INDIAN STATISTICAL INSTITUTE

Semestral Exam

BStat 2nd year

Elements of Algebraic Structures

Maximum marks: 50 Time: 210 minutes

November 21, 2025

1. (a) Let G be a finite group, acting on a nonempty finite set X. For $x \in X$, define the *orbit* $[x]$ and the *stabilizer* G_x of x. [2]
   (b) With notations as above, prove that the number of elements in $[x]$ is the same as the index of G_x in G. [4]
   (c) Now take $G = S_n$ and $X = \{1, 2, \cdots, n\}$. The group G acts on X by $(\sigma, x) \mapsto \sigma(x)$ where $\sigma \in G$ and $x \in X$ (no need to check that this is a group action). For $x \in X$, find the number of elements in $[x]$. Compute the index of G_x in G. [2+2]

2. Let G be a group of order 48. Assume that G has two distinct Sylow 2-subgroups H and K. Prove that:
   (a) The order of $H \cap K$ is 8. [3]
   (b) Prove that $H \cap K$ is normal in G. (Hint: show that $N(H \cap K) = G$, where $N(H \cap K)$ is the normalizer of $H \cap K$ in G.) [4]

3. Let p be a prime. Show that the polynomial $X^{p-1} + X^{p-2} + \cdots + X + 1$ is irreducible in $\mathbb{Z}[X]$. State the result that you have used. [4+2]

4. Let $f(X), g(X) \in \mathbb{Q}[X]$ be such that the product $f(X)g(X) \in \mathbb{Z}[X]$. Prove that the product of any coefficient of f with any coefficient of g is an integer. State the result that you have used. [5+2]

5. Let K be a field consisting of constructible numbers. What is the form of $[K : \mathbb{Q}]$? (Just state the result). Prove that it is impossible to construct, using only a straightedge and compass, the angle 20°. If your solution involves any irreducible polynomial, prove its irreducibility. [1+5]

6. Let p be a prime and let $\mathbb{F}_p$ be the field consisting of p elements. Let $n \geq 1$ and K be a splitting field of the polynomial $X^{p^n} - X$ over $\mathbb{F}_p$.
   (a) Prove that the roots of $X^{p^n} - X$ in K are all distinct. [2]
   (b) Let $\mathbb{F}$ be the subset of K consisting of those p^n distinct roots of $X^{p^n} - X$. Prove that $\mathbb{F}$ is a subfield of K. Show that $\mathbb{F} = K$. [5]
   (c) Conclude that there exist finite fields of order p^n for any $n \geq 1$. [2]
   (d) Let F be a finite field of characteristic p. Show that F must be a splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$ for some $n \geq 1$. [4]

7. Find all integer solutions of the equation $Y^2 + 1 = X^3$. You may use, without proof, the facts that $\mathbb{Z}[i]$ is a UFD, and the units of $\mathbb{Z}[i]$ are $\{1, -1, i, -i\}$. [7]