Abstract Algebra Chapter 3

—— —— (-)

December 30, 2022

Important Statements:

One-Step Subgroup Test:

Let G be a group and H a nonempty subset of G. If ab^{-1} is in H whenever a and b are in H, then H is a subgroup of G. (In additive notation, if $a - b$ is in H whenever a and b are in H, then H is a subgroup of G.)

Two-Step Subgroup Test:

Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a and b are in H (H is closed under the operation), and a^{-1} is in H whenever a is in H (H is closed under taking inverses), then H is a subgroup of G.

Finite Subgroup Test:

Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

$\langle a \rangle$ Is a Subgroup:

Let G be a group, and let a be any element of G. Then, $\langle a \rangle$ is a subgroup of G.

Center of a Group:

The *center*, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G. i.e.

$$Z(G) = \{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}$$

Center is a Subgroup:

The center of a group G is a subgroup of G.

Centralizer of a in G:

Let a be a fixed element of a group G. The *centralizer* of a in G, $C(a)$, is the set of all elements in G that commute with a. i.e.

$$C(a) = \{g \in G \mid ga = ag\}$$

$C(a)$ is a Subgroup:

For each a in a group G, the centralizer of a is a subgroup of G.

Notation:

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

End of Chapter Exercises

Question 1.

For each group in the following list, find the order of the group and the order of each element in the group. What relation do you see between the orders of the elements of a group and the order of the group?

(a) $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

(b) $U(10) = \{1, 3, 7, 9\}$

(c) $U(12) = \{1, 5, 7, 11\}$

(d) $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

(e) $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$

The order of each element of a group is a divisor of the order of the group.

Question 2.

Let $\mathbb{Q}$ be the group of rational numbers under addition and let $\mathbb{Q}^\star$ be the group of nonzero rational numbers under multiplication. In $\mathbb{Q}$, list the elements in $\langle \frac{1}{2} \rangle$. In $\mathbb{Q}^\star$, list the elements in $\langle \frac{1}{2} \rangle$.

$\langle \frac{1}{2} \rangle$ in $\mathbb{Q} = \{\frac{n}{2} \mid n \in \mathbb{Z}\}$

$\langle \frac{1}{2} \rangle$ in $\mathbb{Q}^\star = \{\left(\frac{1}{2}\right)^n \mid n \in \mathbb{Z}\}$

Question 3.

Let $\mathbb{Q}$ and $\mathbb{Q}^\star$ be as in Question 2. Find the order of each element in $\mathbb{Q}$ and in $\mathbb{Q}^\star$.

The elements of $\mathbb{Q}$ and $\mathbb{Q}^\star$ have infinite order, except their respective identity elements.

Question 4.

Prove that in any group, an element and its inverse have the same order.

Let G be a group with element a, and $|a| = n$. Then, n is the lowest integer for which $a^n = e$.

$$\begin{aligned} e &= e^{-1} \\ &= (a^n)^{-1} \\ &= (a * a * \cdots * a)^{-1} \\ &= a^{-1} * a^{-1} * \cdots * a^{-1} \\ &= (a^{-1})^n \end{aligned}$$

Question 5.

Without actually computing the orders, explain why the two elements in each of the following pairs of elements from $\mathbb{Z}_{30}$ must have the same order: $\{2, 28\}, \{8, 22\}$. Do the same for the following pairs of elements from $U(15)$: $\{2, 8\}, \{7, 13\}$.

For $\{2, 28\}, \{8, 22\}$, it is easy to see that each element is the inverse of its corresponding element. By the previous Question, they have the same order.

For $U(15) : \{2, 8\}, \{7, 13\}$, a similar argument holds.

More thoroughly, $2 + 28 = 0 \mod 30$ and $8 + 22 = 0 \mod 30$. Also $2 * 8 = 16 = 1 \mod 15$ and $7 * 13 = 91 = 1 \mod 15$.

Question 6.

Suppose that a is a group element and $a^6 = e$. What are the possibilities for $|a|$? Provide reasons for your answer.

The posibilities for $|a|$ are 1,2,3, and 6.

If a itself is the identity element, then $|a| = 1$.

If $a^2 = e$, then $a^6 = (a^2)^3 = e^3 = e$. And similarly for $|a| = 3$.

If $|a| = 4$, then $a^6 = e * a^2 \neq e$. Also, if $|a| = 5$, then $a^6 = e * a \neq e$. So neither 4 or 5 are the order of a.

Question 7.

If a is a group element and a has infinite order, prove that $a^m \neq a^n$ when $m \neq n$.

Without loss of generality, assume $m > n$. For the purpose of contradiction, assume $a^m = a^n$.

$$\begin{aligned} a^m &= a^n * a^{m-n} && \text{Associativity} \\ &= a^m * a^{m-n} && \text{Equality of } m \text{ and } n \\ &= a^n * a^{m-n} * a^{m-n} && \text{Associativity} \\ &= a^m * a^{m-n} * \cdots * a^{m-n} && \text{Repetition of above} \end{aligned}$$

Because we know that $a^{m-n} \neq e$ (else either $|a| = m - n$, or $m = n$ contradicting our assumption), and $a^{m-n} = e$ is the only way the above equalities hold, our presupposition must be false and so $a^m \neq a^n$. $\square$

Question 8.

Let x belong to a group. If $x^2 \neq e$ and $x^6 = e$, prove that $x^4 \neq e$ and $x^5 \neq e$. What can we say about the order of x?

Clearly, $|a| \neq 1$ or 2.

To see that $x^4 \neq e$ we need to show that $x^4 = x^{-2} \neq e$. We get $x^4 = x^{-2}$ by multiplying both sides of $x^6 = e$ with x^{-2}. For the purpose of contradiction assume $x^{-2} = e$, then $e = e^{-1} = (x^2)^{-1} \Rightarrow x^2 = e$ which goes against our presupposition.

To see that $x^5 \neq e$, with a similar argument as above, we need to show that $x^5 = x^{-1} \neq e$. Again we assume $x^{-1} = e$ but then, $x = e$ and $|x| = 1$. So $|a| \neq 5$.

It may be that $|a|$ is either 3 or 6, but no higher.

Question 9.

Show that if a is an element of a group G, then $|a| \leq |G|$.

Question 10.

Show that $U(14) = \langle 3 \rangle = \langle 5 \rangle$. (Hence, $U(14)$ is cyclic.) Is $U(14) = \langle 11 \rangle$?

Firstly, $U(14) = \{1, 3, 5, 9, 11, 13\}$

Then,

$$\begin{aligned}\langle 3\rangle &= \{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\}\\ &= \{1, 3, 9, 27, 81, 243\}\\ &= \{1, 3, 9, 13, 11, 5\}\\ &= U(14)\end{aligned}$$

Similarly,

$$\begin{aligned}\langle 5\rangle &= \{5^0, 5^1, 5^2, 5^3, 5^4, 5^5\}\\ &= \{1, 5, 25, 125, 625, 3125\}\\ &= \{1, 5, 11, 13, 9, 3\}\\ &= U(14)\end{aligned}$$

We also see that,

$$\begin{aligned}\langle 11\rangle &= \{11^0, 11^1, 11^2, 11^3, 11^4, 11^5\}\\ &= \{1, 11, 121, 1331, 14641, 161051\}\\ &= \{1, 11, 9, 1, 11, 9\}\\ &\neq U(14)\end{aligned}$$

Question 11.

Show that $U(20) \neq \langle k\rangle$ for any k in $U(20)$. (Hence, $U(20)$ is not cyclic.)

We have $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$ and,

$$\begin{aligned}\langle 1\rangle &= \{1\}\\ \langle 3\rangle &= \{1, 3, 7, 9\}\\ \langle 7\rangle &= \{1, 3, 7, 9\}\\ \langle 9\rangle &= \{1, 9\}\\ \langle 11\rangle &= \{1, 11\}\\ \langle 13\rangle &= \{1, 9, 13, 17\}\\ \langle 17\rangle &= \{1, 9, 13, 17\}\\ \langle 19\rangle &= \{1, 19\}\end{aligned}$$

Question 12.

Prove that an Abelian group with two elements of order 2 must have a subgroup of order 4.

Let a, b be elements of G an Abelian group, and $\langle a \rangle = \langle b \rangle = 2$. i.e.

$$a^2 = e \text{ and } b^2 = e$$

Question 13.

Find groups that contain elements a and b such that $|a|, |b|$, and $|ab|$?

(a) $|ab| = 3$

(b) $|ab| = 4$

(c) $|ab| = 5$

Question 14.

Suppose that H is a proper subgroup of $\mathbb{Z}$ under addition and that H contains 18, 30, and 40. What are the possibilities for H?

Our strategy to find the subgroup H we find the smallest element and determine its "span". From 30 and 40 we see that $10 \in H$. Also, from 18 and 30 we have $12 \in H$. Therefore we also have $2 \in H$. So,

$$H = \{2n \mid n \in \mathbb{Z}\} = \langle 2 \rangle$$

Question 15.

Suppose that H is a proper subgroup of $\mathbb{Z}$ under addition and that H contains 12, 30, and 54. What are the possibilities for H?

Using the same strategy as above, we find the minimal nonidentity element to be 6. From this we have that $H = \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle,$ or $\langle 6 \rangle$.

Question 16.

Prove that the dihedral group of order 6 does not have a subgroup of order 4.

Question 17.

For each divisor $k > 1$ of n, let $U_k(n) = \{x \in U(n) \mid x \bmod k = 1\}$. (For example, $U_3(21) = \{1, 4, 10, 13, 16, 19\}$ and $U_7(21) = \{1, 8\}$.) List the elements of

(a) $U_4(20)$

(b) $U_5(20)$

(c) $U_5(30)$

(d) $U_{10}(30)$

Prove that $U_k(n)$ is a subgroup of $U(n)$.

Let $H = \{x \in U(10) \mid x \bmod 3 = 1\}$. Is H a subgroup of $U(10)$?

Question 18.

If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G. (Can you see that the same proof shows that the intersection of any number of subgroups of G, finite or infinite, is again a subgroup of G?)

Question 19.

Let G be a group. Show that $Z(G) = \cap_{a \in G} C(a)$. (This means that intersection of all subgroups of the gorm $C(a)$.)

Question 20.

Let G be a group, and let $a \in G$. Prove that $C(a) = C(a^{-1})$.

Question 21.

For any group element a and any integer k, show that $C(a) \subseteq C(a^k)$. Use this fact to complete the following statement: "In a group, if R is an integer and x commutes with a, then ...?" Is the converse true?

Question 22.

Complete the partial Cayley group table given below.

Question 23.

Suppose G is the group defined by the following Cayley table.

(a) Find the centralizer of each memeber of G.

(b) Find $Z(G)$.

(c) Find the order of each element of G. How are these orders arithmetically related to the order of the group?

Question 24.

If a and b are distinct group elements, prove that either $a^2 \neq b^2$ or $a^3 \neq b^3$.

Question 25.

Prove Theorem 3.6

Question 26.

Prove that $C(H)$ is a subgroup of G.

Question 27.

Must the centralizer of an element of a group be Abelian?

Question 28.

Must the center of a group be Abelian?

Question 29.

Let G be an Abelian group with identity e and let n be some fixed integer. Prove that the set of all elements of G that satisfy the equation $x^n = e$ is a subgroup of G. Give an example of a group G in which the set of all elements of G that satisfy the equation $x^2 = e$ does not form a subgroup of G.

Question 30.

Suppose a belongs to a group and $|a| = 5$. Prove that $C(a) = C(a^3)$. Find an element a from some group such that $|a| = 6$ and $C(a) \neq C(a^3)$.

Question 31.

Determine all finite subgroups of $\mathbb{R}^\star$, the group of nonzero real numbers under multiplication.

Question 32.

Suppose n is an even positive integer and H is a subgroup of $\mathbb{Z}_n$. Prove that either every member of H is even or exactly half of the members of H are even.

Question 33.

Suppose a group contains elements a and b such that $|a| = 4$, $|b| = 2$, and $a^3b = ba$. Find $|ab|$.

Question 34.

Suppose a and b are group elements such that $|a| = 2, b \neq e$, and $aba = b^2$. Determine $|b|$.

Question 35.

Let a be a group element of order n, and suppose that d is a positive divisor of n. Prove that $|a^d| = n/d$.

Question 36.

Consider the elements $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ from $SL(2, \mathbb{R})$. Find $|A|, |B|$, and $|AB|$. Does your answer surprise you?

Question 37.

Consider the element $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ in $SL(2, \mathbb{R})$. What is the order of A? If

we view $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ as a member of $SL(2, \mathbb{Z}_p)$ (p is a prime), what is the order of A?

Question 38.

For any positive integer n and any angle θ, show that in the group $SL(2, \mathbb{R})$,

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^n = \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}$$

Use this formula to find the order of

$$\begin{bmatrix} \cos 60^o & -\sin 60^o \\ \sin 60^o & \cos 60^o \end{bmatrix} \text{ and } \begin{bmatrix} \cos\sqrt{2^o} & -\sin\sqrt{2^o} \\ \sin\sqrt{2^o} & \cos\sqrt{2^o} \end{bmatrix}$$

(Geometrically, $A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ represents a rotation of the plane θ degrees.)

Question 39.

Let G be the symmetry group of a circle. Show that G has elements of every finite order as well as elements of infinite order.

Question 40.

Let x belong to a group of $|x| = 6$. Find $|x^2|, |x^3|, |x^4|$, and $|x^5|$. Let y belong to a group and $|y| = 9$. Find $|y^i|$ for $i = 2, 3, ..., 8$. Do these examples suggest any relationship between the order of the power of an element and the order of the element?

Question 41.

D_4 has seven cyclic subgroups. List them. Find a subgroup of D_4 of order 4 that is not cyclic.

Question 42.

$U(15)$ has six cyclic subgroups. List them.

Question 43.

Prove that a group of even order must have an element of order 2.

Question 44.

suppose G is a group that has exactly eight elements of order 3. How many subgroups of order 3 does G have?

Question 45.

Let H be a subgroup of a finite group G. Suppose that g belongs to G and n is the smallest positive integer such that $g^n \in H$. Prove that n divides $|g|$.

Question 46.

Compute the orders of the following groups,

(a) $U(3), U(4), U(12)$

(b) $U(5), U(7), U(35)$

(c) $U(4), U(5), U(20)$

(d) $U(3), U(5), U(15)$

On the basis of your answers, make a conjecture about the relationship among $|U(r)|, |U(s)|$, and $|U(rs)|$.

Question 47.

Let $\mathbb{R}^\star$ be the group of nonzero real number under multiplication and let $H = \{x \in \mathbb{R}^\star \mid x^2 \text{ is rational}\}$. Prove that H is a subgroup of $\mathbb{R}^\star$. Cana the exponent 2 be replaced by any positive integer and still have H be a subgroup?

Question 48.

Compute $|U(r)|, |U(s)|$, and $|U(rs)|$. Do these groups provide a counterexample to your answer to Question 46? If so, revise your conjecture.

Question 49.

Find a cyclic subgroup of order 4 in $U(40)$.

Question 50.

Find a noncyclic subgroup of order 4 in $U(40)$.

Question 51.

Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ under addition.
Let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G \mid a + b + c + d = 0 \right\}$. Prove that H is a subgroup of G. What if 0 is replaced by 1?

Question 52.

Let $H = \{A \in GL(2, \mathbb{R} \mid \det A \text{ is an integer power of } 2)\}$.Show that H is a subgroup of $GL(2, \mathbb{R})$.

Question 53.

Let H be a subgroup of $\mathbb{R}$ under addition. Let $K = \{2^a \mid a \in H\}$. Prove that K is a subgroup of $\mathbb{R}^\star$ under multiplication.

Question 54.

Let G be a group of functions from $\mathbb{R}$ to $\mathbb{R}^\star$, where the operation of G is multiplication of functions. Let $H = \{f \in G \mid f(2) = 1\}$. Prove that H is a subgroup of G. Can 2 be replaced by any real number?

Question 55.

Let $G = GL(2, \mathbb{R})$ and $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a \text{ and } b \text{ are nonzero integers} \right\}$ under the operation of matrix multiplication. Prove or disprove that H is a subgroup of $GL(2, \mathbb{R})$.

Question 56.

Let $H = \{a + bi \mid a, b \in \mathbb{R}, ab \geq 0\}$. Prove or disprove that H is a subgroup of $\mathbb{C}$ under addition.

Question 57.

Let $H = \{a + bi \mid a, b \in \mathbb{R}, a^2 + b^2 = 1\}$. Prove or disprove that H is a subgroup of $\mathbb{C}^\star$ under multiplication. Describe the elements of H geometrically.

Question 58.

The smallest subgroup containing a collection of elements S is the subgroup H with the property that if K is any subgroup containing S then K also contains H. (So, the smallest subgroup containing S is contained in every subgroup that contains S.) The notation for this subgroup is $\langle S \rangle$. In the group $\mathbb{Z}$,find

(a) $\langle 8, 14 \rangle$

(b) $\langle 8, 13 \rangle$

(c) $\langle 6, 15 \rangle$

(d) $\langle m, n \rangle$

(e) $\langle 12, 18, 45 \rangle$

In each part, find an integer k such that the subgroup is $\langle k \rangle$.

Question 59.

Let $G = GL(2, \mathbb{R})$.

(a) Find $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$

(b) Find $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$

(c) Find $Z(G)$

Question 60.

Let G be a finite group with more than one element. Show that G has an element of prime order.

Question 61.

Let a belong to a group and $|a| = m$. If n is relatively prime to m, show that a can be written as the nth power of some element in the group.

Question 62.

Let G be a finite Abelian group and let a and b belong to G. Prove that the set $\langle a, b\rangle = \{a^i b^j \mid i, j \in \mathbb{Z}\}$ is a subgroup of G. What can you say about $|\langle a, b\rangle|$ in terms of $|a|$ and $|b|$?