
Definitions

Define the following terms.

1. group
2. order
3. homomorphism
4. isomorphism
5. automorphism
6. inner-automomorphism.

Computations

7. Construct an explicit isomorphism $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, *)$. What is $(\phi)^{-1}$?
8. Show that multiplication by π is automorphism $\phi : (\mathbb{R}, +) \to (\mathbb{R}, +)$. What is $(\phi)^{-1}$?
9. Prove that $(\mathbb{Z}, +)$ is isomophic to a proper subgroup of itself.

10. Let $G = U(15) \bigoplus Z_{10} \bigoplus S_5$. Find the order of (2,3,(123)(15)).
11. Find the inverse of (2,3,(123)(15)) in the group G above.
12. Find the cyclic subgroups of $U(30)$.

13. Decode the following message. Assume the RSA algorithm was used to produce it, the encryption exponent was e = 11, and the primes were p = 71 and q = 43. Decode the message by breaking the message into two digit groups. Assume A = 01, B = 02, ..., Z = 26 and a space is 28.
    534 1580 1496 485 494 1496 2370 440 1496 1875 485 2276 2265 485 01 485 440 2353 2370 2603 01 1875 485 2265 1411 2048 2445 2370 2353 1411
14. Suppose my RSA public key information is e = 11 and n = 899. Send me a short scrambled message.

Symmetries of objects

15. Describe the group of rotational symmetries of the tetrahedron.
16. Describe the group of rotational symmetries of the cube.

Symmetric groups

17. How many elements of order 3 are there in S_4?
18. Compute this product in S_4. (123)(314)
19. What is the order of this element in S_4? (1234)(24)(1432)

Short proofs

20. Explicitly show that an inner-automorphism is an isomorphism.

21. Use the result above to show that if two cycles are conjugate in S_4 then they have the same cycle length.

22. Let $f : G \to K$ be a homomorphism. Prove that $ker(f)$ is a normal subgroup of G.

23. If $H < G$ and $|G : H| = 2$ show that $H \lhd G$. Use this to prove that $A_4 \lhd S_4$.

24. Show that no group can have exactly two elements of order two.

25. Consider $G = U(16)$ and $H = \{1, 15\}$ and $K = \{1, 9\}$.
(a) Determine if H and K are isomorphic subgroups of G. Justify your conclusions.
(b) Determine if G/H and G/K are isomorphic factor groups. Justify your conclusions.

26. Show that $SL(2, \mathbb{R}) \lhd GL(2, \mathbb{R})$ and the factor group $GL(2, \mathbb{R})/SL(2, \mathbb{R})$ is isomorphic to some very familiar group. What is this group? (Justify your answer.)

27. Prove that $D_4/Z(D_4)$ is isomorphic to $Z_2 \bigoplus Z_2$.