Assignment-2, MTH204A, IIT Kanpur

04 January 2018

Module -02

1. Let G be a finite group such that $3 \nmid |G|$ and $a^3b^3 = (ab)^3$ for all $a, b \in G$. Prove that G is abelain.

2. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $(a, n) = 1$. Prove that $n \mid \phi(a^n - 1)$, where ϕ is the Euler ϕ-function.

3. Show that the groups $(\mathbb{Z}^{\oplus r}, +) \cong (\mathbb{Z}^{\oplus s}, +)$ if and only if $r = s$.

4. Can we have $(\mathbb{R}^{\oplus r}, +) \cong (\mathbb{R}^{\oplus s}, +)$ if r and s are different ?

5. Let G be a finite group and f be an automorphism of G with the property that $f(x) = x$ for $x \in G$ if and only if $x = 1$. Prove that every $g \in G$ can be represented as $g = x^{-1}f(x)$ for some $x \in G$.

6. Let G be a finite group and f be an automorphism of G with the property that $f(x) = x$ for $x \in G$ if and only if $x = 1$. Assume that f^2 = identity on G. Then deduce that G is abelain.

7. Show that $Z(G_1 \times G_2 \cdots \times G_n) \cong Z(G_1) \times \cdots \times \mathbb{Z}(G_n)$.

8. Show that $(\mathbb{Z}/7\mathbb{Z})^{\times}$ is a cyclic group.

9. Let G be a group of odd order and N is a normal subgroup of G of order p where p is a prime of the form $p = 2^{2^n} + 1$. Then show that $N \subset Z(G)$.

10. Determine all groups of order pq where p and q are primes. More precisely show that

    (a) If $p = q$, then G is abelian and determine all such G.

    (b) If $p > q$ and $q \nmid p - 1$ then also deduce that G is abelian and determine all such G.

    (c) If $p > q$ and $q \mid p - 1$ then prove that there is a non-abelian group of order pq.

(d) Any two non-abelian group of order pq are isomorphic.

11. Let G be a group of oder m with $1 < m < 60$ and also assume that m is not a prime number. Then show that G is not simple.

12. Let G be a group and H, K subgroups of G of finite index in G. Prove that $H \cap K$ has finite index in G.

13. Let G be a group and set $C = \{xyx^{-1}y^{-1} \mid x, y \in G\}$. Now define $G' =< C >$; the subgroup generated by C. The show that G' is a normal subgroup of G.

14. Let G be a finite group and M, N be normal subgroups of G such that $G/M \cong G/N$. Then is $M \cong N$?

15. Write down examples of a cyclic and a non-cyclic subgroup of $(\mathbb{Q}, +)$.

16. Let $m \in \mathbb{N}$. Determine End$(\mathbb{Z}/m\mathbb{Z})$:= Hom$(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ and Aut$(\mathbb{Z}/m\mathbb{Z})$:= Automorphism$(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$.

17. Let G be a finite abelian group in which the number of solutions in G of the equation $x^n = 1$ is at most n for every $n \in \mathbb{N}$. Prove that G must be a cyclic group.

18. Write down all the conjugate classes in D_n and study the class equation.

19. Prove or disprove: A group G can never be written as the set theoretic union of two proper subgroups H_1 and H_2.

20. Prove Wilson Theorem: Let p be a prime then

$$(p-1)! \equiv -1 \pmod{p}.$$

21. If P is a p-Sylow subgroup of G, then $N_G(N_G(P)) = N_G(P)$.

22. Show that $\mathbb{Q}/\mathbb{Z}$ has no proper subgroup of finite index.

23. If H and K are finite subgroups of a group G then

$$|HK| = |H||K|/|H \cap K|.$$

24. G is a group of order p^n and H is a proper subgroup of G. Then normalizer of H strictly contains H.

25. If G is a group of order p^2q wherep, q are prime numbers, then G has a non-trivial proper normal subgroup.

Module-03

1. Prove that a group of order 72 is not simple.

2. Classify all groups of order 30.

3. Calculate the order of $\text{Aut}(\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z})$.

4. Determine the no of subgroups of order p in $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

5. Show that if H is a finite index subgroup of a group G then show that

$$\bigcup_{g \in G} gHg^{-1} \neq G$$

6. If G acts transitively on a finite set A with $|A| > 1$ then G necessarily contain an element g_0 which has no fixed points i.e. $g_0 a \neq a$ for any $a \in A$.

7. Show that A_n is generated by 3-cycles.

Module-04

1. Definition: Let $H_1, H_2, \cdots, H_k$ are subgroups of a group G. We say that G is the (internal) direct product of $H_1, H_2, \cdots, H_k$ if
   (a) Each H_i is normal in G.
   (b) $G = H_1 \cdots H_k$.
   (c) $H_i \cap \hat{H}_i = 1$ for all i, where $\hat{H}_i := H_1 \cdots H_{i-1} H_{i+1} \cdots H_k$.

   Let G be (internal) direct product of $H_1, H_2, \cdots H_k$. Then we have the following
   (a) $H_i \cap H_j = 1$ for $i \neq j$.
   (b) If $g \in G$, then we can write $g = h_1 h_2 \cdots h_k$ with $h_i \in H_i$ are all unique.
   (c) If $h_i \in H_i$ and $h_j \in H_j$ then $h_i h_j = h_j h_i$ for all distinct i, j.
   (d) $G \cong H_1 \times \cdots \times H_k$ under the map $h_1 h_2 \cdots h_k \longrightarrow (h_1, h_2, \cdots, h_k)$.

2. Let G be an abelian group of order n with $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ where p_i's are distinct primes. Then use the above exercise to show that $G = G(p_1) \oplus \cdots \oplus G(p_r)$ where for each $i \leq i \leq r$, we define $G(p_i) = \{x \in G \mid x^{p_i^n} = 1 \text{ for some } n \in N\}$.

3. Let G be a finite abelian group and let y be an element of G such that the order of y is maximal. Then show that for any x in G with order of $x = n$ satisfies $n \mid m$. (you can give a proof without using the structure theorem for finitely generated abelian group.)

4. (a) Let A be an abelian group and let f be a surjective group homomorphism from A to a free abelian group A' with $\text{Ker}(f) = B$. Then show that there is a subgroup C of A with $C \cong A'$ such that $A \cong B \oplus C$.
   (b) Use this to show subgroup of finitely generated free abelian group is free.

(c) Without invoking structure theorem, prove that a finitely generated torsion abelian group is finite.

5. Classify all groups of (i) order 8, (ii) order 12.

6. (a) Compute the centre of S_n.
   (b) Show that A_4 is not simple.
   (c) Prove that every element of S_n can be uniquely written as product of disjoint cycles.
   (d) Prove that any two disjoint cycles in S_n commute.
   (e) Prove that A_n is generated by 3-cycles (for $n \geq 3$).
   (f) Let $n \geq 5$ and $\sigma \neq 1 \in A_n$. Prove that σ' has a conjugate $\sigma' \neq \sigma$ in A_n such that $\sigma(i) = \sigma'(i)$ for some i.
   (g) For $n \geq 5$, prove that any two 3-cycles in A_n are conjugate within A_n.

7. (a) Prove that any simple non-abelian group of order 60 is isomorphic to A_5.
   (b) Prove that any simple non-abelian group of order < 100 is isomorphic to A_5.

8. Compute $\mathrm{Hom}(\mathbb{Q}, \mathbb{Z}/n\mathbb{Z})$ for any n.

Module-05

1. Prove Burnside's Lemma: If G is a finite group acting on a finite set X with r orbits, then
$$r = \frac{1}{\#G} \sum_{g \in G} \mathrm{Fix}_g(X)$$
where $\mathrm{Fix}_g(X) = \{x \in X \mid gx = x\}$.

2. Follow these steps to derive the structure theorem of finitely generated abelian groups.

   (a) Prove that the rank of a finitely generated free abelian group is well defined and if F is a free abelian group of rank n then any subgroup is a free abelian group of rank $\leq n$.
   (b)
   - Recall $GL_n(\mathbb{Z})$ is the set of $n \times n$ integer matrices which are invertible over $\mathbb{Z}$ i.e. those square integer matrices whose determinant is a unit in $\mathbb{Z}$.
   - Define a $m \times n$ matrix $A = A_{m,n} \in M_{m,n}(\mathbb{Z})$ to be diagonal if $a_{i,j} = 0$ whenever $i \neq j$.
   - An elementary matrix in $GL_n(\mathbb{Z})$ is given by one of the following 3 types of matrices.
     - Interchange two rows (or two columns).
     - multiply a row (or a column) by a unit in $\mathbb{Z}$.

– Add an integer multiple of a row (or a column) to another.

Now let $A_{m,n} \in M_{m,n}(\mathbb{Z})$. Then show that there exist $Q \in GL_m(\mathbb{Z})$ and $P \in GL_n(\mathbb{Z})$ such that $A' := QAP^{-1}$ is a diagonal matrix with diagonal entries satisfies (i) each $d_i := a_{ii}$ is non negative and (ii) $d_i \mid d_{I+1}$ for all $i \geq 1$. (hint: If $A \neq 0$ bring the element with smallest absolute value to a_{11} position and if necessary make it positive. Now repeatedly use division algorithm, row and column operations.)

(c) Recall a homomorphism T between two finitely generated free abelian group $C_1 \cong \mathbb{Z}^n$ and $C_2 \cong \mathbb{Z}^m$ is given by a matrix $T(A) = A_{m,n} \in M_{m,n}(\mathbb{Z})$. Then show that there exists basis $\mathcal{B}_1$ of C_1 and $\mathcal{B}_2$ of C_2 with respect to which the matrix of T has the form of a diagonal matrix with non negative diagonal entries such that $d_i := a_{ii} \mid d_{i+1} = a_{i+1,i+1}$ for all $i \geq 1$.

(d) Let $0 \neq N$ be a subgroup of a finitely generated free abelian group $F \cong \mathbb{Z}^n$ with rank of $N = n \leq m$. Then show that $\exists$ a basis $w_i, \cdots, w_m$ of F and $v_1, \cdots, v_n$ of N such that for each $1 \leq j \leq n-1$, $v_j = d_j w_j$ with $d_j \in \mathbb{N}$ and $d_i \mid d_{i+1}$ for $1 \leq j \leq n-1$.

(e) Deduce that if $0 \neq G$ is a finitely generated abelian group then

$$G \cong \mathbb{Z}^n \bigoplus_{1 \leq i \leq m} \frac{\mathbb{Z}}{d_i \mathbb{Z}},$$

where $n \in \mathbb{N} \cup \{0\}$ and $d_i \mid d_{i+1}$ for $1 \leq i < n$.

3. *Let A be an additive subgroup of $\mathbb{R}^2 \cong \mathbb{C}$. Assume that in every bounded subset of $\mathbb{R}^2$ (in the usual topology) there are only finite number of points of A. Show that A is a free abelian group with at most 2 generators. Such a subgroup is called a lattice in $\mathbb{R}^2$.
(* = This problem is <u>not relevant to</u> quiz or examination).

4. Let R be a ring and $a, b \in R$ are arbitrary elements. Then prove that

   (a) $0.a = a.0 = 0$.

   (b) $-a = (-1)a$.

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

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

5. (a) If $x^2 = x$ for all x in a ring R then show that R is a commutative ring.

   (b) If $x^3 = x$ for all x in a ring R then show that R is a commutative ring.

6. Prove that a finite integral domain is a field.

7. Prove that an ideal I in a commutative ring R is a maximal ideal if and only if R/I is a field.

8. Let I, J be ideals in a commutative ring R.

   (a) Prove that $\text{Ann}(I) = \{x \in R | \ ux = 0 \text{ for all } u \in I\}$ is an ideal in R.

   (b) Prove that $\sqrt{I} = \{x \in R | \ x^n \in I \text{ for some } n \in \mathbb{N}\}$ is an ideal in R.

   (c) Prove that $(I : J) = \{x \in R | \ xy \in I \text{ for all } y \in J\}$ is an ideal in R.

9. Let K be a field. Then show that any homomorphism from K to another ring R is either zero or injective.

10. If every proper ideal is a prime ideal in a ring R then show that the ring is a field.

11. Show that there is a ring isomorphism between $\frac{\mathbb{R}[X]}{(X^2+1)}$ and $\mathbb{C}$.

12. (a) If K is a field then show that $K[X]$ is a PID.

    (b) Show that $\mathbb{Z}[X]$ is not a PID.

13. Let K be any field and let $f(X) \in K[X]$ be an irreducible polynomial of degree n. Then show that $\frac{K(X)}{(f(X))}$ is a field containing K and $\frac{K(X)}{(f(X))}$ is also a vector space of dimension n over K.

14. Let R be a commutative ring. Determine $(R[X])^*$, the group of units in R.

15. Prove that $\mathbb{Z}[i]$ is an Euclidean domain.

16. Let R be a UFD. Prove that $x \in R$ is prime if and only if x is irreducible.

Module-06

1. Define characteristic of a field to be the smallest positive integer n such that $n = n.1 = 0$ in K. If no such integer n exists then we say characteristic of the field is 0.

   (a) Prove that the characteristic of a field is always a prime number or zero.

   (b) Prove that for any field F contains as a subring either (a copy of) $\mathbb{Z}$ or (a copy of) $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

2. (a) Show that every irreducible element is a prime in a UFD.

   (b) Show that for every irreducible element x in a PID R, (x) is a maximal ideal. Hence every irreducible element is a prime element in a PID.

   (c) Show that every non-zero prime ideal is a maximal ideal in a PID.

3. Let $R = \mathbb{Z}[\sqrt{-5}]$. Show that $R \cong \frac{\mathbb{Z}[X]}{(X^2+5)}$ is an integral domain. Observe the identity in R,

$$6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

   Use this to show R is not a UFD and hence not a PID or ED.

4. Prove that a finite subgroup of the multiplicative group F^* of any field F is cyclic.

5. Prove that any maximal ideal of $\mathbb{C}[X]$ is of the form $(X - a)$ where $a \in \mathbb{C}$. Thus the set of maximal ideals of $\mathbb{C}[X]$ are in bijection with $\mathbb{C}$. Is the corresponding statement true for $\mathbb{R}[X]$?

6. Let K be the field $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ where d is a square-free integer. Set O_K to be the subring of K given by $O_K = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ where

$$\omega = \begin{cases} \sqrt{d} & \text{if } d = 2, 3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d = 1 \pmod 4 \end{cases}$$

Define a norm $N : K \longrightarrow \mathbb{Q}$ given by $N(a+b\sqrt{d}) = a^2 - bd^2 = (a+b\sqrt{d})(a-b\sqrt{d})$. Then show that for $a + b\omega \in O_K$,

   (a)
$$N(a + b\omega) = \begin{cases} a^2 - db^2 & \text{if } d = 2, 3 \pmod 4 \\ a^2 - ab + \frac{1-\sqrt{d}}{4} b^2 & \text{if } d = 1 \pmod 4 \end{cases}$$

   (b) $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in K$ and in particular for $\alpha, \beta \in O_K$.

   (c) An element $\alpha \in O_k$ is in $O_K^\times$ if and only if $N(\alpha) = \pm 1$.

7. (a) Determine all the prime ideals in $\mathbb{Z}[\iota]$. Deduce that $\mathbb{Z}[\iota]$ is a PID.

   (b) Determine the group $(\mathbb{Z}[\iota])^*$.

   (c) Prove that $(\mathbb{Z}[\sqrt{2}])^*$ is infinite. Use this to prove $X^2 - 2Y^2 = 1$ has infinitely many integer solutions.

   (d) Prove that the $\mathbb{Z}[\sqrt{-2}]$ is an Euclidean Domain.

8. Prove the prime avoidance lemma: Let R be a commutative ring and I be an ideal such that $I \subset \bigcup_{1 \le i \le n} P_i$, where each P_i is a prime ideal in R. Then show that $I \subset P_i$ for some i.

9. Let G be any finite group of order $n > 1$. For any field K, show that the group ring $K[G]$ is never an integral domain i.e. it contains (left and right) divisors of zero.