Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 3, 2020

Problems in the section 2.1. $\sim$ 2.3.

1. In the following determine whether the systems described are groups. If they are not, point out which of the group axioms fail to hold.
a) $G =$ set of all integers, $a \cdot b \equiv a - b$.

Solution. G is not a group. For instance,

$$1 - (2 - 1) = 1 - 1 = 0 \neq -2 = (1 - 2) - 1,$$

which shows that the associative property is not preserved in G. □

b) $G =$ set of all positive integers, $a \cdot b = ab$, the usual product of integers.

Solution. G is not a group. There is no inverse of $2 \in G$ in G. □

c) $G = a_0, a_1, \cdots, a_6$ where

$$\begin{cases} a_i \cdot a_j = a_{i+j} & \text{if } i + j < 7, \\ a_i \cdot a_j = a_{i+j-7} & \text{if } i + j \geq 7 \end{cases}$$

Solution. G is a group. We have the operation table as follows:

$\cdot$	a_0	a_1	a_2	a_3	a_4	a_5	a_6
a_0	a_0	a_1	a_2	a_3	a_4	a_5	a_6
a_1	a_1	a_2	a_3	a_4	a_5	a_6	a_0
a_2	a_2	a_3	a_4	a_5	a_6	a_0	a_1
a_3	a_3	a_4	a_5	a_6	a_0	a_1	a_2
a_4	a_4	a_5	a_6	a_0	a_1	a_2	a_3
a_5	a_5	a_6	a_0	a_1	a_2	a_3	a_4
a_6	a_6	a_0	a_1	a_2	a_3	a_4	a_5

The above operation table shows that G is closed under associative operation $\cdot$. Clearly, a_0 is the only identity element. We also see that the inverses of a_i are a_{7-i}, respectively (and also unique). Therefore, G is a group. □

d) $G =$ set of all rational numbers with odd denominators, $a \cdot b \equiv a + b$, the usual addition of rational numbers.

Solution. We shall slightly change the conditions of the question a bit, by re-defining the set G as: $G =$ set of all rational numbers $\frac{a}{b}, b \neq 0$ where b can be written odd. Now we claim that G is a group: For any two arbitrary elements $x, y \in G$, it follows that

$$x = \frac{a_1}{2b_1 + 1}, \quad y = \frac{a_2}{2b_2 + 1}, \quad x \cdot y = \frac{2a_1b_2 + a_1 + 2a_2b_1 + a_2}{(2b_1 + 1)(2b_2 + 1)}, \quad a_1, a_2, b_1, b_2 \in \mathbb{Z}$$

implying G is closed under the given operation. Associativity is clear, since the operation is just inherited from the usual addition defined on $\mathbb{Q}$, which is clearly associative. Moreover, we have $0 = \frac{0}{1}$ as the identity element, and for any $x \in G$, $-x \in G$ is the unique inverse. Therefore, G is a group. □

2. Prove that if G is an abelian group, then for all $a, b \in G$ and for all integers n, $(a \cdot b)^n = a^n \cdot b^n$.

Proof. We use mathematical induction. For $n = 1$, the hypothesis is trivially true. Suppose we assume that the hypothesis is true for $n = k$, that is, $(a \cdot b)^k = a^k \cdot b^k$. Now for $n = k+1$,

$$(a \cdot b)^{k+1} = (a \cdot b)(a \cdot b)^k = a \cdot (a \cdot b)^k \cdot b = a \cdot a^k \cdot b^k \cdot b = a^{k+1} \cdot b^{k+1},$$

implying that the hypothesis is valid for $n = k + 1$. Hence proved. □

3. If G is a group such that $(a \cdot b)^2 = a^2 \cdot b^2$ for all $a, b \in G$, show that G must be abelian.

Proof. From the given relation, by applying left and right cancellation law simultaneously we get $b \cdot a = a \cdot b$. This shows that G is abelian. □

4. If G is a group in which $(a \cdot b)^i = a^i \cdot b^i$ for three consecutive integers i for all $a, b \in G$, show that G is abelian.

Proof. We can assume that

$$(a \cdot b)^{n+1} = a^{n+1} \cdot b^{n+1}, \quad (a \cdot b)^n = a^n \cdot b^n, \quad (a \cdot b)^{n-1} = a^{n-1} \cdot b^{n-1}$$

for some integer $n \in \mathbb{Z}$. From the first and second equations, we have that

$$\begin{aligned} (a \cdot b)(a \cdot b)^n = (a \cdot b)^{n+1} = a^{n+1} \cdot b^{n+1} &\implies a \cdot b \cdot a^n \cdot b^n = a^{n+1} \cdot b^{n+1} \\ &\implies b \cdot a^n = a^n \cdot b. \end{aligned}$$

Similarly from the second and thrid equations, we have $b \cdot a^{n-1} = a^{n-1} \cdot b$. Moreover,

$$a^n \cdot b = b \cdot a^n = (b \cdot a^{n-1}) \cdot a = (a^{n-1} \cdot b) \cdot a \implies a \cdot b = b \cdot a$$

implying G is abelian. □

5. Show that the conclusion of Problem 4 does not follow if we assume the relation $(a \cdot b)^i = a^i \cdot b^i$ for just two consecutive integers.

Proof. From the assumption, we have

$$(a \cdot b)^{n+1} = a^{n+1} \cdot b^{n+1}, \quad (a \cdot b)^n = a^n \cdot b^n,$$

but $(a \cdot b)^{n-1} \neq a^{n-1} \cdot b^{n-1}$. But if we assume G to be abelian(for the sake of contradiction), we have $(a \cdot b)^i = a^i \cdot b^i$ for all $i \in \mathbb{Z}$. This yields a contradiction and hence, G cannot be abelian. □

6. In S_3 give an example of two elements x, y such that $(x \cdot y)^2 \neq x^2 \cdot y^2$.

Proof. Take $x = \phi, y = \psi \cdot \phi$. Then we have

$$(x \cdot y)^2 = (\phi \cdot (\psi \cdot \phi))^2 = (\psi^2)^2 = \psi \neq e = e \cdot e = (\phi)^2 \cdot (\psi \cdot \phi)^2 = x^2 \cdot y^2.$$

Hence proved. □

7. In S_3 show that there are four elements satisfying $x^2 = e$ and three elements satisfying $y^3 = e$.

Proof. By simple calculations, we can check that $x = e, \phi, \phi \cdot \psi, \psi \cdot \phi$ satisfies $x^2 = e$ and $y = e, \psi, \psi^2$ satisfies $y^3 = e$. □

8. If G is a finite group, show that there exists a positive integer N such that $a^N = e$ for all $a \in G$.

Proof. Let us write $G = \{a_1, a_2, \cdots, a_m\}$. Choose any $a_i \in G$. Consider the following sequence of the elements of G:

$$a_i, a_i^2, a_i^3, \cdots, a_i^m, a_i^{m+1}, \cdots$$

Since every elements of the above sequence is in G, clearly $a_i^j = a_i^k$ for some positive integers $j, k (k > j)$. Let $n_i = k - j$. Then $a_i^{n_i} = e$. Now set $N = n_1 n_2 \cdots n_m$. Consequently, $a^N = e$ for any $a \in G$. □

9. a) If the group G has three elements, show it must be abelian.

Proof. Let $G = \{e, a, b\}$, a group of three elements. It follows that $a \cdot b \neq a, b$ otherwise it would imply that b and a are identity elements, respectively. The only possibility is that $a \cdot b = e$, and $b \cdot a = e$ for the same reason, vice versa. This implies $a \cdot b = b \cdot a$, so that G is abelian. □

b) Do part a) if G has four elements.

Proof. For the sake of contradiction, assume that $a \cdot b \neq b \cdot a$ for some non-identity elements $a, b \in G$. Clearly, $a \cdot b \neq a, b$. Suppose $a \cdot b = e$. But this implies $a = b^{-1}$, so that $b \cdot a = e = a \cdot b$, which is a contradiction. So we have $a \cdot b \neq e, a, b, b \cdot a$, implying G constitute of at least 5 or more elements. But G is a group of 4 elements, therefore a contradiction. □

c) Do part a) if G has five elements.

Proof. As in the part b), we have 5 distinct elements $e, a, b, a \cdot b, b \cdot a$ in G. Consider $a \cdot a = a^2 \in G$. By simple case by case comparison, it is must that $a^2 = e$. Now we consider $a \cdot (b \cdot a) = aba$. This, in fact, must equal to one of the elements in G. But

$$\begin{aligned}
aba = e &\implies a \cdot b = a \implies b = e \quad \perp, \\
aba = a &\implies b \cdot a = e \quad \perp, \\
aba = b &\implies a \cdot b = b \cdot a^{-1} \implies a \cdot b = b \cdot a \quad \perp, \\
aba = a \cdot b &\implies a = e \quad \perp, \\
aba = b \cdot a &\implies a = e \quad \perp,
\end{aligned}$$

so that a contradiction. This shows that G must be abelian. □

10. Show that if every element of the group G is its own inverse, then G is abelian.

Proof. It is easy to see that

$$a \cdot b = a^{-1} \cdot b^{-1} = (b \cdot a)^{-1} = b \cdot a$$

for all $a, b \in G$. Hence G is abelian. □

11. If G is a group of even order, prove it has an element $a \neq e$ satisfying $a^2 = e$.

Proof. For any element $a \in G$, a has unique inverse b. Hence, we can pair them up, in a way that

$$e, (a_1, b_1), (a_2, b_2), \cdots$$

where $a_i, b_i \in G$ are non-identity distinct elements and satisfies $a_i \cdot b_i = e$. Suppose one of the element in G is of self-inverse, then we are done. If not, since the elements in each pair (a_i, b_i) are distinct, and since G is of even order, this result in left over of an element $g \in G$, with no distinct inverse element. This forces that g is of self inverse, and hence, $g^2 = e$. □

12. Let G be a nonempty set closed under an associative product, which in addition satisfies:
a) There exists an $e \in G$ such that $a \cdot e = a$ for all $a \in G$.
b) Give $a \in G$, there exists an element $y(a) \in G$ such that $a \cdot y(a) = e$. Prove that G must be a group under this product.

Proof. Note that

$$\begin{aligned} e \cdot a &= (a \cdot y(a)) \cdot (a \cdot e) \\ &= a \cdot y(a) \cdot a \cdot (y(a) \cdot y(y(a))) \\ &= a \cdot y(a) \cdot y(y(a)) \\ &= a \cdot e \end{aligned}$$

and

$$\begin{aligned} y(a) \cdot a &= y(a) \cdot (a \cdot e) \\ &= y(a) \cdot a \cdot (y(a) \cdot y(y(a))) \\ &= y(a) \cdot y(y(a)) \\ &= e \end{aligned}$$

These finish the proof. □

13. Prove, by an example, that the conclusion of Problem 12 is false if we assume instead: a) There exists an $e \in G$ such that $a \cdot e = a$ for all $a \in G$. b) Given $a \in G$, there exists $y(a) \in G$ such that $y(a) \cdot a = e$.

Proof. Consider the set $G = \left\{ \begin{pmatrix} x & x \\ y & y \end{pmatrix} : x, y \text{ are non negative rationals, not both zero} \right\}$. By setting $e = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, we have

$$\begin{pmatrix} x & x \\ y & y \end{pmatrix} \cdot e = \begin{pmatrix} x & x \\ y & y \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & x \\ y & y \end{pmatrix}$$

for all x, y. Morever, by setting $y(a) = \begin{pmatrix} \frac{1}{x+y} & \frac{1}{x+y} \\ 0 & 0 \end{pmatrix}$, it is easy to see that

$$y(a) \cdot \begin{pmatrix} x & x \\ y & y \end{pmatrix} = \begin{pmatrix} \frac{1}{x+y} & \frac{1}{x+y} \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x & x \\ y & y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = e.$$

But G is not a group, since

$$e \cdot a = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x & x \\ y & y \end{pmatrix} = \begin{pmatrix} x+y & x+y \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} x & x \\ y & y \end{pmatrix} = a.$$

□

14. Suppose a finite set G is closed under an associative product and that both cancellation laws hold in G. Prove that G must be a group.

Proof. Let $a \in G$. By considering the infinite collection $a, a^2, a^3, \cdots$, since G is finite, there must be positive integers $k, l (k > l)$ satisfying $a^k = a^l$. Let $e = a^{k-l}$. Now for any $b \in G$, $b \cdot a^k = b \cdot a^l \implies b \cdot a^{k-l} = b$. For the inverse element, we set $a^{-1} = a^{k-l-1}$. Then $a \cdot a^{-1} = a \cdot a^{k-l-1} = a^{k-l} = e$. Now with the help of Problem 12, G is now a group. □

15. a) Using the result of Problem 14, prove that the nonzero integer modulo p, p a prime number, form a group under multiplication mod p.

Proof. Note that the given set is finite and closed under multiplication mod p. What we have to show is, in this set, the left and right cancellation laws must hold. But from the basic number theoretic discussion, whenever $\gcd(a, p) = 1$,

$$ab \equiv ac \mod p \implies b \equiv c \mod p, \quad ba \equiv bc \mod p \implies b \equiv c \mod p.$$

Now we apply the result of Problem 14. Since every elements a in the set is relatively prime to p, above relation holds entirely in the set. Thence given set is a group. □

b) Do part a) for the nonzero integers relatively prime to n under multiplication mod n.

Proof. Just change p into n in the above discussion. Then we are done. □

16. In Problem 14 show by an example that if one just assumed one of the cancellation laws, then the conclusion need not follow.

Proof. Let G be the given set. Define a binary operation $\cdot : G \times G \to G$ by $x \cdot y = y$. Then for any $x, y, z \in G$,

$$x \cdot (y \cdot z) = x \cdot z = z = y \cdot z = (x \cdot y) \cdot z$$

implying the operation is associative, and

$$x \cdot y = x \cdot z \implies y = z$$

implying left cancellation law holds. But the clearly right cancellation law does not hold. □

17. Prove that in Problem 14 infinite examples exist, satisfying the conditions, which are not groups.

Proof. Consider the set of all non-negative integers. Then clearly it is closed under usual addition of the integers, satisfying both the cancellation laws. But there is no inverse of every positive integers, proving that it is not a group. □

18. For any $n > 2$ construct a non-abelian group of order $2n$.

Proof. Define G by:

$$G = \{x^i y^j : i = 0, 1, j = 0, 1, 2, \cdots, n-1, x^2 = e, y^n = e, xyx^{-1} = y^{-1}\}.$$

Clearly G is a non-abelian group of order $2n$. For a detailed proof, you can refer to the Problem 17 of section 2.7. □

19. If S is a set closed under an associative operation, prove that no matter how you bracket $a_1 a_2 \cdots a_n$, retaining the order of the elements, you get the same element in S (e.g., $(a_1 \cdot a_2) \cdot (a_3 \cdot a_4) = a_1 \cdot (a_2 \cdot (a_3 \cdot a_4))$; use induction on n.

Proof. If $n = 1$, then it is trivial. Suppose we use strong induction on n, that is, the way of bracketing the elements of number less than n, with retaining its order, does not change its output. Now considering any arbitrary bracket-ization of $a_1, a_2, \cdots a_n$, there must be an outermost bracket(this may not be unique), with at least one or more elements a_i lying outside of that specific bracket. Then this bracket must consist of at most $n-1$ elements of the S. Applying induction hypothesis, we can just purely consider the elements in this bracket as a single element, resulting into at most $n-1$ product of elements. But by applying induction hypothesis again, we are done. □

20. Let G be th set of all real 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $ad - bc \neq 0$ is a rational number. Prove that G forms a group under matrix multiplication.

Proof. Let $A \in G, A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. By the definition of determinant, $ad - bc = \det(A)$. Suppose $A, B \in G$. Then by the property of determinant, $\det(AB) = \det(A)\det(B)$. As $\det(A), \det(B) \neq 0$ and rational, so does $\det(AB)$. Hence, G is closed under usual matrix multiplication. Associativity also holds clearly. The identity element is $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. For the inverse element of $A \in G$, just take the well known $A^{-1} = \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Now we see that G is a group. □

21. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, where $ad \neq 0$. Prove that G forms a group under matrix multiplication. Is G abelian?

Proof. Let $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, B = \begin{pmatrix} p & q \\ 0 & r \end{pmatrix} \in G$. Then

$$A \cdot B = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} p & q \\ 0 & r \end{pmatrix} = \begin{pmatrix} ap & aq + br \\ 0 & dr \end{pmatrix} \in G.$$

Hence G is closed under matrix multiplication. Associativity is also clear. We also take $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ as the identity element, and inverse element of $A \in G$ as $A^{-1} = \frac{1}{ad}\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix}$. Therefore, G is a group. But it is not abelian, since

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 7 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 5 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

□

22. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, where $a \neq 0$. Prove that G is an abelian group under matrix multiplication.

Proof. Let $A = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, B = \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \in G$. Then

$$A \cdot B = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & (ab)^{-1} \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = B \cdot A.$$

Hence G is closed under matrix multiplication and abelian. Associativity is also clear. We also take $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ as the identity element, and inverse element of $A \in G$ as $A^{-1} = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}$. Therefore, G is an abelian group. □

23. Construct in the G of Problem 21 a subgroup of order 4.

Proof. Let $H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$. It is easy to see that they are closed under matrix multiplication. We have the identity element $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Moreover, every elements are of self-inverses. Therefore, H is a subgroup of G of order 4. □

24. Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are integers modulo 2, such that $ad - bc \neq 0$. Using matrix multiplications as the operation in G, prove that G is a group of order 6..

Proof. Checking G a group can be done with the help of Problem 14. We now show that G is a group of order 6. In fact, we shall prove a more general result, that is, finding the order of such group where integers are given with modulo p, p a prime number. For an arbitrary element $A \in G$, possible numbers of filling the first low in the matrix is p^2. Since we have $ad - bc \neq 0$, we discard the possibilities of filling the low with all zero. Hence, we have $p^2 - 1$ possibilities of filling up the first low. Now, we fill the second low of the

matrix. The condition $ad - bc \neq 0$ implies that the first low and second low in the matrix must be linearly independent, so that we discard the possibilities that second low being the multiple of the first low, that is, p possibilities. Hence there are $p^2 - p$ possibilities of filling up the second low for each given fixed first low. Consequently, there are $(p^2 - 1)(p^2 - p)$ elements in G. Let $p = 2$. Then there are $(2^2 - 1)(2^2 - 2) = 6$ elements in G. This is to be proved. □

25. a) Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $ad - bc \neq 0$ and a, b, c, d are integers modulo 3, relative to matrix multiplication. Show that $o(G) = 48$.

Proof. Using the arguments made in Problem 24, the order of G is $(3^2-1)(3^2-3) = 48$. □

b) If we modify the example of G in part a) by insisting that $ad - bc = 1$, then what is $o(G)$?

Proof. We again prove a more general result, that is, for the mod p, p a prime number. Note that any element in G can be made into determinant 1 by dividing(mod p) the second row by $1, 2, \cdots, p-1$. Hence there are $\dfrac{(p^2 - 1)(p^2 - p)}{p - 1} = p(p^2 - 1)$ elements, with determinant 1. For $p = 3$, there are 24 elements. □

26. a) Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where and a, b, c, d are integers modulo p, p a prime number, such that $ad - bc \neq 0$. G forms a group relative to matrix multiplication. what is $o(G)$?
sol) From the arguments made in Problem 24 25, we know that $o(G) = (p^2 - 1)(p^2 - p)$.

b) Let H be the subgroup of the G of part a) defined by

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

What is $o(H)$?
sol) From the arguments made in Problem 24 25, we know that $o(H) = p(p^2 - 1)$.