Nurture Programme 2008 - ISI Bangalore
Some problems in algebra and number theory

This set of problems encompasses all topics in algebra and number theory to be studied in the first year of the programme. Don't despair if you are unable to solve many of them; they can be discussed during the contact programme.

Q 1.
Let G be any group.
(i) If $g \in G$ has order n and d is any integer, find the order of g^d.
(ii) If $a^3 = e$ and $aba^{-1} = b^2 \neq e$, find $O(b)$.
(iii) If G is abelian, then prove that for each integer m, the map $\theta : G \to G; g \mapsto g^m$ is a homomorphism. Give examples to show this may or may not hold for nonabelian groups.

Q 2.
If G is a group which has only finitely many subgroups in all, show that G must be finite.

Q 3.
Let G, H be cyclic groups (not necessarily finite). Find all homomorphisms between them.

Q 4.
(i) Suppose G is any group (not necessarily finite) and H is a subgroup such that there are exactly n distinct left cosets of H in G. Prove that n is also the number of distinct right cosets of H in G.
(ii) Let H, K be subgroups of finite indices in a group G. Prove that $H \cap K$ has index at most the product of the indices of H and K. When does equality hold?

Q 5.
(i) Let $\sigma \in S_n$ have order a prime p. Then,show that

$$\#\{i \leq n : \sigma(i) = i\} \equiv n \quad mod\ p$$

(ii) Show that a transposition (a, b) and the n-cycle $(1, 2, \cdots, n)$ generate the whole of S_n if and only if $(a - b, n) = 1$.

Q 6.
(i) Let p be a prime and let $GL_n(\mathbf{Z}_p)$ denote the set of $n \times n$ matrices with entries in the integers modulo p and with determinant not equal to 0 modulo

p. Find the order of $GL_n(\mathbf{Z}_p)$.
(ii) Exhibit a one-one homomorphism from S_n into $GL_n(\mathbf{Z}_p)$. Hence, deduce that $n!$ divides $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$.

Q 7.
Let G be any group and let $g \in G$ have order mn where $(m,n)=1$. Prove that there is some power g^k so that the order of g^k is m and the order of g^{k-1} is n.

Q 8.
(i) For a prime p, compute the product of all the elements of the group $\mathbf{Z}_p^*$ under multiplication mod p. Deduce Wilson's congruence.
(ii) Let G be any group of order n and let p any prime number. Consider the subset S of $G \times \cdots \times G$ (p times) defined by $S = \{(g_1,\cdots,g_p) : g_1g_2\cdots g_p = e\}$. Prove that $|S| \equiv \#\{g : g^p = e\}$ mod p.
(iii) Use this to prove Cauchy's theorem and Fermat's little theorem for any prime p.

Q 9.
(i) Show that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is not conjugate to a diagonal matrix.
(ii) Show that the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ are conjugate by a matrix in $GL_2(\mathbf{C})$ but that they are not conjugate by a matrix in $GL_2(\mathbf{R})$.

Q 10.
If $p < q$ are primes, show that a group of order pq must be cyclic unless $p|(q-1)$. Construct a nonabelian group of order pq when $p|(q-1)$.

Q 11.
Call an abelian group A *divisible* if for each $a \in A$ and natural number n, there exists $b \in A$ such that $nb = a$ (here we are writing A additively). Prove that $\mathbf{Q}$ has no proper nontrivial divisible subgroups. Deduce that the groups $\mathbf{Q}$ and $\mathbf{Q} \oplus \mathbf{Q}$ are not isomorphic.

Q 12.
For $1 \leq r \leq n$, let $x(r)_1, x(r)_2, \cdots x(r)_n$ be complex numbers satisfying :

$$\sum_{r=1}^{n} x(r)_i \overline{x(r)_j} = 0 \ , \ if\ i \neq j \ ,$$

$$\sum_{r=1}^{n} |x(r)_i|^2 = 1 \ , \ forall\ i.$$

Prove that

$$\sum_i |x(r)_i|^2 = 1 \ \forall \ r,$$

$$\sum_i x(r)_i \overline{x(s)_i} = 0 \ \forall \ r \neq s.$$

Q 13.
Let V be a finite dimensional rational or real or complex) vector space.
(i) Show that $V \neq \bigcup\limits_{i=1}^{n} V_i$ for proper subspaces $V_1, \cdots, V_n$ of V.
(ii) If W_1, W_2 are subspaces of the same dimension, prove that they have a common complement; that is, there exists a subspace W of V such that $V = W \oplus W_1 = W \oplus W_2$.

Q 14.
Let $a_1, \ldots, a_n$ be distinct complex numbers. Show that every complex polynomial $f = c_0 + c_1 X + \ldots + c_{n-1} X^{n-1}$ of degree $< n$ can be written as $\sum\limits_{i=1}^{n} \lambda_i (X + a_i)^{n-1}$ for some λ_i, by considering the system of linear equations in the variables λ_i obtained by equating coefficients of corresponding powers of X.

Q 15.
Prove that the number of conjugacy classes in S_n is the number $p(n)$ of partitions of n.
For example, $\{I\}, \{(1,2),(1,3),(2,3)\}, \{(1,2,3),(1,3,2)\}$ are the conjugacy classes of S_3 and there are three partitions of $3: \ 3, 2+1, 1+1+1$.

Q 16.
Let $\theta : G \rightarrow G$ be an automorphism of a finite group G such $\theta(g) = g^{-1}$ for more than 3/4-ths of the elements of G. Prove that $\theta(x) = x^{-1}$ for all $x \in G$. If θ takes g to g^{-1} for exactly 3/4-ths of the elements of G, prove that G has an abelian subgroup of index 2.

Q 17.
Suppose G is a nonabelian finite group. Then, show that the number of elements $(x, y) \in G \times G$ such that $xy = yx$ is at the most $\frac{5}{8}|G|^2$.

Q 18.
If $G = \bigcup_{i=1}^{n} H_i g_i$, then show that all the H_i's of infinite index can be dropped without affecting this decomposition.

Q 19.
Let G be a finite simple group and $p||G|$. If G has exactly $n > 1$ p-Sylow

subgroups, show that G is isomorphic to a subgroup of A_n.

Q 20.
For any prime p and any n, prove that each p-group $P \leq GL(n, \mathbf{Z}_p)$ is conjugate to a subgroup of the group $U = U(n, \mathbf{Z}_p)$ consisting of upper triangular matrices with 1's on the diagonal. Hence, compute the number of p-Sylow subgroups.

Q 21.
Decide whether the following equations have solutions in integers x, y, N :

$$x^2 + 5x - 12 = 31N$$

$$y^2 + 6y + 7 = 317N$$

Q 22.
Let p be a prime > 2 and let $a_1, \cdots, a_{\phi(p-1)}$ denote the primitive roots mod p. For any natural number k, determine the sum $\sum_{i=1}^{\phi(p-1)} a_i^m$.

Q 23.
Prove that $1 + \frac{1}{2} + \cdots + \frac{1}{p-1} = \frac{a}{b}$ with $p^2|a$ if p is a prime > 3.

Q 24.
Prove for any prime $p > 2$ that

$$\frac{2 - 2^p}{p} \equiv -\sum_{j=1}^{p-1} \frac{2^j}{j} \quad mod \quad p.$$

More generally, for any natural number n and an odd prime p, prove

$$\frac{n^p - n}{p} \equiv -\sum_{r=1}^{p-1} \frac{1^r + 2^r + \cdots + n^r}{r} \quad mod \quad p.$$

Q 25.
Let $n \equiv 1$ mod 4 be a nonsquare positive integer such that $n = a^2 + 4b^2$ for some integers a, b. Assume that $x^2 - ny^2 = -1$ has an integer solution $(x, y) = (t_1, t_2)$ (this is true for prime $n \equiv 1$ mod 4). Show that $n = rs$ for some r, s where $rx^2 - sy^2 = a$ has an integer solution.