings:

Theorem: 4.1 Let R be a ring and $a, b \in R$. Then (i) $0a = a0 = 0$

(ii) $a(-b) = (-a)b = -ab$. (iii) $(-a)(-b) = ab$ (iv) $a(b-c) = ab - ac$.

Proof: (i) $a0 = a(0+0) = a0 + a0$.

$\therefore a0 = 0$ (by cancellation law in $(R, +)$) $\therefore$ similarly $0a = 0$.

(ii) $a(-b) + ab = a(-b+b) = a0 = 0$.

$\therefore a(-b) = -(ab)$

Similarly $(-a)b = -(ab)$.

(iii) By (ii) $(-a)(-b) = -[a(-b)] = -(-ab) = ab$.

(iv) $a(b-c) = a[b+(-c)] = ab + a(-c)$

$= ab - ac$

(2 solved problems) in Page number 4.4.

4.3 Isomorphism:

Let $(R, +, \cdot)$ and $(R', +, \cdot)$ be two rings. A bijection $f: R \to R'$ is called an isomorphism if

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

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

If $f: R \to R'$ is an isomorphism, we say that R is isomorphic to R' and we write $R \cong R'$.

Note: Let R and R' be two rings and $f: R \to R'$ be an isomorphism. Then clearly f is an isomorphism of the group $(R, +)$ to the group $(R', +)$

Hence $f(0) = 0'$ and $f(-a) = -f(a)$.

Scanned by CamScanner

4.4 Types of rings:

A ring R is said to be commutative $ab=ba$ for all $a,b \in R$.

Definition: Let R be a ring. We say that R is a ring with identity if there exists an element $1 \in R$ such $a1=1a=a$ for $a \in R$

eg: $M_2(R)$ is a ring with identity.

Theorem 4.2: In a ring with identity the identity element is unique

Let $1, 1'$ be multiplicative identities. Then $1.1'=1$ (Considering $1'$ as identity) and $1.1'=1'$ (considering 1 as identity)

$\therefore 1=1'$ Hence the identity element is unique.

Definition: Let R be a ring with identity. An element $u \in R$ is called a unit in R if it has a multiplicative inverse of u is denoted by u^{-1}.

For example in $(\mathbb{Z}, +, \cdot)$ 1 and -1 are units.

In $M_2(R)$ all the non singular matrices are units.

In Q, R and C every non-zero element is a unit.

Theorem 4.3: Let R be a ring which identity. The set of all units in R is a group under multiplication.

Let U denote the set of all units in R.

Clearly $1 \in U$. Let $a, b \in U$. Hence a^{-1}, b^{-1} exists in R.

Now $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1a^{-1} = aa^{-1} = 1$

Similarly $(b^{-1}a^{-1})(ab)=1$.

Hence $ab \in U$. Also $(a^{-1})^{-1}=a$ and hence $a \in U \Rightarrow a^{-1} \in U$.

Hence U is a group under multiplication.

Definition: Let R be ring with identity element. R is called a skew field or a dividing ring if every non zero element in R is a unit.

Scanned by CamScanner

For every non element $a \in R$, there exists a Multiplication inverse $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Thus in a skew field the non-zero element form a group under Multiplication.

Definition: * A commutative skew field is called a field.

* In other words a field is a system $(F, +, \cdot)$ satisfying the following conditions.

(i) $(F, +)$ is an abelian groups.

(ii) $(F - \{0\}, \cdot)$ is an abelian groups.

$a \cdot (b+c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$

Theorem: 4.4 In a skew field R,

(i) $ax = ay, a \neq 0 \Rightarrow x = y$ } cancellation laws in ring }

(ii) $xa = ya, a \neq 0 \Rightarrow x = y$ }

(iii) $ax = 0 \Leftrightarrow a = 0$ or $x = 0$

Proof: (i) Let $ax = ay$ and $a \neq 0$.

Since R is a skew field there exists $a^{-1} \in R$.

Such that $aa^{-1} = a^{-1}a = 1$

Hence $ax = ay \Rightarrow a^{-1}(ax) = a^{-1}(ay) \Rightarrow x = y$

(ii) Can be Proved similarly.

(iii) If $a = 0$ or $x = 0$, then clearly $ax = 0$ Conversely let $ax = 0$ and $a \neq 0$ $\therefore ax = a0$

$x = 0$ by (i)

Definition: Let R be a ring. A non zero element $a \in R$ is said to be a zero-divisor if there exists a non-zero element $b \in R$ such that $ab = 0$ or $ba = 0$.

Theorem: 4.5. A ring R has no zero-divisors iff cancellation law is valid in R.

Let R be a ring without zero-divisors

Let $ax = ay$ and $a \neq 0$

$\therefore ax - ay = 0$. Hence $a(x-y) = 0$ and $a \neq 0$

$\therefore x - y = 0$ (since R has no zero divisors).

Scanned by CamScanner

$\therefore a = y$ Thus cancellation law be valid in R.

Let $ab = 0$ and $a \neq 0$. Then $ab = 0 = a0$.

Hence by cancellation law $b = 0$

Hence R has no zero-divisors.

Theorem: 4.6 Any unit in R cannot be a zero-divisor.

Proof: Let $a \in R$ be a unit. Then $ab = 0 \Rightarrow a^{-1}(ab) = 0 \Rightarrow b = 0$

Similarly $ba = 0 \Rightarrow b = 0$

Hence a cannot be a zero-divisor.

Definition: A commutative ring with identity having no zero-divisors is called an integral domain.

Thus is an integral domain $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$ or equivalently $ab = 0$ and $a \neq 0 \Rightarrow b = 0$; or $a \neq 0$ and $b \neq 0 \Rightarrow ab \neq 0$.

Theorem 4.7 Z_n is an integral domain iff n prime.

Let Z_n be an integral domain.

We claim that n is prime. Suppose n is not prime.

Then $n = pq$ where $1 < p < n$ and $1 < q < n$.

Clearly $p \otimes q = 0$.

Hence p and q are zero-divisors.

$\therefore Z_n$ is not an integral domain which is a contradiction.

Hence n is prime.

Conversely, suppose n is prime. Let $a, b \in Z_n$.

Then $a \otimes b = 0 \Rightarrow ab = qn$ where $q \in Z_n$

$\Rightarrow n \mid ab$

$\Rightarrow n \mid a$ or $n \mid b$ (Since n is prime)

$\Rightarrow a = 0$ or $b = 0$

$\therefore Z_n$ has no zero divisors. Also Z_n is a commutative ring with identity. Hence Z_n is an integral domain.

Theorem: 4.8 Any field is an integral domain:-

It is enough if we prove that F has no zero divisors

Scanned by CamScanner

Let $a, b \in F$, $ab = 0$ and $a \neq 0$.

Since F is a field a^{-1} exists. Now, $ab = 0 \Rightarrow a^{-1}(ab) = 0$

$\Rightarrow b = 0$

$\therefore$ F has no zero-divisors.

Hence F is an integral domain.

Theorem 4.9 Let R be a commutative ring with identity 1. Then R is an integral domain iff the set of non-zero elements in R is closed under Multiplication.

Let R be an Integral domain. Let $a, b \in R - \{0\}$ since R has no zero-divisors $ab \neq 0$ so that $R - \{0\}$ is closed under Multiplication. Conversely, suppose $R - \{0\}$ is Productor of any two non-zero element is a non zero element. Hence R has no zero-divisors so that R is an integral domain.

Theorem 4.10 Let R be a Commutative ring with identity. Then R is an integral domain iff cancellation law is valid in R.

The result is an immediate consequence of Theorem 4.5

Theorem 4.11 Any finite integral domain is a field.

Let R be a finite integral domain. We need to only to Prove that every non-zero element in R has a multiplicative inverse. Let $a \in R$ and $a \neq 0$

Let $R = \{0, 1, a_1, a_2 \ldots an\}$

Consider $\{a1, 0a_1, aa_2 \ldots aan\}$.

By theorem 4.9 all these elements are non-zero and all these elements are distinct by Theorem 4.10.

Hence $aa_i = 1$ for some $a_i \in R$. Since R is commutative $aa_i = a_i a = 1$ so that $a_i = a^{-1}$.

Hence R is a field.

Theorem 4.12 Z_n is a field iff n is prime

By theorem 4.7 Z_n is an integral domain iff n is Prime. further Z_n is finite. Hence the result follows from theorem 4.11

Scanned by CamScanner

Theorem 4.13 A finite commutative ring R without zero divisors is a field

If we prove that R has an identity element then R becomes an integral domain and hence by the theorem 4.11 it is field. So we prove the existence of identity

Let $R=\{0,a_1,\cdots a_n\}$

Let $a\in R$ and $a\neq 0$. Then the elements $aa_1, aa_2, \cdots aa_n$ are distinct and non zero.

$\therefore aa_i=a$ for some i. Since R is commutative we have $aa_i=a_ia=a$. we now p.t a_i is identity element of R. Let $b\in R$. Then $b=aa_j$ for some j.

$\therefore a_ib=a_i(aa_j)=(a_ia)a_j=aa_j=b$.

Thus $a_ib=ba_i=b$

Since $b\in R$ is arbitary a_i is Identity R.

Hence the theorem.

Solved Problems (9 Sums) in 4.11.

4.5 Characteristic of a ring:

Let R be a ring. If there exists a positive integer n such that $na=0$ for all $a\in R$ then the least such positive integer is called the characteristic of the ring R. If no such positive integer exists then the ring is said to be characteristic zero.

4.14 Let R be a ring with identity 1. If 1 is an element of finite order in the group $(R,+)$ then the order of 1 is the characteristic of R. If 1 is of infinite order, the characteristic of the ring is 0.

Suppose the order of 1 is n. Then n is the least positive integer such that $n.1=0$.

(i.e) $1+1+\cdots+1$ (n times) $=0$ Now. let $a\in R$

Then $na=a+a+\cdots+a$ (n times)

$=1.a+1.a+\cdots+1.a$

$=(1+1+\cdots+1)a$

$=0.a$

$=0$

Scanned by CamScanner

Thus $na=0$ for all $a \in R$.

Hence the characteristic of the ring is n.

If a is of infinite order then there is no positive integer n such that $n.1=0$. Hence the characteristic of the ring is 0.

Theorem 4.15 The characteristic of an integral domain D is either 0 or a prime number.

If the characteristic of D is 0 then there is nothing to prove. If not be the characteristic of D be n.

If n is not prime, let $n=pq$, where $1<p<n$ and $1<q<n$

Since characteristic of D is n we have $n.1=0$

Hence $n.1 = pq.1 = (p.1)(q.1)=0$. Since D is an integral domain either $p.1=0$ or $q.1=0$

Since p, q are both less than n, this contradicts the definition of the characteristic of D.

Hence n is a prime number.

Corollary: The characteristic of any field is either 0 or a prime number

Proof: Since every field is an integral domain the result follows

Note: The characteristic of an arbitary ring need not be prime for example Z_6 is of characteristic 6.

The converse of the above theorem is not true (i.e) If the characteristic of a ring R is prime then R need not be an integral domain. Eg: ring $(\mathcal{P}(S), \Delta, \cap)$ is of characteristic 2 but it is not an integral domain. If A and B are two disjoint nonempty subsets of S we have $A \cap B \neq 0$ and hence A and B are zero divisors in $\mathcal{P}(S)$.

Theorem 4.16 In an integral domain D of characteristic p, the order of every element in the additive group is p.

Let $a \in D$ be any non-zero element.

Let the order of a be n. Then n is the least positive integer such that $na=0$. Now, by the definition of the characteristic of D we have $pa=0$

Scanned by CamScanner

Hence n/p Now since p is prime $n=1$ or $n=p$

If $n=1$, $na=a=0$ which is contradiction.

Hence $n=p$ Thus the order of a is p

Note: The above result is not true for ~~identity~~ arbitrary ring. eg: the characteristic of the ring Z_6 is 6 whereas the order of $2 \in Z_6$ is 3.

4.6 Subrings:

A non empty subset S of a ring $(R, +, \cdot)$ is called a subring if S itself is a ring under the same operation as in R

eg: $2Z$ is a subring of Z

Z is a subring of Q.

4.17 A non-empty subset S of a ring R is a subring iff $a, b \in S \Rightarrow a-b \in S$ and $ab \in S$.

Let S be a subring of R. Then $(S, +)$ is a subgroup of $(R, +)$. Hence $a, b \in S \Rightarrow a-b \in S$. Also since S itself is a ring $ab \in S$. Conversely, let S be a non-empty subset of R such that $a, b \in S \Rightarrow a-b \in S$ and $ab \in S$.

Then $(S, +)$ is a subgroup of $(R, +)$

Also S is closed under multiplication. The associative and distributive laws are consequence of the consequences of corresponding laws in R.

Hence S is a subring.

Solved problems (3 sums) in pg. 4.17.

Theorem 4.18 The intersection of two subrings of a Ring R is a subring of R.

Let A, B be two subrings of R.

Let $a, b \in A \cap B$ Then $a, b \in A$ and B. Since A and B are subrings $a-b$ and $ab \in A$ and B

$\therefore a-b$ and $ab \in A \cap B$

$\therefore A \cap B$ is subring of R (by 4.17)

Scanned by CamScanner

Note: * The union of two subring of a ring need not be a subring.

* The union of two subrings of a ring is again a subring iff one is contained in the other (Proof 3.20)

Definition: A non-empty subset S of a field $(F, +, \cdot)$ is called a subfield if S itself is a field under the same operations as in F.

Eg: $\mathbb{Q}$ is a subfield R and R is subfield of C.

Theorem 4.19 A non empty subset S of a field F is a subfield iff

(i) $a, b \in S \Rightarrow a-b \in S$ and

(ii) $a, b \in S$ and $b \neq 0 \Rightarrow ab^{-1} \in S$.

The proof follows by applying Theorem 3.17 to group $(F, +)$ and $(F-\{0\}, \cdot)$

4.7 Ideals:

Let R be a ring. A non empty subset of R is called a left ideal of R if

(i) $a, b \in I \Rightarrow a-b \in I$.

(ii) $a \in I$ and $x \in R \Rightarrow xa \in I$.

I is called a right ideal of R if

(i) $a, b \in I \Rightarrow a-b \in I$

(ii) $a \in I$ and $x \in R \Rightarrow ax \in I$.

I is called an ideal of R if I is both a left ideal and a right ideal. Thus in an ideal the product of an element in the ideal and an element in the ring is an element of the ideal. In a commutative ring the concepts of the left ideal right ideal coincide.

Definition: If R is a commutative ring than $aR = Ra$ is an ideal. This is called the principal ideal generated by a and is denoted by (a).

Remark: * Every left ideal of a ring R is subring of R

Let I be a left ideal of R. Let $a, b \in I$. Then by definition $a-b$ and $ab \in I$. Hence I is a subring of R.

Scanned by CamScanner

* Similarly every right ideal of R is also a subring of R

* Any ideal of R is a subring of R. by (i) and (ii).

* However a subring of R need not be an ideal of R.

Theorem 4.20 Let R be ring with identity 1. If I is an ideal of R and $1 \in I$, then $I = R$

Obviously $I \subseteq R$. Now let $r \in R$. Since $1 \in I, r.1 = r \in I$. Thus $R \subseteq I$. Hence $R = I$.

Theorem 4.21 Let F be any field. Then the only ideals of F are $\{0\}$ and F. (i.e) A field has no proper ideals.

*Let I be an ideal of F. Suppose $I \neq \{0\}$. We shall Prove that $I = F$. Since $I \neq \{0\}$, there exists an element $a \in I$ such that $a \neq 0$.

*Since F is a field a has a multiplicative inverse $a^{-1} \in F$. Now, $a \in I$ and $a^{-1} \in F \Rightarrow aa^{-1} = 1 \in I$.

*Hence by theorem 4.20 $I = F$

Theorem 4.22 Let R be a commutative ring with identity. Then R is a field iff R has no proper ideals.

If R is a field, by theorem 4.21, R has no proper ideals. Conversely suppose R has no proper ideals.

To prove that R is a field we need to show that every non zero element in R has an inverse. Let $a \in R$ and $a \neq 0$.

Consider the principal ideal aReal.

Since R is a ring with identity $a = a.1 \in aR$.

$\therefore aR \neq \{0\}$. Since R has no proper ideals $aR = R$.

Hence there exits $x \in R$ such that $ax = 1$

Thus x is the inverse of a.

Hence R is a field.

Scanned by CamScanner

Definition: An integral domain R is said to be a Principle ideal domain (PID) if every ideal of R is a principal ideal

Eg: * $\mathbb{Z}$ is a principal ideal domain since any ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$.

* Any field F is a principal ideal domain since the only ideals of F are (0) and (1) = F (by 4.8.1)

4.8 Quotient Rings:

Theorem 4.23 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.

Let I be an ideal R.

TO P. Multiplication is well defined.

Let $I+a_1 = I+a$ and $I+b_1 = I+b$. Then $a_1 \in I+a$ and $b_1 \in I+b$.

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

Hence $a_1 b_1 = (i_1+a)(i_2+b) = i_1 i_2 + i_1 b + a i_2 + ab$

Now since I is an ideal we have $i_1 i_2, i_1 b, a i_2 \in I$.

Hence $a_1 b_1 = i_3 + ab$ where $i_3 = i_1 i_2 + i_1 b + a i_2 \in I$

$a_1 b_1 \in I + ab$.

Hence $I + ab = I + a_1 b_1$

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

T.P I is an ideal of R

Let $i \in I$ and $x \in R$. we have to Prove that $ix, xi \in I$.

Now, $I + ix = (I+i)(I+x) = (I+0)(I+x) = I+0x = I$

$\therefore ix \in I$. Similarly $xi \in I$.

Hence I is an ideal.

Definition: Let R be any ring and I be an ideal of R. we have two well defined binary operations in R/I gn by $(I+a)+(I+b) = I+(a+b)$ and $(I+a)(I+b) = I+ab$. It is easy to verify that R/I is a ring under these operations.

The ring R/I is called the quotient ring of R modulo I.

Scanned by CamScanner

4.9 Maximal and prime ideals:

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

Theorem: 4.24: Let R be commutative ring with identity An ideal M of R is maximal iff R/M is a field.

Let M be a maximal ideal in R.

Since R is a commutative ring with identity $M \neq R$, R/M is also a commutative ring with identity. Now, let $M+a$ be a non zero element in R/M so that $a \notin M$. we shall now prove that $M+a$ has a multiplicaties inverse in R/M.

Let $U = \{ ra+m / r \in R \text{ and } m \in M \}$

we claim that U in an ideal of R.

$(r_1a+m_1) - (r_2a+m_2) = (r_1-r_2)a + (m_1-m_2) \in U$

Also, $r(r_1a+m_1) = (rr_1)a + rm_1 \in U$ [since $rm_1 \in M$]

$\therefore$ U is an ideal of R.

Now, let $m \in M$. Then $m = 0a + m \in U$.

$\therefore M \subseteq U$. Also $a = 1a + 0 \in U$ and $a \notin M$

$\therefore M \neq U$. $\therefore$ U is an ideal of R properly containing M. But M is a maximal ideal of R.

$\therefore U = R$. Hence $1 \in U$.

$\therefore 1 = ba + m$ for some $b \in R$ Now,

$M+1 = M+ba+m = M+ba$ (since $m \in M$)

$= (M+b)(M+a)$

Hence $M+b$ is the inverse of $M+a$.

Thus every non-zero element of R/M has and inverse. Hence R/M is a field.

Conversely, suppose R/M is a field.

$\therefore$ Let U be any ideal of R properly containing M.

Scanned by CamScanner

$\therefore$ there exists an element $a \in U$ such that $a \notin M$.

$\therefore M+a$ is a non zero element of R/M.

Since R/M is a field $M+a$ has an inverse, say $M+b$,

$\therefore (M+a)(M+b) = M+1$.

$\therefore M+ab = M+1$. $\therefore 1-ab \in M$.

But $M \subseteq U$. Hence $1-ab \in U$. Also $a \in U$ $ab \in U$

$\therefore 1 = (1-ab)+ab \in U$. Thus $1 \in U$.

$\therefore U = R$. Thus there is no proper ideal of R properly containing M. Hence M is a maximal ideal in R.

Definition: 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 $b \in P$.

Theorem 4.25 Let R be any commutative ring with identity. Let P be an ideal of R. Then P is a prime ideal $\Leftrightarrow$ R/P is an integral domain.

Let P be prime ideal. Since R is a commutative ring with identity R/P is also commutative ring with identity.

Now, $(P+a)(P+b) = P+0$.

$\Rightarrow P+ab = P$

$\Rightarrow ab \in P$

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

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

Thus R/P has no zero divisors.

$\therefore R/P$ is an integral domain. Conversely, suppose R/P is an integral domain. We claim that 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 $b \in P$.

$\therefore P$ is a prime ideal of R.

Corollary: Let R be a commutative ring with identity. Then every maximal ideal of R is a prime ideal of R.

Scanned by CamScanner

Proof: Let M be maximal ideal of R

$\therefore$ R/M is a field (by theorem 4.24)

$\therefore$ M is a prime ideal (4.25

R/M is an integral domain. (by theorem 4.9

Note: The converse of the above statement is not true for example, (0) is prime ideal of $\mathbb{Z}$ but not a maximal ideal of $\mathbb{Z}$.

4.10 Homomorphism of rings:

Let R and R' be rings. A function $f: R \to R'$ is called homomorphism if

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

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

f is 1-1 f is called monomorphism, f is onto f is epimorphism

A homomorphism of a ring onto itself is called endomorphism

Theorem 4.26 Let R and R' be rings and $f: R \to R'$ be a homomorphism. Then, (See an IR book 4.25)

Proof: Since f is homomorphism of the group $(R,+)$ to $(R',+)$ the results (i) and (ii) follow from theorem 3.55

(iii) Since S is subring of R, $(S,+)$ is a subgroup of $(R,+)$ and hence $f(S)$ is a subgroup of $(R',+)$

Now let $a', b' \in f(S)$. Then $a' = f(a)$ and $b' = f(b)$ for some $a, b \in S$. $\therefore a'b' = f(a)f(b) = f(ab) \in f(S)$

Hence $f(S)$ is a subring of R'.

Let S be an ideal of R.

To prove that $f(S)$ is an ideal of $f(R)$ it is enough if we prove that $x' \in f(R)$ and $a' \in f(S) \Rightarrow x'a'$ and $a'x' \in f(S)$. Let $x' = f(x)$ and $a' = f(a)$ where $x \in R$ and $a \in S$.

Now since S is an ideal of R, xa and $ax \in S$.

Scanned by CamScanner

Hence $f(xa) = f(x)f(a) = x'a' \in f(S)$

Similarly $ax' \in f(S)$. Hence $f(S)$ is an ideal of $f(R)$.

(v) Let S' be a subring of R'. Since $(S', +)$ is a subgroup of $(R', +)$, $f^{-1}(S')$ is a subgroup of $(R, +)$

Now let $a, b \in f^{-1}(S')$ Then $f(a), f(b) \in S'$.

$\therefore f(ab) = f(a)f(b) \in S'$ (since S' is a subring of R')

$\therefore ab \in f^{-1}(S')$ Hence $f^{-1}(S')$ is a subring of R.

(vi) Proof is similar to that of (v)

(vii) Let R be ring with identity 1. let $a' \in f(R)$. Then $a' = f(a)$ for some $a \in R$. Now $a'f(1) = f(a)f(1) = f(a1) = f(a) = a'$

Similarly $f(1)a' = a'$. Also $f(1) \neq 0$.

Hence $f(1)$ is the identity of $f(R)$

(viii) Proof is left to the reader.

Definition: The kernel k of a homomorphism f of a ring R to ring R' is defined by $\{a / a \in R \text{ and } f(a) = 0\}$

Theorem 4.27: Let $f: R \to R'$ be a homomorphism. Let K be the kernel of f. Then K is an ideal of R.

Proof: By definition $K = f^{-1}(\{0\})$

Since $\{0\}$ as an ideal of $f(R)$, by (vi) of theorem 4.26 K is an ideal of R.

Scanned by CamScanner