

1. Define $f : X \rightarrow Y$ is one-to-one.
Define $f : X \rightarrow Y$ is onto.
Define g is the inverse of f .
2. Prove f is 1-1 onto iff f has an inverse.
3. Define transposition, n -cycle, disjoint cycles, parity, sign, crossing pair, crossing number, S_n , A_n .
4. Prove: Every permutation is the finite product of disjoint cycles.
5. Prove: Every cycle is the product of transpositions.
6. Prove: The order of an n -cycle is n .
7. Prove: If $\sigma = \tau_1\tau_2 \cdots \tau_n$ where the τ_i are disjoint cycles then

$$|\sigma| = lcm(|\tau_1|, |\tau_2|, \dots, |\tau_n|)$$

8. Prove: If the identity $\epsilon = \alpha_1 \cdots \alpha_n$ where α_i are transpositions, then n is even.
9. Prove: Every permutation can be written as either an even number of transpositions or an odd number, but not both.
10. Define homomorphism, isomorphism, automorphism, $G \simeq G'$, G is isomorphic to G' , $Aut(G)$, $Inn(G)$.
11. Prove h homomorphism implies $h(x^n) = h(x)^n$ for $n \in \mathbb{Z}$.
12. Prove h isomorphism implies $|x| = |h(x)|$.
13. Prove: Any two cyclic groups of the same order are isomorphic.
14. Prove: Every finite group is isomorphic to a subgroup of S_n for some n .
15. Prove: $Aut(\mathbb{Z}_n)$ is isomorphic to U_n .
16. State and Prove Lagrange's Thm.
17. Prove the corollaries of Lagrange:
 1. $|a|$ divides $|G|$ for all $a \in G$.
 2. If $|G|$ prime then G is cyclic.
 3. If $|G| = n$ then $a^n = e$ for all $a \in G$.
 4. (Little Fermat) If p prime then $a^p \equiv_p a$ for any integer a .

18. Prove: Let $\alpha : G \rightarrow G$ be an automorphism. Prove that α^{-1} is an automorphism of G .
19. Define $G \times H$ (this is the same as the book denotes $G \oplus H$).
20. Prove that $\mathbb{Z}_n \times \mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{nm}$ iff n and m are relatively prime.
21. State and Prove the Chinese remainder theorem.
22. Prove: Suppose that n and m are relatively prime, then $U(n) \times U(m) \simeq U(nm)$.
23. Define aH , Ha , $aHbH$, $H \triangleleft G$.
24. Suppose H is a subgroup of G . Prove the following are all equivalent:
1. $H \triangleleft G$
 2. $\forall a \in G \ aH \subseteq Ha$
 3. $\forall a \in G \ aHa^{-1} \subseteq H$
 4. $\forall a \in G \ aHa^{-1} = H$
 5. $\forall a, b \in G \ aHbH = abH$
25. Prove: Suppose $H \triangleleft G$. Then the cosets of H , $\{aH : a \in G\}$ form a group under the binary operation $(aH, bH) \mapsto aHbH$. This group is called the factor group or quotient group, G/H .
26. Prove: Suppose $\phi : G \rightarrow G'$ is a homomorphism. Then
- (1) $\ker(\phi) \stackrel{\text{def}}{=} \{x \in G : \phi(x) = e'\} \triangleleft G$
 - (2) ϕ is one-to-one iff $\ker(\phi) = \{e\}$
 - (3) $\phi(G) \stackrel{\text{def}}{=} \{\phi(x) : x \in G\}$ is a subgroup of G' .
 - (4) ϕ is onto iff $\phi(G) = G'$.
27. Prove: Suppose $H \triangleleft G$ then the quotient map defined by $\phi(a) = aH$ is an onto homomorphism

$$\phi : G \rightarrow G/H$$

with kernel H .

28. Prove: Suppose $\rho : G \rightarrow G'$ is any onto homomorphism and let $H = \ker(\rho)$ and let $\phi : G \rightarrow G/H$ be the quotient map. Then there exists an isomorphism

$$\alpha : G/H \rightarrow G'$$

such that $\rho = \alpha \circ \phi$.