Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 6, 2020

Problems in the Section 2.8.

1. Are the following mappings automorphism of their respective groups?
a) G a group of integers under addition, $T : x \to -x$.

Solution. T is clearly a homomorphism since $(x+y)T = -(x+y) = -x-y = xT + yT$. Surjection and injection are clear as $(-x)T = x$ for all $x \in \mathbb{Z}$ and $-x = -y$ implies $x = y$. Hence, T is an automorphism. □

b) G group of positive reals under multiplication, $T : x \to x^2$.

Solution. T is an automorphism. Note that $(xy)T = (xy)^2 = x^2y^2 = (xT)(yT)$ so that T is a homomorphism. It has the trivial kernel. Hence, injective. Moreover, $\sqrt{x}T = x$ for any $x > 0$ in reals. Thus, T is bijective and hence an automorphism. □

c) G cyclic group of order 12, $T : x \to x^3$.

Solution. Let $G = (a)$ for some $a \in G$. T is not an automorphism since $aT = a^3 = a^5T$ but $a \neq a^5$. □

d) G is the group S_3, $T : x \to x^{-1}$.

Solution. T is not an automorphism since $(xy)T = y^{-1}x^{-1} \neq x^{-1}y^{-1} = xTyT$ for any order 2 element x and any order 3 element y. □

2. Let G be a group, H a subgroup of G, T an automorphism of $(H)T = \{hT : h \in H\}$. Prove $(H)T$ is a subgroup of G.

Proof. Let $h_1T, h_2T \in (H)T$. Then $h_1T \cdot h_2T = (h_1h_2)T \in (H)T$ and $(h_1^{-1})T = (h_1T)^{-1} \in (H)T$. These facts imply that $(H)T$ is a subgroup of G. □

3. Let G be a group, T an automorphism of G, N a normal subgroup of G. Prove that $(N)T$ is an normal subgroup of G.

Proof. Clearly, $(N)T$ is a subgroup. Now, since T is an automorphism, for any $g \in G$, $g_0T = g$ with some $g_0 \in G$. Choose $nT \in (N)T$. Then $g(nT)g^{-1} = g_0TnTg_0^{-1}T = (g_0ng_0^{-1})T \in (N)T$ implying $(N)T$ is normal in G. ☐

4. For $G = S_3$, prove that $G \simeq \mathscr{I}(G)$

Proof. Note that for $G = S_3$, $Z(G) = \{e\}$. Using $G/Z(G) \simeq \mathscr{I}(G)$, we have $G \simeq \mathscr{I}(G)$. ☐

5. For any group G prove that $\mathscr{I}(G)$ is a normal subgroup of $\mathscr{A}(G)$ (the subgroup $\mathscr{A}(G)/\mathscr{I}(G)$ is called the group of outer automorphisms of G.

Proof. Let $T \in \mathscr{A}(G)$ and $T_g \in \mathscr{I}(G)$. For all $x \in G$,

$$(x)TT_gT^{-1} = (xT)T_gT^{-1} = (g(xT)g^{-1})T^{-1} = ((g_0)T(xT)(g_0^{-1})T)T^{-1} = g_0xg_0^{-1} = xT_{g_0} \in \mathscr{I}(G)$$

for some $g_0 \in G$. Hence, $\mathscr{I}(G)$ is normal in $\mathscr{A}(G)$. ☐

6. Let G be a group of order 4, $G = \{e, a, b, ab\}$, $a^2 = b^2 = e$, $ab = ba$. Determine $\mathscr{A}(G)$.

Proof. Let us consider G as a set of 4 elements. Then the number of bijections between the same G are given by $4! = 24$. But among these, since we seek a homomorphism, identity element e must be mapped to e. Thus we are left out with $4!/4 = 3!$ choices. Listing the candidates for the automorphisms, we have

$$e = \begin{pmatrix} e & a & b & ab \\ e & a & b & ab \end{pmatrix}, \phi = \begin{pmatrix} e & a & b & ab \\ e & b & a & ab \end{pmatrix}, \psi = \begin{pmatrix} e & a & b & ab \\ e & b & ab & a \end{pmatrix},$$
$$\begin{pmatrix} e & a & b & ab \\ e & a & ab & b \end{pmatrix}, \begin{pmatrix} e & a & b & ab \\ e & ab & a & b \end{pmatrix}, \begin{pmatrix} e & a & b & ab \\ e & ab & b & a \end{pmatrix}.$$

Note that $\phi^2 = e$, $\psi^3 = e$, and

$$\psi \cdot \phi = \begin{pmatrix} e & a & b & ab \\ e & a & ab & b \end{pmatrix}, \phi \cdot \psi = \begin{pmatrix} e & a & b & ab \\ e & ab & a & b \end{pmatrix}, \psi^2 \cdot \phi = \begin{pmatrix} e & a & b & ab \\ e & ab & b & a \end{pmatrix}.$$

Now we check that 6 bijections are in fact, homomorphisms. Observe that

$$\begin{aligned}
&e(ab) = ab = e(a)e(b), \quad \phi(ab) = ab = ba = \phi(a)\phi(b),\\
&\psi(ab) = a = b^2a = b(ba) = b(ab) = \psi(a)\psi(b),\\
&(\psi\phi)(ab) = b = a^2b = a(ab) = (\psi\phi)(a)(\psi\phi)(b),\\
&(\phi\psi)(ab) = b = ba^2 = (ba)a = (ab)a = (\phi\psi)(a)(\phi\psi)(b),\\
&(\psi^2\phi)(ab) = a = ab^2 = (ab)b = (\psi^2\phi)(a)(\psi^2\phi)(b).
\end{aligned}$$

Therefore, these 6 bijections are the whole automorphisms of G. Moreover, $\mathscr{A}(G) \simeq S_3$. ☐

7. a) A subgroup C of G is said to be a characteristic subgroup of G if $(C)T \subset C$ for all automorphisms T of G. Prove a characteristic subgroup of G must be a normal subgroup of G.

Proof. Let $g \in G$ and $T \in \mathscr{A}(G)$. Choose $c \in C$. Note that $gcg^{-1}T = gTcTg^{-1}T = g_0(cT)g_0^{-1} = (cT)T_{g_0} \in C$ for some $g_0 \in G$. Hence, C is normal in G. $\square$

b) Prove that the converse of a) is false.

Proof. Consider the group G defined in the Problem 6(Klein-4 group). Let $N = \{e, a\}$. Clearly, N is normal in G. But for $\phi \in \mathscr{A}(G)$, $a\phi = b \notin N$. This implies N is not a characteristic subgroup of G. $\square$

8. For any group G, prove that the commutator subgroup G' is a characteristic subgroup of G.

Proof. Let $a, b \in G$. It is enough to show that $aba^{-1}b^{-1}$ is closed under automorphism T in G'. Note that

$$aba^{-1}b^{-1}T = (aT)(bT)(a^{-1}T)(b^{-1}T) \in G'.$$

Hence, G' is a characteristic subgroup of G. $\square$

9. If G is a group, N a normal subgroup of G, M a characteristic subgroup of N, prove that M is a normal subgroup of G.

Proof. Let $g \in G$. Define a mapping $\phi_g : N \to N, n \mapsto gng^{-1}$. Since N is normal in G, this is well defined automorphism in N. Now, choose $m \in M$. Since $mT \in M$, so does $m\phi_g = gmg^{-1} \in M$. Thus, M is normal in G. $\square$

10. Let G be a finite group, T an automorphism of G with the property that $xT = x$ for $x \in G$ if and only if $x = e$. Prove that every $g \in G$ can be represetned as $g = x^{-1}xT$ for some $x \in G$.

Proof. Let us define a mapping $\phi : G \to G$ by $\phi(x) = x^{-1}(xT)$. Note that if $x^{-1}(xT) = y^{-1}(yT)$, we have $yx^{-1} = (yx^{-1})T$ implying $x = y$. Thus, ϕ is in fact an injection. Now by Pigeonhole Principle, we have ϕ a bijection. Hence, every $g \in G$ can be represented as $g = x^{-1}xT$ for some $x \in G$. $\square$

11. Let G be a finite group, T an automorphism of G with the property that $xT = x$ if and only if $x = e$. Suppose further that $T^2 = I$. Prove that G must be abelian.

Proof. Let $g \in G$. Then there is a $x \in G$ such that $g = x^{-1}xT$. Consequently, $g^{-1} = (x^{-1}xT)^{-1} = (x^{-1})Tx$. Also, $gT = (x^{-1}xT)T = (x^{-1})Tx$. Thus, we have $gT = g^{-1}$ for all $g \in G$. Now, for any $x, y \in G$,

$$xyx^{-1}y^{-1} = xy(xT)(yT) = xy \cdot (xy)T = xy(xy)^{-1} = xyy^{-1}x^{-1} = e \implies xy = yx.$$

Hence G is abelian. □

12. Let G be a finite group and suppose the automorphism T sends more than three-quarters of the elements of the elements of G onto their inverses. Prove that $xT = x^{-1}$ for all $x \in G$ and that G is abelian.

Proof. We shall denote the number of elements of a finite set S by $|S|$. We define a set A by

$$A = \{x \in G : xT = x^{-1}\}.$$

Choose $a \in A$. Let $K = A \cap a^{-1}A$. Observe that

$$\begin{aligned} |K| = \left|A \cap a^{-1}A\right| &= |A| + \left|a^{-1}A\right| - \left|A \cup a^{-1}A\right| \\ &> \frac{3}{4}|G| + \frac{3}{4}|G| - |G| = \frac{1}{2}|G| \end{aligned}$$

so that $|K| > \frac{1}{2}|G|$. Let $k \in K$. Then we have $T(ak) = a^{-1}k^{-1} = k^{-1}a^{-1}$ so that $k \in N(a)$. Hence, $K \subset N(a)$. But from $|K| > \frac{1}{2}|G|$, by Lagranges theorem, $N(a) = G$. Clearly, $a \in Z(G)$. But since this holds for every $a \in A$, we have that $|Z(G)| > \frac{3}{4}|G| \implies Z(G) = G$. Hence, G is abelian. □

13. In Problem 12, can you find an example of a finite group which is non-abelian and which has an automorphism which maps exactly three-quarters of the elements of G onto their inverses?

Proof. Let G be the group of quaternions. Define $T : G \to G$ by $xT = -x$. Clearly T is an automorphism in G. Note that for $\pm i, \pm j, \pm k$, T sends those to their inverses. But $1T = -1, -1T = 1$. Hence, T is an automorphism sending exactly third quarters of G to their inverses but G is non-abelian. □

14. Prove that every finite group having more than two elements has a nontrivial automorphism

Proof. Let us first consider non-abelian case. Since $\mathscr{I}(G) \simeq \dfrac{G}{Z(G)}$, We know that there exits a $g \in G$ such that $T_g \neq I$. Suppose G is an abelian group with not every elements is of its self inverses. Define $T : G \to G$ by $gT = g^{-1}$. Clearly T is an automorphism with $x_0 \neq x_0^{-1}$ for some $x_0 \in G$. Thus, $T \neq I$. Now if G is an abelian group with every elements is of its self inverses. Choose any $a, b \neq e \in G$. We define a mapping $T : G \to G$ by interchanging a and b while keeping rest of the elements fixed. Then T is also a non-trivial automorphism. Hence, we have proved that every finite group having more than two elements has a nontrivial automorphism. □

15. Let G be a group of order $2n$. Suppose that half of the elements of G are of order 2, and the other half form a subgroup H of order n. Prove that H is of odd order and is an abelian subgroup of G.

Proof. Suppose H is of even order. Then H must contain an element of order 2, which is a contradiction. Thus, H is of odd order. Now, since $[G : H] = 2$, H is normal in G. Thus, we can represent G as $G = H \amalg xH$ for some $x^2 = e$. Since we know that the elements of $G - H$ are of order 2, $(xh)^2 = e$ for all $h \in H$. Now choose $a, b \in H$. Consequently,

$$ab = axx^{-1}b = xa^{-1}b^{-1}x = x(ba)^{-1}x = x^2(ba) = ba$$

so that H is abelian. Hence proved. □

16. Let $\phi(n)$ be the Euler ϕ-function. If $a > 1$ is an integer, prove that $n \mid \phi(a^n - 1)$.

Proof. Consider the group $G = U_{a^n-1}$. Then the number of elements in G is given by $\phi(a^n - 1)$. Note that $\gcd(a^k, a^n - 1) = 1$ for any $k \in Z$. Also, note that $(a) = \{a^k : k = 0, 1, \cdots n-1\}$, a subgroup of G generated by a, is of order n. Thus, by Lagranges theorem, $n \mid \phi(a^n - 1)$. □

17. Let G be a group and Z be the center of G. If T is any automorphism of G, prove that $(Z)T \subset Z$.

Proof. Let $g \in G, z \in Z$. Since $g_0T = g$ for some $g_0 \in G$,

$$g(zT) = (g_0T)(zT) = (g_0z)T = (zg_0)T = (zT)(g_0T) = (zT)g.$$

Hence $(Z)T \subset Z$. □

18. Let G be a group and T an automorphism of G. If, for $a \in G$, $N(a) = \{x \in G : xa = ax\}$, prove that $N(aT) = (N(a))T$.

Proof. Let $x \in N(aT)$. Then $x(aT) = (aT)x \iff x_0a = ax_0$ for some x_0 such that $x_0T = x$. Thus, $x = x_0T \in (N(a))T$. Now suppose $y = xT \in (N(a))T$. Then by definition, $xa = ax$, so that $y(aT) = (aT)y$. Hence, $y \in N(aT)$. Therefore, we conclude that $N(aT) = (N(a))T$. □

19. Let G be a group and T an automorphism of G. If N is a normal subgroup of G such that $(N)T \subset N$, show how you could use T to defined an automorphism of G/N.

Proof. This problem quite faulty; We need further assumption that $[G : N] < \infty$. □

20. Use the discussion following Lemma 2.8.3. to construct a) a non-abelian group of order 55.

Solution. Define $G = (a)$, $a^{11} = e$, $\phi : a^i \mapsto a^{3i}$. Then $\phi^5 = I$ so that ϕ is an automorphism of G of order 5. Let x be a symbol where we formally subject to the following condition: $x^5 = e$, $x^{-1}a^i x = \phi(a^i) = a^{3i}$. Consider

$$G' = \{x^i a^j : i = 0, 1, \cdots, 4,\ j = 0, 1, \cdots 10\},$$

where $x^i a^j = x^k a^l \iff i \equiv k \pmod 5, j \equiv l \pmod{11}$ and $x^5 = a^{11} = e$, $x^{-1}ax = a^3$. Then G' is a non-abelian group of order 55. □

b) a non-abelian group of order 203.

Solution. Define $G = (a)$, $a^{29} = e$, $\phi : a^i \mapsto a^{-4i}$. Then $\phi^7 = I$ so that ϕ is an automorphism of G of order 7. Now apply the method established for the above problem a). In this way, we obtain a non-abelian group of order 203. □

21. Let G be the group of order 9 generated by elements a, b, where $a^3 = b^3 = e$. Find all the automorphisms of G.

Solution. First, we know that the group of order 9 is abelian. Now, suppose ϕ is an automorphism of G. Since the order of element is preserved under automorphisms and every elements in G is of order 3, there are 8 possibilities for the values of $\phi(a)$ and remaining 7 for the values of $\phi(b)$. But not every 56 mappings is automorphism. Note that we have to remove out the case where $\phi(ab) = e$. Suppose $\phi(ab) = \phi(a)\phi(b) = a^p b^q a^r b^s = a^{p+r} b^{q+s}$. $\phi(ab) = e \iff p + r \equiv 0 \pmod 3, q + s \equiv 0 \pmod 3$, where not both p, q are zero at the same time and similarly for r, s. The possible ordered pair of p, q, r, s for $\phi(ab) = e$ are:

$$(0, 1, 0, 2), (0, 2, 0, 1), (1, 1, 2, 2), (1, 2, 2, 1)$$
$$(1, 0, 2, 0), (2, 1, 1, 2), (2, 2, 1, 1), (2, 0, 1, 0).$$

Hence, there are 48 automorphisms in G. □