Computer Algebra

2-1-19

- Algebraic Numbers: Prime & Factoring, Trapdoors & public key, finite Fourier transform, fast form transform, polynomial ring & several variables. Complexity with respect to multiplication. Shift registers & coding. Finite Boolean algebra, Equivalence classes of switching functions. Monoids & automata.

1-4 Chapter
upto Finite Fourier Transform

Q→ Whether 2 is a QR of $\mathbb{F}_{25}$
Find $x \in \mathbb{F}_{25}$ s.t $x^2 = 2$

→ Construct a field of order 25 ∴ $\mathbb{F}_{5^2}$
i.e field of order 2 in $\mathbb{Z}_5$

$$x^2 + bx + c \quad , \quad b, c \in \mathbb{Z}_5$$

$$\therefore \quad x^2 + 3 = 0 \Rightarrow x^2 - 2 = 0$$

7-1-19

Algebraic Numbers

- Group $(G, *)$: If a group satisfies only associative property with respect to $*$ then it is called semi-group.
i.e. $a*(b*c) = (a*b)*c$

Group $\Rightarrow$ Monoid $\Rightarrow$ Semi-group
$\not\Leftarrow$ $\not\Leftarrow$
monoid → Semi-group + existance of identity – inverse

- Field : $(\mathbb{Z}_m, +, \cdot)$ is a field iff m is a Prime no.
i.e. if m is prime then product of 2 nos. less than m & greater than 1 can't be 'm' i.e. product of 2 nos. can't be 0 so inverse does not exist.

9-1-19

Book : Algebra for computer science by L. Garding & T. Tambour.

- Finite Field
- Characteristic of Ring / Field

→ A least positive integer n is called characteristic of R(F) if
$na = 0 \ \forall a \in R(F)$

Characteristic of $\mathbb{Z}_2 \cdot \{0, 1\}$ $\quad 0+0=0$, $1+1=0$ $\quad \therefore 2$

$$|\mathbb{Z}_2(x)| < 1 + x + x^2 > = \{ |ax+b + <1+x+x^2>| \}$$

$$= \{ \bar{0}, \bar{1}, \bar{x}, \overline{1+x} \} \quad \text{characteristic} = 2$$

Scanned by CamScanner

- Characteristic of any boolean ring is 2.

$a^2 = a$, $a + a \in R \Rightarrow (a+a)^2 = a+a$

$a^2 + a^2 + 2a = a + a$

Boolean ring: $R = \{a \mid a^2 = a\}$

$a + a + 2a = a + a \Rightarrow 2a = 0$

$\text{charac.}(R) = 2$

Q → Characteristic of Finite Field.

→ Characteristic of Field will always be a Prime.

Let p is characteristic then $pa = 0 \quad \forall a \in F$

Suppose p is composite then $p = m \cdot n$, $1 < m, n < p$

$\therefore (m \cdot n) a = 0$

$(m \cdot a) \cdot n = 0$

If $n \neq 0$ then $ma = 0$.

If $m \cdot a \neq 0$ then $n = 0$

Contradiction ∴ our suppose was wrong ∴ p is a Prime.

$F = Z_p[x] / \langle f(x) \rangle$

$Z_p[x]$ ↓ Set of all polynomials over Z_p

- $\forall \alpha \in F_{p^n}$ there exist a polynomial such that $f(\alpha) = 0$

- Cyclotomic Cosets

$(n, q) = 1$

$C_i = \{ (i \cdot q^j \pmod n) \in Z \}$

$\bigcup_{j=1}^{t} C_{i_j} = Z$

$j = 0, 1, 2, \ldots$

Tutorial

① Show that $\binom{p}{j} \equiv 0 \pmod p$ for any $1 \leq j \leq p-1$

② Show that $\binom{p-1}{j} \equiv (-1)^j \pmod p$ for any $1 \leq j \leq p-1$

③ Show that for any two elements α, β in a field of char. p, we have $(\alpha+\beta)^{p^k} = \alpha^{p^k} + \beta^{p^k}$, for $k \geq 0$

④ Verify that the following polynomials are irreducible over $\mathbb{F}_2$

ⓐ (i) $1 + x + x^2 + x^3 + x^4$

(ii) $1 + x + x^4$

(iii) $1 + x^3 + x^4$

ⓑ (i) $1 + x^2$

(ii) $2 + x + x^2$

(iii) $2 + 2x + x^2$

} over $\mathbb{F}_3$

5 (a) Find the order of the elements 2, 7, 10 and 12 in $\mathbb{F}_{17}$

(b) Find the order of the elements $\alpha, \alpha^3, \alpha+1$ and α^3+1 in $\mathbb{F}_{16}$, α is a root of $1+x+x^4$.

Ans-2) $\binom{p-1}{j} = \dfrac{(p-1)!}{j!\,(p-(1+j))!} = \dfrac{(p-1)!}{1\cdot 2\cdot 3 \cdots j\,(p-(j+1))(p-(j+2))\cdots(p-(p-1))}$

$$= \frac{(p-1)\cdots(p-j)}{1\cdot 2 \cdots j} \pmod p$$

$$= \frac{(-1)\cdots(-j)}{1\cdot 2\cdots j} = \frac{(-1)^j\,\cancel{(p-1)\cdots(p-j)}}{\cancel{1\cdot 2\cdots j}}$$

Ans-1) $\binom{p}{j} = \dfrac{p(p-1)\cdots(p-j+1)}{1\cdot 2\cdots j}$ Here, p is prime so $1\cdot 2 \cdots j$ does not divide numerator

$\therefore$ Proved.

Ans-3) $(\alpha+\beta)^{p^k}$

$$= \alpha^{p^k} + \beta^{p^k} + \cancel{\sum {}^{p^k}C_i\, \alpha^{p^k - i}\cdot \beta^i} \xrightarrow{} 0 \quad = \alpha^{p^k} + \beta^{p^k}$$

14-1-19

Field Extensions (of Finite Field Galois Field)

$f(x) = x^2+1 = (x-\alpha_1)(x-\alpha_2)$

$\alpha_1, \alpha_2 \in$ Field F then $f(x)$ is reducible in F.

Here, $\alpha_1 \& \alpha_2 \notin R$ $\therefore x^2+1$ is irreducible in R.

i.e. x^2+1 can not be factorized in R

$R(i) = \{a+ib\}$ $a,b \in R$

$= C$ $a,b \in F$ i.e. Extension of R.

Every field is v.s over its sub-field.

- If K is extension of F ($K \supset F$) and $\dim_F K = [K:F] =$ finite then K is called finite extension of F.

$|Z_p[x]/\langle x^2+1\rangle| = p^2 = Z_p^{[x]}$

Eg: x^4+1. Find the smallest field in which it can be factored.

$\rightarrow (x^4+1) = (x^2+i)(x^2-i) = (x-\sqrt{i})(x+\sqrt{i})(x-\sqrt{-i})(x+\sqrt{-i})$

$\therefore a+ib = \sqrt{i} \Rightarrow a^2-b^2+2ib = i$

$a^2-b^2 = 0$ & $2ib - i = 0$ $\therefore \left(\frac{1}{2}+\frac{1}{2}i\right), \left(-\frac{1}{2}+\frac{1}{2}i\right)$

$a^2 = b^2$, $b = 1/2$

Illy other

Scanned by CamScanner

15-1-19

Z(integers)

→ M is any non-empty set
Let (M, +) is additive abelian group.
Then there exist an operation.

$$M \times Z \to M$$
$$mx \in M$$

then $(M, +, \cdot)$ is called Z-module (or module over Z)

if ① $(m_1 + m_2) \cdot z_1 = m_1 z + m_2 z$ $\quad \forall z_1, z_2 \in \mathbb{Z}$

② $m_1 (z_1 + z_2) = m_1 z_1 + m_2 z_2$ $\quad m, m_1, m_2 \in M$

③ $m_1 (z_1 z_2) = (m_1 z_1) z_2$

Q→ P.T : If P is a prime & p/ab then p/a or p/b

→

16-1-19

Euclidean Algorithm

→ If $a, b (\neq 0)$ any two +ve integers, then $\exists$ q & r s.t

$$a = bq + r \quad , r < b$$

- Congruence

$a, b \in Z$, $a \equiv b \pmod m$
$\Rightarrow m \mid a-b$

congruence is equivalence relation

- Reflexive : $a \cong a$
- Symmetric : If $a \cong b$ then $b \equiv a$
- Transitive : If $a \cong b$ & $b \cong c$ then $a \cong c$

Q→ Show that if $x \equiv y \pmod m$ & $z \equiv u \pmod m$
then $x \pm z \equiv y \pm u \pmod m$

Q→ $ab \equiv 1 \pmod m$
iff $(a, m) = 1$

→ $m \mid ab-1$ if $m \mid ab$ then $m \mid 1$
$\therefore m \nmid ab \quad \therefore \gcd(a, m) = 1$

Now, $\gcd(a, m) = 1$

- Chinese Remainder Theorem

→ $x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

. . .

$N_i M_i \equiv 1 \pmod{m_i}$

then $x = \sum a_i M_i N_i \bmod M$, $M = m_1 m_2 \ldots$

$M_i = \cancel{m_i}\ \frac{M}{m_i}$

- Fermat Theorem

$\cancel{a^{\phi(n)-1} \equiv 1 \pmod n}$ if $\cancel{\gcd(a, n) = 1}$

else $\cancel{a^{\phi(n)} \equiv a \pmod n}$

$a^{p-1} \equiv 1 \pmod p$ → $\gcd(a, p) = 1$

$a^p \equiv a \pmod p$

- Euler phi

- Fermat Little Theorem

- Wilson Theorem → when p is a prime $(p-1)! \equiv -1 \pmod p$

- Euler's Function (phi function) 21-1-19

→ Let n be a positive integer.

$\phi(n)$ = no. of integers relative prime to n.

Theorem: When $q = p^k$, k is an integer then,

$\phi(q) = q(1 - \frac{1}{p})$ & for any integer m & n $\phi(mn) = \phi(m)\phi(n)$.

Finally show that $\phi(m) = m \prod (1 - \frac{1}{p})$

22-1-19

Squares & quadratic reciprocity theorem

a is called square mod p if $\exists\ b \in \mathbb{Z}$ such that $a \in \mathbb{Z}$

$b^2 \equiv a \pmod p$

a is called quadratic residue mod p.

Q→ 2 is square in F_{25}, find out $\alpha \in F_{25}$ such that $\alpha^2 = 2$

→

Legendre Symbol

$(a, p) = 1$

$$(a/p) = \begin{cases} -1 & a \text{ is not square mod } p \\ 1 & a \text{ is square mod } p. \end{cases}$$

Q→ when $p > 2$ Prove: $(2/p) = (-1)^c$ where $c = \frac{p^2 - 1}{8}$

23-1-19

① Verify that $3^{10} \equiv 16 \pmod{19}$ by explicit calculations

② Compute $\phi(6)$, $\phi(32)$ and $\phi(18)$ & verify that Euler's theorem holds for $m = 6$ & 32 for some $a > 1$

③ Show that $(3|73) = 1$ & $(17|73) = -1$

④ Show that 2 is a quadratic residue of every prime of the form $8n \pm 1$ & not a quadratic residue of the primes of the form $8n \pm 3$

⑤ Show that there are infinitely many primes of the form $4K+1$.

⑥ We know that $\sqrt{2}$ & $\sqrt{3}$ ~~are~~ is an algebraic integer. Find the equation & all its roots.

⑦ Show that $2\cos\frac{2\pi}{n}$ is an algebraic integer for every integer n

⑧ Let x is an algebraic number. Show that mx is an algebraic integer for some natural number m.

→ 1) by repeating square

2) $\phi(6) = 2$, $\phi(18) = 6$, $\phi(32) = 16$

$\phi(mn) = \phi(m)\cdot\phi(n)$ $\qquad (m,n) = 1$

$\phi(6) = \phi(2)\cdot\phi(3) = 1\cdot 2 = 2$

$\phi(18) = \phi(9)\cdot\phi(2) = \cancel{4\cdot 1} = \cancel{4}\ 6\cdot 1 = 6$

$\phi(32) = \phi(32)\cdot\phi(1) = 16$.

3) $\left(\frac{3}{73}\right) = \left(\frac{73}{3}\right)(-1)^{\frac{72}{2}\cdot\frac{2}{2}} = \left(\frac{1}{3}\right) = (+1)^{\frac{3-1}{2}} = 1$

$\left(\frac{17}{73}\right) = \left(\frac{73}{17}\right) \times (-1)^{\frac{72}{2}\cdot\frac{16}{2}}$

$= \frac{5}{17} = \frac{17}{5}(-1)^{\frac{4}{2}\cdot\frac{16}{2}}$

$= \frac{2}{5} = \frac{5}{2}(-1)^{2\cdot 1} = \left(\frac{1}{2}\right) = -1$

Primes & Factoring

28-1-19

→ Most properties of prime can be used to show that a number is composite.

• **Theorem** : A natural number N is prime iff for every prime p dividing '$N-1$', there is an integer 'a' such that

$$a^{N-1} \equiv 1\ (N) \ \& \ a^{(N-1)/p} \not\equiv 1\ (N)$$

Proof: Let $Pr(N)$ is the set of all integers relatively prime to N

$$|Pr(N)| = \phi(N).$$

Let N be a prime, then an integer 'a' such that

$a^{N-1} \equiv 1 \pmod p$, $\Rightarrow$ either $|a| = N-1$ or $|a| / N-1$

n, $a^n = \phi$ if $a^n = 1$ then $n | N-1$.

by second condition : $\left(\frac{N-1}{p}\right)$ is not factor of $N-1$.

$\phi(N) = N-1$ & n both have same power q of p in factoring.

$\phi(N)$ has q power of p in factors.

Format Number : $F(n) = 2^{2^n} + 1$

Theorem : A necessary & sufficient condition for $F(N)$ to be prime is that $3^{(F(N)-1)/2} \equiv -1 \bmod (F(n))$ i.e. $3^{(F(n)-1)} \equiv 1 \bmod (F(n))$

Proof: Assume that $F(n)$ is not a prime then there is a prime $p < F_n$ dividing $F(n)$.

Choose $F(n) - 1 = N = 2^{2n}$ consider a group $Z_p^* = \{1, 2, \dots p-1\} \bmod p$ is a cyclic grp w.r.t multiplication

$a \in G$ if n is least +ve integer s.t $a^n = e \Rightarrow |a| = n$

if $a^m = e \Rightarrow n | m$ s.t $p < F_n$

order $3 | N \Rightarrow |3| = N = F(n) - 1$ $\quad 3 \in Z_p^*$

either $|3|$ is $N = F(n) - 1$ $\quad |Z_p^*| = p-1$

or $|3| \mid N = F(n) - 1$ $\quad \Rightarrow F(n) - 1 | p - 1$

but $3^{(F(n)-1)/2} \equiv -1\ (p) \Rightarrow |3| \nmid F(n) - 1$

• Converse: Assume $F(n)$ is prime then we have to show that

$$3^{(F(n)-1)/2} \equiv -1 \pmod{F(n)}$$

→ Then $Z_{F(n)}^* = (Z / F(n))^*$ is cyclic grp with order $F(n) - 1$

We need to show that $(3|F(n)) = -1$

$$F(n) = 2^{2^n} + 1$$

$$\left(\frac{3}{F(n)}\right) = (-1)^{\left(\frac{3-1}{2}\right)\cdot\left(\frac{F(n)-1}{2}\right)} \cdot \left(\frac{F(n)}{3}\right)$$

$$= (-1)\left(\frac{F(n)}{3}\right)$$

$\therefore$ $F(n)$ is prime $\therefore$ $3^{F(n)-1} \equiv 1 \bmod F(n)$

$3^{\frac{F(n)-1}{2}} \equiv -1 \bmod F(n)$?

Theorem : When N is odd prime. Then $J(N)$ is subgroup of $P_r(N)$. Where $J(N)$ = set of congruence class mod N. and $P_r(N)$ = set of elements relative prime to N

- Jacobi symbol :-

Let Q be an odd integer then Jacobi symbol (a/Q) as follows

$Q = P_1 P_2 \dots P_K$

then (1) $(a|1) = 1$

(2) $(a/Q) = 0$ where $(a, Q) > 1$

(3) $(a/Q) = (a/P_1)\cdot(a/P_2)\dots(a/P_K)$ where $(a,Q)=1$

- Properties :-

Suppose Q & Q' are any two odd integers then

(1) $(P/Q)(P/Q') = (P/QQ')$

(2) $(P/Q)(P'/Q) = (PP'/Q)$

(3) if $(P,Q)=1$ then $(P/Q^2) = (P^2/Q) = 1$

(4) when $(PP', QQ') = 1 \Rightarrow \left(\frac{P'P^2}{Q'Q^2}\right) = \left(\frac{P'}{Q'}\right)$

Q→ Suppose Q is an odd integer then

$(-1/Q) = (-1)^{(Q-1)/2}$

and $(2/Q) = (-1)^{(Q^2-1)/Q}$

30-1-19

Let $J(N)$ be the set of congruence class mod N satisfying the congruence $(a/N) \equiv a^{N-1/2} (N)$

Jacobi Symbol.

where N is odd integer.

Theorem : When N is odd and not a prime, then $J(N)$ is proper subgroup of $P_r(N)$. Where $P_r(N)$ = Set of all integers relative prime to N.

Proof :
$$(a/N) \equiv a^{N-1/2} \bmod (N) \rightarrow (1)$$

Since $P_r(N)$ is a group if N is prime then $J(N) = P_r(N)$

- If N is prime
  p

then $(a/p) \equiv a^{p-1/2} (p)$

1 or -1

$\Rightarrow \quad a^{p-1} \equiv 1 (p) \quad \therefore |a| = p-1$

$\therefore P_r(p) = p-1 = |a| = |J(N)|$

- If N is not prime

$J(N) \subset P_r(N)$

$N = p^k$, then $|P_r(N)| = |\phi(N)| = |\phi(p^k)| = p^{k-1}(p-1)$

$N-1 = p^k - 1$

which is a contradiction

- case 2) $N = rs$, $(r,s) = 1$

If there is an 'a' in $P_r(N)$ with $(a/N) = -1$

using CRT we can choose b in $P_r(N)$ with $b \equiv a \bmod r$

and $b \equiv 1 \bmod s$

then $b \equiv a \bmod N$.

then $(b/N) \equiv b^{N-1/2} (N) \equiv (a/N) \equiv -1 \pmod r$

then $b^{N-1/2} \equiv 1 \bmod s$

Theorem : Quadratic Reciprocity

suppose that P & Q are odd positive integers and $(P,Q) = 1$ then $(P/Q) \cdot (Q/P) = (-1)^{\frac{(P-1)(Q-1)}{4}}$

Tutorial

① Calculate Jacobi $\left(\frac{1111}{8093}\right)$.

② Determine whether or not the congruence $x^2+6x-50 \equiv 0 \pmod{7}$ has a solution

③ For an odd prime p and $a, b, c \in \mathbb{Z}$ with $(a,p)=1$ we consider the congruence $y^2 \equiv ax^2+bx+c \pmod{p}$ Prove that the number of sol^n with $1 \le x, y \le p$ is equal to :-

(i) $p - \left(\frac{a}{p}\right)$ if $p \nmid D$

(ii) $p + (p-1)\left(\frac{a}{p}\right)$ if $p \mid D$, where $D = b^2-4ac$

④ Suppose that Q is an odd positive integer. then prove that
$\left(-\frac{1}{Q}\right) = (-1)^{(Q-1)/2}$ and $\left(\frac{2}{Q}\right) = (-1)^{(Q^2-1)/8}$

⑤ Prove Quadratic Reciprocity Theorem

→ ① $\left(\frac{1111}{8093}\right) = \left(\frac{101}{8093}\right)\left(\frac{11}{8093}\right) = \left(\frac{13}{101}\right)\left(\frac{8}{11}\right)$

$= \left(\frac{10}{13}\right)\left(\frac{2}{11}\right)\left(\frac{2}{11}\right)\left(\frac{2}{11}\right) \longrightarrow ①$

$= \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = \left(\frac{3}{5}\right) = -1$

5-2-19

Factoring of Large numbers

→ The method of factoring large numbers are
trial method

1) Knuth method (1982)

→ The first step look at integer x & y in between 0 & N.
such that $x^2-y^2 \equiv 0 (N)$ → $x-y \equiv 0(N)$
→ $x+y \equiv 0(N)$ → discard it

then N has the proper factor of $x-y$ in second stage,
look for squares mod N

$$x^2 \equiv (-1)^{e(0)} p_1^{e(1)} p_2^{e(2)} \cdots p_n^{e(n)} \mod N.$$

$p_1, p_2, \cdots p_n$ are primes

If a set $\{x_1, x_2, \cdots x_r\}$ of such numbers x have been found with the property that the sum of the vectors of their exponents has even components $2f(0), \ldots 2f(n)$ then

$$x \equiv x_1 x_2 \ldots x_r \qquad y \equiv (-1)^{f(0)} p_1^{f(1)} \cdots p_r^{f(r)} \mod N$$

have the property

$$x^2-y^2 \equiv 0 (N)$$

Trapdoors & Public Key

<u>Theorem</u> : If N is a product of distinct primes p & $\lambda(N)$ is the least common multiple of all $\phi(p)$, then

$$a^{\lambda(N)+1} \equiv a\,(N)$$

Proof : $N = p_1 p_2 \dots p_n$ $\qquad a \equiv 0\,(p)$ or $(a,b)=1$

then $a^{p-1} \equiv 1\,(p)$ by F.L.T

3. Abstract Algebra & Modules

6-2-19

- <u>Modules</u> : Let $(M,+)$ is an abelian group and R be a ring (with unity). Then M is called left (Right) module over R if $\exists$ a binary operation $*$ $R \times M \to M$ such that following axiom is satisfied.

$r \cdot m \in M \;\forall\; r \in R, m \in M$

1) $(r_1+r_2)\cdot m = r_1 m + r_2 m$ $\qquad r, r_1, r_2 \in R$

2) $r(m_1+m_2) = r m_1 + r m_2$ $\qquad m, m_1, m_2 \in M$

3) $(r_1 r_2)(m) = r_1(r_2 m)$ $\qquad 1 \in R$

4) If R is with unity then $1\cdot m = m$

if 4th holds then M is called unital Module.

Exp : 1) All V.S over F are module over F

2) A Ring R over itself is module R_R or ${}_R R$ or $R(R)$

$M_R \to$ right R-module

${}_R M \to$ left R-module

Exp: 3) if S is subring of R then $R(S) \mid R_S\,({}_S R)$ also module over S.

4) $[Z]_{m\times n}$ is module over Z.

- <u>Submodules</u> : A non-empty subset N of a module ${}_R M$ is called submodule of ${}_R M$ if $a, b \in N \Rightarrow a-b \in N$

- <u>Cyclic module</u> : Z = set of all integers

$2Z = \langle 2 \rangle$ $\qquad$ i.e. $mZ = \langle m \rangle$

Let M be a left R-module. Then M is called cyclic if $M = Rx \;\forall x \in M$

Theorem: Every submodule N of a cyclic module M is cyclic. 11-2-1

$\longrightarrow$ $M = Rx = \{rx \mid r \in R, x \in M\}$

Exp: $M = (Z_6, +, \cdot) = \{0, 1, 2, 3, 4, 5\}$ Mod 6 $\qquad \cdot R \times M \to M$

$R = Z$

$Z_6(Z)$ is a Z-module $\to$ cyclic or not

cyclic

Theorem proof: Let ${}_R M$ be a cyclic module. Then

$M = Rx = \{rx \mid r \in R, x \in M\}$

if N is submodule of M. $\{N \leq M\}$

then $r_1 x, r_2 x \in N$

by property of submodule

$(r_1 - r_2)x \in N \Rightarrow N = Rx \Rightarrow N$ is cyclic.

Exp: $Z_6(Z)$ is cyclic module.

$\hookrightarrow$ its submodule are $A = \{0, 3\}$ mod 6

$B = \{0, 2, 4\}$ mod 6.

Theorem: Let A & B be cyclic submodules of a module M and suppose that orders m & n of A & B are co-prime. Then $A+B$ be a cyclic submodule of order mn

Problem: How many element of order 5 there in a cyclic module of order 20?

→ $M = R_n = \langle n \rangle$

$|M| = 20$ cyclic Module

↓ cyclic group

By Lagr. theorem 20

↓

1, 2, 4, 5, 10, 20

for a cyclic: For each divisor there exist a unique subgroup

- Quotient Module

→ M is any set and $N \subseteq M$ then,

Right coset of N is M

$N_m = \{nm \mid m \in M\}$

$N = \{n_1, n_2, \dots\}$, $N_m = \{n_1 m, n_2 m, \dots\}$

for a module M, let N is any submodule of M.

then, M/N = set of all cosets of ~~N m~~ N in M

$\{m_1, m_2 \dots\}$

$\{Nm_1, Nm_2, \dots\}$

M/N is R-module

$M/N = \{N + m \mid m \in M\} \Rightarrow (M/N, +)$ is abelian sub.

Normal sub. if left & right coset are same.

Q → Show that M/N is R-module

- $R \times N \to N$ $R \times \frac{M}{N} \to \frac{M}{N}$

$r(N+m) = rN + rm = N + m_1 \in M/N$

Exp: $Z/mZ \cong Z_m$

$Z/2Z \cong Z_2$

↓ quotient Module

- Every Ring is module over itself

Direct sum of Module

→ Let M_1 & M_2 are any two modules over ring R. Then

$M = M_1 \oplus M_2$ = direct sum of M_1 & M_2

$M = M_1 + M_2$ & $M_1 \cap M_2 = \{0\}$

$Z_6(Z) = \{0,1,2,3,4,5\}$ mod 6

↓

$A = \{0, 2, 4\}$ mod 6 $B = \{0, 3\}$ mod 6.

then, $Z_6 = A \oplus B$ where $Z_6 = A + B$ & $A \cap B = \{0\}$

Module Morphism

→ Let M & N are any two modules over Ring R. then f is called homomorphism from M to N, if

$$f : M \rightarrow N$$
$$f(m_1 + m_2) = f(m_1) + f(m_2)$$
$$f(rm) = r f(m) \quad \forall\, m, m_1, m_2 \in N,\ r \in R$$

⇒ if f is one-one & onto then f is called isomorphism

Exp: $\mathbb{C}(R) \rightarrow \mathbb{C}(\mathbb{R})$

$$z \rightarrow \bar{z}$$
$$f(z_1 + z_2) = (\overline{z_1 + z_2}) = \bar{z}_1 + \bar{z}_2$$
$$f(\alpha z) = \overline{\alpha z} = \alpha \bar{z} = \alpha f(z)$$

- When M & N are R-module

$$f : M \rightarrow N$$
$$\text{Ker} f = \{ x \in M \mid f(x) = 0_N \}$$

Ker f is submodule of M.

$$x_1, x_2 \in \text{Ker} f \Rightarrow f(x_1) = 0,\ f(x_2) = 0$$
$$f(x_1 - x_2) = f(x_1) - f(x_2) = 0$$
$$\Rightarrow x_1 - x_2 \in \text{Ker} f$$

$$\text{image } f = \{ f(x) \in N \mid x \in M \}$$

img f is submodule of N.

Fundamental Theorem of module homomorphism :-

13-2-1

→ Homomorphic image of a module is isomorphic to some of its Quotient module $f : M \rightarrow M'$

$$f(M) \cong M / \text{Ker} f$$

Proof: It is given that for any two R-module M & N $f : M \rightarrow N$ is module homomorphism.

Now, consider a map $\phi : M/\text{Ker} f \rightarrow f(M)$

$$\phi(\text{Ker} f + m) = f(m)$$

Let $m_1 + \text{Ker} f = m_2 + \text{Ker} f$

$$\Rightarrow m_1 - m_2 \in \text{Ker} f$$
$$\therefore f(m_1 - m_2) = 0 \Rightarrow f(m_1) = f(m_2)$$
$$\Rightarrow \phi \text{ is well defined.}$$

Next show that: ϕ is homomorphism :-

① $\phi(a + b) = \phi(a) + \phi(b)$

$\phi(ra) = r\phi(a)$

Scanned by CamScanner

Let $m_1 + \ker f,\ m_2 + \ker f \in M/\ker f$

$$\phi(m_1 + \ker f + m_2 + \ker f) = \phi(m_1 + m_2 + \ker f)$$
$$= f(m_1 + m_2) = f(m_1) + f(m_2) = \phi(m_1 + \ker f) + \phi(m_2 + \ker f)$$
$$\phi(r(m + \ker f)) = \phi(rm + \ker f)$$

- $M \to N$

$HOM(M, N)$ = Set of all module homomorphism from M to N.

Q→ $HOM_R(M, N)$ is R-Module ?

: If M & N are finite cyclic module of order m & n such that m & n are relatively prime then their no. of homomorphism is 0.

In homomorphism image of 0 will always be 0.

Q→ No of homomorphism in $Z_8 \to Z_{18}$, $Z_8 \to Z_{12}$

Structures of Finite Module

→ Let a & b be elements of order m & n, in a module M.

The order of $a + b = mn$, where $(m, n) = 1$

If n does not divide m then module $Za + Zb$ has elements of order $> m$