

Instructions:

1. The point value of each exercise occurs adjacent to the problem.
2. No books or notes or calculators are allowed.

Page	Points Possible	Points
2	22	
3	22	
4	18	
5	18	
6	16	
7	20	
8	20	
9	20	
10	16	
11	14	
12	14	
Total	200	

1. Let G be a finite group of order pqr , where $p > q > r$ are prime integers.

(a) (5 pts) If G fails to have a normal subgroup of order p , how many elements does G have of order p ?

Justify your answer.

(b) (5 pts) If G fails to have a normal subgroup of order q , justify the assertion that G has at least q^2 element of order q .

2. (12 pts) Let G be a group with $|G| = 2k$, where k is an odd positive integer. Prove or disprove that G must have a subgroup of order k .

3. Let p be a prime integer, let \mathbb{F}_p denote the finite field with p elements, and let $G = GL_2(\mathbb{F}_p)$ be the group of 2×2 invertible matrices with entries in \mathbb{F}_p .

(a) (5 pts) What is the order of the group G ?

(b) (5 pts) Exhibit a Sylow p -subgroup of G .

(c) (12 pts) How many Sylow p -subgroups does G have? Justify your answer.

4. (18 pts) Prove that the ring $R = \mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain.

5. (18 pts) Let R be a commutative ring with $1 \neq 0$, and consider the polynomial

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[x],$$

Assume there exists a nonzero polynomial $q(x) = b_m x^m + \cdots + b_0 \in R[x]$ such that $q(x)p(x) = 0$. Prove or disprove that there exists a nonzero element $b \in R$ such that $bp(x) = 0$.

6. Let F be a field and let \mathcal{P} be the set of all nonconstant monic polynomials $f = f(x) \in F[x]$. For each $f \in \mathcal{P}$, let x_f be an indeterminate. Let R be the polynomial ring over F in the indeterminates $\{x_f : f \in \mathcal{P}\}$. Thus $R = F[\{x_f : f \in \mathcal{P}\}]$. Let I be the ideal of R generated by the polynomials $f(x_f)$.

(a) (8 pts) Prove that $I \neq R$.

(b) (8 pts) Prove that there exists an extension field K of F such that each nonconstant monic polynomial $f(x) \in F[x]$ has a root in K .

7. Let $f(x) \in \mathbb{Q}[x]$ be a monic polynomial of degree n and let $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ be the roots of $f(x)$. Let G be the Galois group of $f(x)$ over \mathbb{Q} .

(a) (10 pts) Prove that $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if the action of G on $\{\alpha_1, \dots, \alpha_n\}$ is transitive.

(b) (10 pts) If the action of G on $\{\alpha_1, \dots, \alpha_n\}$ is doubly transitive, prove or disprove that \mathbb{Q} is the only proper subfield of $\mathbb{Q}(\alpha_1)$.

8. Let p be a prime integer. Recall that a field extension K/F is called a p -extension if K/F is Galois and $[K : F]$ is a power of p .

(a) (10 pts) If K/F and L/K are p -extensions, prove that the Galois closure of L/F is a p -extension.

(b) (10 pts) Give an example where K/F and L/K are p -extensions, but L/F is not Galois.

9. (20 pts) Let L/\mathbb{Q} be the splitting field of the polynomial $x^6 - 2 \in \mathbb{Q}[x]$. Diagram the lattice of subfields of L/\mathbb{Q} . For each subfield, give generators and list its degree over \mathbb{Q} . Indicate which of these subfields are Galois over \mathbb{Q} .

10. Let a and b be relatively prime positive integers.

(a) (8 pts) Prove that every integer n has the form $n = ax + by$, where $x, y \in \mathbb{Z}$ and $0 \leq x < b$.

(b) (8 pts) What is the largest integer n that cannot be written in the form $ax + by$, where x and y are both nonnegative integers? Justify your answer.

11. (8 pts) Let p be a prime integer, let $Z_p = \langle x \rangle$ be a cyclic group of order p and let $G = Z_p \times Z_p$. Describe the group $\text{Aut}(G)$. In particular, what is $|\text{Aut}(G)|$?

12. (6 pts) Let G be a finite group and let C be the center of G . If G/C is cyclic, does it follow that $C = G$? Justify your answer.

13. A subgroup M of a group G is said to be a *maximal subgroup* if $M \neq G$ and the only subgroups of G that contain M are M and G .

(a) (7 pts) If the group G is finitely generated and H is a proper subgroup of G , prove that there exists a maximal subgroup M of G such that $H \leq M$.

(b) (7 pts) Assume that G is finitely generated and has a unique maximal subgroup M . Prove or disprove that G is a cyclic group of order p^n , where p is a prime number and n is a positive integer.