Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 6, 2020

Problems in the Section 2.7.

1. In the following, verify if the mappings defined are homomorphisms and in those cases in which they are homomorphisms, determine the kernel.
a) G is a group of nonzero real numbers under multiplication, $\overline{G} = G, \phi(x) = x^2$ all $x \in G$.

Solution. ϕ is a homomorphism. Note that $\phi(xy) = (xy)^2 = x^2y^2 = \phi(x)\phi(y)$ in G. Let K be the kernel of ϕ. $x^2 = 1$ implies $x = -1$ or $x = 1$. Hence, $K = \{-1, 1\} \simeq \mathbb{Z}_2$. □

b) G, $\overline{G}$ as in a), $\phi(x) = 2^x$

Solution. ϕ is not a homomorphism as $\phi(2 \cdot 1) = 2^2 = 4 \neq 8 = 2^2 \cdot 2^1 = \phi(2)\phi(1)$. □

c) G is the group of real numbers under addition, $\overline{G} = G$, $\phi(x) = x + 1$ all $x \in G$.

Solution. ϕ is not a homomorphism as $\phi(2) = 3 \neq 4 = 2 + 2 = \phi(1) + \phi(1)$. □

d) $G, \overline{G}$ as in c), $\phi(x) = 13x$ for $x \in G$.

Solution. ϕ is a homomorphism. Note that $\phi(x+y) = 13(x+y) = 13x+13y = \phi(x)+\phi(y)$ in G. Let K be the kernel of ϕ. Since $13x = 0 \iff x = 0$, $K = \{0\}$. □

e) G be any abelian group, $\overline{G} = G$, $\phi(x) = x^5$ all $x \in G$.

Solution. ϕ is a homomorphism. Note that $\phi(xy) = (xy)^5 = x^5y^5 = \phi(x)\phi(y)$ in G. Let K be the kernel. Sicen $x^5 = e \iff x$ is of order 5 or $x = e$, K is the collection of all elements of G of order 5. □

2. Let G be any group, g a fixed elements in G. Define $\phi : G \to G$ by $\phi(x) = gxg^{-1}$. Prove that ϕ is an homomorphism of G onto G.

Proof. Note that $\phi(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \phi(x)\phi(y)$ for all $x, y \in G$. Hence, ϕ is a homomorphism. Suppose $\phi(x) = e$. Equivalently, $gxg^{-1} = e \implies x = e$, so that the kernel K of ϕ is (e). Thus, ϕ is an isomorphism(injection). Further, for all $x \in G$, $\phi(g^{-1}xg) = x$, implying ϕ is onto. Therefore, ϕ is an onto isomorphism(automorphism). □

3. Let G be any finite abelian group of order $o(G)$ and suppose the integer n is relatively prime to $o(G)$. Prove that every $g \in G$ can be written as $g = x^n$ with $x \in G$.

Proof. Consider a mapping $\phi : G \to G$ defined as $\phi(x) = x^n$. Note that $\phi(xy) = (xy)^n = x^n y^n = \phi(x)\phi(y)$ so that ϕ is a homomorphism. Suppose $x^n = e$. Then since $\gcd(n, o(G)) = 1$, $n\lambda + o(G)\mu = 1$ for some $\lambda, \mu \in \mathbb{Z}$, $x = x^{n\lambda + o(G)\mu} = e$, implying the kernel K of ϕ is (e), so that ϕ is an isomorphism(injection). Now by Pigeonhole principle, as ϕ is an injection from G to G, it is also onto. Therefore, ϕ is a bijection. This finishes the proof. □

4. a) Given any group G and a subset U, let $\hat{U}$ be the smallest subgroup of G which contains U. Prove there is such a subgroup $\hat{U}$ in G.

Proof. Let $\hat{U} = \bigcap_{U \subset W \leq G} W$, intersection of all subgroups of G containing U. Clearly, $\hat{U}$ is a subgroup of G containing U. Let W' be another subgroup of G containing U. Then $\bigcap_{U \subset W \leq G} W \subset W'$, implying $\hat{U}$ is the smallest subgroup of G containing U. □

b) If $gug^{-1} \in U$ for all $g \in G, u \in U$, prove that $\hat{U}$ is a normal subgroup of G.

Proof. Note that every elements in $\hat{U}$ can be represented as in the form of finite products of U, raised to integer exponents. That is,

$$u \in \hat{U} \iff u = u_1^{k_1} u_2^{k_2} \cdots u_n^{k_n}, \quad u_i \in U,\ k_i \in \mathbb{Z},\ i = 1, 2, \cdots, n,$$

Let $u \in \hat{U}$. Adopting the representation of u introduced above,

$$\begin{aligned} gug^{-1} &= g u_1^{k_1} u_2^{k_2} \cdots u_n^{k_n} g^{-1} \\ &= (gu_1g^{-1})^{k_1} (gu_2g^{-1})^{k_2} \cdots (gu_ng^{-1})^{k_n} \\ &= (u_1')^{k_1} (u_2')^{k_2} \cdots (u_n')^{k_n} \in \hat{U} \quad (\because g u_i g^{-1} = u_i' \in U) \end{aligned}$$

for all $g \in G$. Hence, $\hat{U}$ is normal in G. □

5. Let $U = \{xyx^{-1}y^{-1} : x, y \in G\}$. In this case $\hat{U}$ is usually written as G' and is called the commutator subgroup of G.
a) Prove that G' is normal in G.

Proof. Note that for all $g, x \in G$, $(gxg^{-1})^{-1} = gx^{-1}g^{-1}$ and hence

$$\begin{aligned} g(xyx^{-1}y^{-1})g^{-1} &= gx \cdot (g^{-1}g) \cdot y \cdot (g^{-1}g) \cdot x^{-1} \cdot (g^{-1}g) \cdot y^{-1}g^{-1} \\ &= (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1}) \in U. \end{aligned}$$

Now apply b) of the Problem 4. We see that G' is normal in G. □

b) Prove that G/G' is abelian.

Proof. For any $a, b \in G$, $abG' = baa^{-1}b^{-1}abG' = ba(a^{-1}b^{-1}ab)G' = baG'$. Hence, G/G' is abelian. □

c) If G/N is abelian, prove that $G' \subset N$.

Proof. As G/N is abelian, $abN = baN \implies a^{-1}b^{-1}ab \in N$ for all $a, b \in G$. Since $a^{-1}b^{-1}ab \in G'$, and a, b arbitrary, $G' \subset N$. □

d) Prove that if H is a subgroup of G and $G' \subset H$, then H is normal in G.

Proof. Note that $ghg^{-1} = ghg^{-1}h^{-1}h = (ghg^{-1}h^{-1})h \in H$ for all $g \in G, h \in H$. Hence, H is normal in G. □

6. If N, M are normal subgroups of G, prove that $NM/M \simeq N/N \cap M$.

Proof. NM is subgroup of G (Problem 3, Section 2.6). Now consider a mapping $\phi : N \to NM/M$ defined by $\phi(n) = nM$. We show that ϕ is a homomorphism. Note that

$$\phi(n_1 n_2) = n_1 n_2 M = n_1 M n_2 M = \phi(n_1)\phi(n_2)$$

so that ϕ is a homomorphism. Moreover, for any $nM \in NM/M$, $\phi(n) = nM$ so that ϕ is onto. Now, we can apply isomorphism theorem. Note that for $n \in N$, $\phi(n) = M \iff n \in M$, so that the kernel of ϕ is $N \cap M$. Hence,

$$\frac{N}{N \cap M} \simeq \frac{NM}{M}.$$

□

7. Let V be the set of real numbers, and for a, b real, $a \neq 0$ let $\tau_{ab} : V \to V$ defined by $\tau_{ab}(x) = ax + b$. Let $G = \{\tau_{ab} : a, b \in \mathbb{R}, a \neq 0\}$ and let $N = \{\tau_{1b} \in G\}$. Prove that N is a normal subgroup of G and that $G/N \simeq$ group of nonzero real numbers under multiplication.

Proof. We know that N is normal in G, by applying Problem 23 of Section 2.6. Now, we define a mapping $\phi : G \to \mathbb{R} - \{0\}$ by $\phi(\tau_{ab}) = a$. Note that ϕ is a homomorphism since for any non-zero $a, c \in \mathbb{R}$, $b, d \in \mathbb{R}$,

$$\phi(\tau_{ab} \cdot \tau_{cd}) = \phi(\tau_{ac,ad+b}) = a \cdot c = \phi(\tau_{ab})\phi(\tau_{cd}).$$

Moreover, ϕ is cleary onto. Let K be the kernel of ϕ. Then the elements of $k \in K$ satisfies $\phi(k) = 1$. But by the definition of N, we see that K is exactly N. Applying the isomorphism theorem, we have $G/N \simeq \mathbb{R} - \{0\}$. □

8. Let G be the dihedral group defined as the set of all formal symbols $x^i y^j$, $i = 0, 1$, $j = 0, 1, \cdots, n-1$, where $x^2 = e, y^n = e, xy = y^{-1}x$. Prove
a) The subgroup $N = \{e, y, y^2, \cdots, y^{n-1}\}$ is normal in G.

Proof. It it easy to see that $N = (y)$, and hence, a cyclic subgroup of G. Moreover, $[G : N] = 2$, implying N is normal in G. □

b) That $G/N \simeq W$, where $W = \{-1, 1\}$ is the group under the multiplication of the real numbers.

Proof. From $o(G/N) = 2$, we have $G/N \simeq \mathbb{Z}_2$ the only possible case. Hence, $G/N \simeq \{-1, 1\} = W$. □

9. Prove that the center of a group is always a normal subgroup.

Proof. Note that any $z \in Z(G)$ satisfies $gzg^{-1} = z \in Z(G)$ for all $g \in G$. Hence $Z(G)$ is clearly normal in G. □

10. Prove that a group of order 9 is abelian.

Proof. Let G be the group of order 9. Suppose there is an $a \in G$ such that $(a) = G$, we are done. If not, for all $a \in G$, $(a) \subsetneq G$. It is impossible that G to have no non-trivial subgroup, otherwise G would be a group of prime order, contradicting that $o(G) = 9$. So, we can find a subgroup (a) of order 3. Now, take $b \in G - (a)$ and consider (b). The only possible order of b is 3, hence (b) is a subgroup of order 3. Note that,

$$o((a) \cdot (b)) = \frac{o(a) \cdot o(b)}{o((a) \cap (b))}$$

and since $(a) \cap (b) = (e)$, $o((a)(b)) = 9$ and hence $(a)(b) = G$. It is now possible to write G as $G = \{e, a, a^2, b, b^2, ab, ab^2, a^2b, a^2b^2\}$. Now we investigate if which of the elements stated initially, equals $ba \in G$. Observe that

$$\begin{aligned}
&ba \neq e, a, a^2, b, b^2 \quad \text{trivially,} \\
&ba = a^2b \implies aba = b, \quad (ba)^3 = e \implies bababa = bab(aba) = bab^2 \implies ba = b \perp, \\
&ba = ab^2 \implies bab = a, \quad (ba)^3 = e \implies bababa = (bab)aba = a^2ba \implies ba = a \perp, \\
&ba = a^2b^2 \implies (ab)^2 = e \perp,
\end{aligned}$$

hence the only possibility is $ba = ab$. This shows that G is abelian. □

11. If G is a non-abelian group of order 6, prove that $G \simeq S_3$.

Proof. Since G is of even order, there exists an element $a \in G$ such that $a^2 = e$. Obviously, there is no element of order 6, otherwise G would be a cyclic group. We claim that there is an element $b \in G$ of order 3. If not, every non-identity element in G would be order of 2, so that G is abelian, contradicting that G is non-abelian. Thus, there must an element b of order 3. Since $(a) \cap (b) = (e)$, and from the equation

$$o((a) \cdot (b)) = \frac{o(a) \cdot o(b)}{o((a) \cap (b))},$$

we have that $o((a)(b)) = 6$ so that $(a)(b) = G$. Hence, $G = \{e, a, b, b^2, ab, ab^2\}$. We investigate if which of in G equals $b^{-1}a$. Clearly, $b^{-1}a \neq e, a, b, b^2$. Suppose $b^{-1}a = ab^2$. Then $ab = (bb^{-1}) \cdot ab = b(ab^2)b = ba$ implying G is abelian, hence a contradiction. The only remaining possibility is $b^{-1}a = ab$. But this implies that $G = \{e, a, b, b^2, ab, ab^2\}$. This group G with an operation property $ab = b^{-1}a$ is exactly isomorphic to the symmetric group S_3. Therefore, $G \simeq S_3$. □

12. If G is abelian and if N is any subgroup of G, prove that G/N is abelian.

Proof. Since G is abelian, N is normal in G. Moreover, for any $a, b \in G$, $(ab)N = (ba)N$. Thus, G/N is abelian. □

13. Let G be the dihedral group defined in Problem 8. Find the center of G.

Proof. We consider the case of $n > 2$, otherwise the center of G is G itself trivially. By the result of the Problem 17 in Section 2.6, if the order of n is odd, $Z(G) = (e)$, and if the order of n is even, $\{e, y^{n/2}\} \subset Z(G)$. We find if any other elements $x^i y^j$ of G is in $Z(G)$, for the order of n is even. In general, elements of the form xy^k cannot be in the center as if

$$(y^{-1}x)xy^k(xy) = y^{k-1}y^{-1}x = y^{k-2}x,$$

but $k \equiv k - 2 \pmod{n}$ will not hold if $n > 2$. Thus, we consider only the elements of the form y^k. Also note that

$$(xy)y^k(y^{-1}x) = xy^k x,$$

so that if $y^k = xy^k x$, $y^k x = xy^k = y^{-k}x \iff k = 0, n/2$. Hence, the only possible elements of the form y^k are $e, y^{n/2}$. This shows that the center of G is $\{e, y^{n/2}\}$ exactly, whenever $n > 2$ and n is of even order. Summarising,

$$Z(G) = \begin{cases} G, & o(G) = 2, 4 \\ (e), & n > 2, n \equiv 1 \pmod{2} \\ \{e, y^{n/2}\}, & n > 2, n \equiv 0 \pmod{2}. \end{cases}$$

□

14. Let G be as in Problem 13. Find G', the commutator subgroup of G.

Proof. Note that $y^{2k} = y^k x y^{-k} x$ so that $y^{2k} \in G'$. Equivalently, $(y^2) \subset G'$. Note that $(y^2) = N$ if n is odd and $(y^2) = \{e, y^2, \cdots, y^{n-2}\}$ if n is even. Moreover, (y^2) is normal in G. Hence, $o(G/(y^2)) = 2$ if n is odd and $o(G/(y^2)) = 4$ if n is even. Thus, $G/(y^2)$ is abelian. Applying the result of Problem 5 c), $G' \subset (y^2)$. Therefore, $G' = (y^2)$. □

15. Let G be the group of non-zero complex numbers under multiplication and let N be the set of complex numbers of absolute value 1 (that is, $a + bi \in N$ if $a^2 + b^2 = 1$). Show that G/N is isomorphic to the group of all positive real numbers under multiplication.

Proof. Let us define a mapping $\phi : G \to \mathbb{R} - \{0\}$ by $\phi(z) = |z|$. Clearly, ϕ is a homomorphism since $\phi(zw) = |zw| = |z|\,|w| = \phi(z)\phi(w)$. Now for any $k > 0 \in \mathbb{R}$, $\phi(k + 0i) = k$ so that ϕ is onto. We now investigate the kernel of ϕ. Obviously, it is set of all nonzero complex numbers of absolute value 1, that is, exactly, N. Now by isomorphism theorem, $G/N \simeq \mathbb{R} - \{0\}$. □

16. Let G be the group of all nonzero complex numbers under multiplication and let $\overline{G}$ be the group of all real 2×2 matrices of the form $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, where not both a and b are 0, under matrix multiplication. Show that G and $\overline{G}$ are isomorphic by exhibiting an isomorphism of G onto $\overline{G}$.

Proof. Define a mapping $\phi : G \to \overline{G}$ by $\phi(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. ϕ is a homomorphism since

$$\begin{aligned}
\phi((a+bi)\cdot(c+di)) &= \phi(ac - bd + (ad + bc)i) \\
&= \begin{pmatrix} ac - bd & ad + bc \\ ad + bc & ac - bd \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \\
&= \phi(a + bi)\phi(c + di).
\end{aligned}$$

Also, ϕ is clearly one-one and onto. Hence, ϕ yields an isomorphism of G onto $\overline{G}$. □

17. Let G be the group of real numbers under addition and let N be the subgroup of G consisting of all integers. Prove that G/N is isomorphic to the group of all complex numbers of absolute value 1 under multiplication.

Proof. For convenience of the proof, we denote S_1 to be the group of all complex numbers of absolute value 1. We define a mapping $\phi : G \to S_1$ by $\phi(g) = e^{2\pi g i}$, where e is the euler constant, i is the imaginary number. We show ϕ is a homomorphism. Note that

$$\phi(g + h) = e^{2\pi(g+h)i} = e^{2\pi g i} \cdot e^{2\pi h i} = \phi(g)\phi(h)$$

so that ϕ is homomorphism. Moreover, from that fact that arbitrary elements of S_1 is expressible in the form $e^{2\pi ki}$, ϕ is onto. So, we can apply the isomorphism theorem. We now investigate the kernel of ϕ. Since $e^{2\pi ki} = 1 \iff k \in \mathbb{Z}$, N is exactly the kernel of ϕ. Hence, $G/N \simeq S_1$. □

18. Let G be the group of all real 2×2 matrices $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$, with $ad - bc \neq 0$, under matrix multiplication, and let

$$N = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in G : ad - bc = 1 \right\}.$$

Prove that $N \supset G'$, the commutator subgroup of G.

Proof. It is sufficient to check that the determinant of commutator is 1. Note that $\det(ABA^{-1}B^{-1}) = \det(A)\det(B)\det(A^{-1})\det(B^{-1}) = 1$ for all $A, B \in G$. Hence, $G' \subset N$. □

19. In Problem 18 show, in fact, that $N = G'$.

Proof. Note that for any $x \in \mathbb{R}$,

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{-1},$$
$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}^{-1},$$
$$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1}$$

so that $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$ and $\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$ are commutators. Also,

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} -1 & 0 \\ 1 & 2 \end{pmatrix}^{-1}$$

so that $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is also a commutator. We can also check that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & \frac{b}{a} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$$

for $a \neq 0$. If $a = 0$, then it is must that $b \neq 0$ and

$$\begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -\frac{d}{b} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{b} & 0 \\ 0 & b \end{pmatrix}$$

so that in either cases, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a product of commutators. Therefore, $N \subset G'$ and hence, $N = G'$. □

20. Let G be the group of all real 2×2 matrices of the form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, where $ad \neq 0$, under matrix multiplication. Show that G' is precisely the set of all matrices of the form $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$.

Proof. Let N be the set of all matrices of the form $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$. Then from the Problem 21 of section 2.6, We have that N is normal subgroup of G and G/N is abelian, so that $G' \subset N$. Now, take $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in N$. Just like we have done in Problem 19,

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{-1},$$

hence a commutator of G. Hence, $N \subset G'$. Therefore, $N = G'$. □

21. Let S_1 and S_2 be two sets. Suppose that there exists a one-to-one mapping ψ of S_1 into S_2. Show that there exists an isomorphism $A(S_1)$ into $A(S_2)$, where $A(S)$ mean the set of all one-to-one mapping of S onto itself.

Proof. Note that ψ is one-to-one. Hence, we define $g : \psi(S_1) \to S_1$ by $g(y) = \psi^{-1}|_{\psi(S_1)}(y)$. Consequently, $g \circ \psi = id_{S_1}$. Now we define a mapping $f : A(S_1) \to A(S_2)$ by

$$f(\phi)(y) = \begin{cases} \psi \circ \phi \circ g(y), & \text{if } y \in \psi(S_1), \\ id_{S_2}(y), & \text{else} \end{cases}$$

We see that $f(\phi) \in A(S_2)$. Moreover, it is a homomorphism since

$$\begin{aligned} f(\phi_1 \circ \phi_2) &= \begin{cases} \psi \circ \phi_1 \phi_2 \circ g(y) = (\psi \circ \phi_1 \circ g) \circ (\psi \circ \phi_2 \circ g)(y), & \text{if } y \in \psi(S_1), \\ id_{S_2}(y), & \text{else} \end{cases} \\ &= f(\phi_1) f(\phi_2) \end{aligned}$$

and also one-one clearly. Hence, we have exhibited an isomorphism(monomorphism) of $A(S_1)$ to $A(S_2)$. □