Math 71: Abstract Algebra

Prishita Dharampal

Sources: Talked to Sair Shaikh '26, Frank Gallo'27, and Math Stack Exchange.

Problem 1. Let G be a group and $a_1, a_2, \dots, a_r \in G$. We say that $a_1, \dots, a_r$ pairwise commute if a_i commutes with a_j for all i and j. We say that $a_1, \dots, a_r$ are rank independent if $a_1^{e_1} \dots a_r^{e_r} = 1$ implies that e_i is a multiple of $\mid a_i \mid$ for all i. The aim of this problem is to prove:

Proposition 0.1. *Let G be a group and $a_1, a_2, \dots a_r \in G$ be pairwise commuting rank independent elements of finite order. Then $\mid a_1 \dots a_r \mid = lcm(\mid a_1 \mid, \dots, \mid a_r \mid)$.*

1. (DF 1.1 Exercise 24) If a and b are commuting elements, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$. Hint: Do induction on n.

2. If $a_1, \dots, a_r$ are pairwise commuting elements, prove that $(a_1 \dots a_r)^n = a_1^n \dots a_r^n$. Hint: Do induction on r.

3. If $a_1, \dots, a_r$ are pairwise commuting elements of finite order (not necessarily rank independent), prove that $\mid a_1 \dots a_r \mid$ divides $lcm(\mid a_1 \mid, \dots, \mid a_r \mid)$. Hint: Raise $a_1 \dots a_r$ to the power $lcm(\mid a_1 \mid, \dots, \mid a_r \mid)$.

4. Prove the proposition. Hint: Do induction on r; for the base case $r = 1$ there is not much to say, and then you should realize that (after a bit of juggling with least common multipliers) the induction step just boils down to the case $r = 2$. Hint (for a different proof): Use the above characterization of the lcm to prove that $lcm(\mid a_1 \mid, \dots, \mid a_n \mid)$ divides $\mid a_1 \dots a_n \mid$. In any method you choose, be sure to highlight where the rank independence condition is used!

5. Show that disjoint cycles in S_n are rank independent, then deduce DF 1.3 Exercise 15.

Solution.

1. If a and b are commuting elements, then

$$(ab)^n = \underbrace{(ab)(ab)(ab)\dots(ab)}_{n-times}$$
$$(ab)^n = \underbrace{a(ba)b(ab)\dots(ab)}_{n-times}$$
$$(ab)^n = \underbrace{a(ab)b(ab)\dots(ab)}_{n-times}$$
$$(ab)^n = \underbrace{a^2b^2(ab)\dots(ab)}_{n-times}$$
$$(ab)^n = \underbrace{a^2ab^2b\dots(ab)}_{n-times}$$

   if we commute all of the elements to have all a together, we will be left with

$$(ab)^n = a^n b^n$$

2. If all elements in $a \in G$ are pairwise commuting, then let n be the product of all $a \in G$ such that:

$$n = a_1 a_2 \dots a_r$$

   then because a_i commutes with a_j for all i and j,

$$\implies n = a_2 a_1 a_3 \dots a_r$$
$$\implies n = a_2 a_3 a_1 \dots a_r$$

   upon doing this r times,

$$n = a_2 a_3 \dots a_r a_1$$

   and one could do this process n times to move any element n places in the equation, so we can see that the group G is abelian. So we can say,

$$(a_1 \dots a_r)^n = \underbrace{(a_1 \dots a_r)(a_1 \dots a_r)}_{n-times}$$
$$\implies (a_1 \dots a_r)^n = (\underbrace{a_1 \dots a_1}_{\text{n-times}})(\underbrace{a_2 \dots a_2}_{\text{n-times}})\dots(\underbrace{a_r \dots a_r}_{\text{n-times}})$$
$$\implies (a_1 \dots a_r)^n = a_1^n \dots a_r^n$$

3. Let $e_i, 1 \leq i \leq r$ be the orders of elements a_i, $n = a_1 \dots a_r$, $k =\mid n \mid$, then:

$$n^k = (a_1 \dots a_r)^k = 1$$
$$n^k = a_1^k \dots a_r^k = 1$$

   We can say that $k = lcm(\mid a_1 \mid \dots \mid a_r \mid)b, b \in \mathbb{Z}$

   Let $e_i, 1 \leq i \leq r$ be orders of elements from a_1 to a_r and let $n = a_1 \dots a_r$. F Also, we know that $a_i^{e_i} = a_i^{be_i} = 1, b \in \mathbb{Z}^+$ so,

$$e = e_1 \dots e_r$$

$$n^e = (a_1 \dots a_r)^e = 1$$

   for all unique e_i because for any $\mid a_i \mid = \mid a_j \mid = e_i, (a_i a_j)^{e_i} = a_i^{e_i} a_j^{e_i} = 1$. Essentially, e is the lcm of $e_1, \dots, e_r$.

   Also, given that $a_1 \dots a_r$ are not necessarily rank independent there might exist, for some a_i or combination of a_is, an inverse in $a_1 \dots a_r$. Such that for some $a_i, a_j \in n, a_i a_j = 1$ (and their relative positions don't matter because the group is abelian).

4. From above we can see that if all $a_i \in G$ are pairwise commuting, rank independent elements of finite order then:

$$e = lcm(e_1, \dots, e_r)$$
$$\mid a_1 \dots a_r \mid = lcm(\mid a_1 \mid \dots \mid a_r \mid).$$

5. Let $\sigma = m_1 m_2 \dots m_n$, where m_i is a cycle, and n is the total number of cycles, be the permutation of disjoint cycles in S_n. Also, by definition if the cycles are disjoint then they contain no common elements, which means that they don't interact with each other. Thus there are no possible inverse pairs $\in \sigma$. If $\sigma^x = 1$ then $(m_i)^x = 1, \forall i$, so $\mid m_i \mid\mid x$.
   So, the cycles are rank independent.
   Disjoint cycles are commutative, using subpart (4) we can say that because σ is rank indepedent and commutative, then $x = lcm(\mid m_i \mid), \forall i$, and m_i. The order of each cycle is equal to it's length. So $x = lcm$(lengths of the disjoint cycles).

Problem 2. $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$
Use the generators and relations above to show that every element of D_{2n} which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order 2.

Solution.
Elements in D_{2n} have the following orders:

1. Given, $\mid r \mid= n$.

2. Given, $\mid s \mid= 2$.

3. All other elements are multiples of rs, let n be the order of rs, and let n be even:

$$\begin{aligned} e &= (rs)^n \\ &= \underbrace{(rs)(rs)\dots(rs)}_{n-times} \\ &= \underbrace{(sr^{-1})(rs)(sr^{-1})(rs)\dots(rs)}_{n-times} \qquad \text{(replacing every alternate elements with } sr^{-1}\text{)} \\ &= \underbrace{s(r^{-1}r)(ss)(r^{-1}r)s\dots rs)}_{n-times} \\ &= ses = ss = s^2 \end{aligned}$$

$\implies \mid rs \mid\mid n$
The smallest n possible is 2, and we know that $n \neq 1$ because if $x^1 = e \implies x = e$, and $rs \neq e$. Thus, $\mid rs \mid= 2$. Hence, all elements of D_{2n} that are not powers of r have order 2.

For $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$ to be generated by elements s, sr we should be able to obtain the relations in the presentation from the new generators.
So,

1. $r = s(sr) \implies r^n = s^n(sr)^n = 1$

2. $s^2 = s \cdot s = 1$

3. $s(s^n(sr)^n) = s(s^{2n}r^n) = sr^n \implies s(s^{-1}(sr)^{-1}) = s(er^{-1}) = sr^{-1}$
   Then the relation, $rs = sr^{-1}$ can be expressed as:

$$s \cdot sr \cdot s = s(s^{-1}(sr)^{-1})$$

$$ers = s(s^{-1}s^{-1}r^{-1}) = s(s^{2\cdot -1}r^{-1}) = s(er^{-1})$$

$$rs = sr^{-1}$$

Hence, $D_{2n} = \langle s, sr \mid r^n = s^2 = 1, rs - sr^{-1} \rangle$.

Problem 3. Show that $\langle a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle$ gives a presentation D_{2n} in terms of the two generators $a = s$ and $b = sr$ of order 2 computed in the question above. [Show that the relations for r and s follow from the relations for a and b and, conversely, the relations for a and b follow from those for r and s.]

Solution.

1. To show that $D_{2n} = \langle s, sr \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$ gives $\langle a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle$ if $a = s, b = sr$:

   (a) $s^2 = 1 \implies a^2 = 1$, directly from presentations.

   (b) Every element of D_{2n} that is not a power of r has order 2 (from question 2) then,

   $$(sr)^2 = 1 \implies b^2 = 1$$

   (c) $s \cdot sr = r$ and $r^n = 1$
   $(s \cdot sr)^n = s^{2n} r^n = e \cdot r^n = 1.$
   $\implies (ab)^n = 1$

   Hence relations for a, b follow from relations for s, sr.

2. To show that $\langle a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle$ gives $D_{2n} = \langle s, sr \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$ if $a = s, b = sr$:

   (a) $a^2 = 1 \implies s^2 = 1$, directly from presentations.

   (b) $(ab)^n = 1 \implies (s \cdot sr)^n = (s^2 r)^n = (r)^n = 1.$

   (c) $aba = s \cdot sr \cdot s = s^2 rs = rs$, and
   $a(ab)^{-1} = aa^{-1}b^{-1} = s \cdot s^{-1} \cdot (sr)^{-1} = sr^{-1}$
   Thus, $aba = a(ab)^{-1} \implies rs = sr^{-1}$

   Hence relations for s, sr follow from relations for a, b.

Problem 4. Prove that if σ is the m-cycle $(a_1 a_2 \ldots a_m)$, then for all $i \in \{1, 2, \ldots, m\}$, $\sigma^i(a_k) = a_{k+i}$, where $k+i$ is replaced by its least residue mod m when $k+i > m$. Deduce that $\mid \sigma \mid = m$.

Solution.

In a m-cycle, $\sigma(a_k) = a_{k+1}$ with the exception that $\sigma(a_m) = a_1$. To prove $\sigma^i(a_k) = a_{k+i}$ through induction, let's consider:
$i = 1$

$$\sigma^1(a_k) = a_{k+1}$$

This is true by definition. If $k = m$,

$$\sigma^1(a_m) = a_{m+1}$$

But by definition of m-cycle, $\sigma(a_m) = a_1$, so

$$\sigma^1(a_m) = a_{m+1} = a_1$$

which is the least positive residue mod m for m + 1.
Inductive Case: Assuming $\sigma^i(a_k) = a_{k+i \text{ (least positive residue mod m)}}$ holds for i,

$$\sigma^{i+1}(a_k) = \sigma(\sigma^i(a_k))$$
$$\sigma^{i+1}(a_k) = \sigma(a_{k+i})$$
$$\sigma^{i+1}(a_k) = a_{k+i+1}$$

It also holds for $i+1$, and $k+i$ is replaced by it's least positive residue mod m.
The identity for σ would be a cycle such that no permutation occurs: $\sigma^x(a_k) = a_k$. But we know that $\sigma^x(a_k) = a_{k+x}$, so the lease positive residue mod m for x should be m, i.e., $x \in \{m, 2m, \ldots\}$. But order by definition is the least positive integer that gives the identity element upon applying the group action that number of times. So $x = m \implies \mid \sigma \mid = m$.

Problem 5. Let σ be the m-cycle $(12\ldots m)$. Show that σ^i is also an m-cycle if and only if i is relatively prime to m.

Solution.

Showing that $(i, m) \neq 1 \implies$ not m-cycle.
From the question above we know that the permutations would look like:

$$1 \to i+1,\ i+1 \to 2i+1,\ 2i+1 \to 3i+1, \ldots$$

Then suppose there exists a k such that $ki + 1 \to 2$

$$\begin{aligned} ki + 1 &\equiv 2 \text{ (mod m)} \\ ki &\equiv 1 \text{ (mod m)} \end{aligned}$$

But we know that it is not possible for numbers that are not relatively prime (from HW0, Problem 4). Hence, for no will $\sigma^i(a_1) = a_2$ or $\sigma^i(a_k)$ will never equal a_{k+1}. So there will at least be 2-disjoint cycles, and σ^i is not an m-cycle.

If $(i, m) \neq 1 \implies$ not m-cycle then by contrapositive m-cycle $\implies$ $(i, m) = 1$.

Showing that $(i, m) = 1 \implies$ m-cycle.

We know from HW0, Problem 5 that $ki \equiv 1$ (mod m) exists, so for some k, $\sigma^i(a_1) = a_2$ or $\sigma^i(a_k)$ will equal a_{k+1}, (mod m) $\forall k \in \{1, 2, \ldots, m\}$, hence the cycle will be m elements long.

Problem 6. Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.

Solution.
Showing that an element has order 2 in $S_n \implies$ that the cycle decomposition is a product of commuting 2-cycles.

Let $\sigma \in S_n$. σ can be expressed as a product of disjoint commuting cycles such that:

$$\sigma = \sigma_1 \sigma_2 \ldots \sigma_m$$

If $\mid \sigma \mid = 2$,

$$\sigma^2 = (\sigma_1 \sigma_2 \ldots \sigma_m)^2 = e$$
$$\sigma^2 = \sigma_1^2 \sigma_2^2 \ldots \sigma_m^2 = e$$

$\implies \sigma_i^2 = e \implies \mid \sigma_i \mid = 2$ And we know from Problem 4 that for an m-cycle the order of σ is m, thus the length of σ_i 2.

Showing that the product of commuting 2-cycles $\implies$ an element has order 2 in S_n Let n be the product of the commuting 2-cycles, such that:

$$n = n_1 n_2 \ldots n_m$$

Again from Problem 4, we know that for an m-cycle the order of an n-cycle is n. Then for the 2-cycles in n, $\mid n_i \mid = 2$, $\forall 1 \leq i \leq m$. Also because the cycles commute, $e = n_1^2 n_2^2 \ldots n_m^2$ can be written as $e = (n_1 n_2 \ldots n_m)^2 = n^2$. Thus, the product of commuting 2-cycles is an element of order 2 in S_n.

Problem 7. Show that if n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Solution.
For $\mathbb{Z}/n\mathbb{Z}$ to be a field, $(\mathbb{Z}/n\mathbb{Z}, +)$ should be an abelian group and $((\mathbb{Z}/n\mathbb{Z} - \{0\}), \cdot)$ should also be an abelian group. If $((\mathbb{Z}/n\mathbb{Z} - \{0\}), \cdot)$ is an abelian group it must contain the identity element e and $c^{-1}\, \forall c : cc^{-1} = e.$, and follow the axioms of associativity and commutativity.

1. In $((\mathbb{Z}/n\mathbb{Z} - \{0\}), \cdot)$ $e = 1$ because $\forall c \in \mathbb{Z}/n\mathbb{Z}^\times$ $c \cdot 1 = c$.

2. For c to have an inverse in the group, there must exist a a such that $a \cdot c = 1$ (mod n). Again from HW0 Problems 4 & 5, we know that $a \cdot c \equiv 1$ (mod n) is only possible if $1 \leq a \leq n$ is co-prime with n. But if $\forall a < n : (a, n) = 1$ then n is prime.

Problem 8. Let $H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in F \right\}$—called the Heisenberg group over F. Let $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$ be elements of $H(F)$.

1. Compute the matrix product XY and deduce that the $H(F)$ is closed under matrix multiplication. Exhibit explicit matrices such that $XY \neq YX$ (so that $H(F)$ is always non-abelian.
2. Find an explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverses.
3. Prove the associative law of $H(F)$ and deduce that $H(F)$ is a group of order $\mid F \mid^3$. (Do not assume that matrix multiplication is associative).
4. Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.
5. Prove that every nonidentity element of the group $H(\mathbb{R})$ has infinite order.

Solution.

1.

$$XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$$

$$YX = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & e+dc+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$$

$$af \neq dc \implies XY \neq YX$$

Thus the group is not abelian.

The results of both XY and YX give us matrices expressed using sums of $a, b, c, d, e, f \in F$ (from definition). Because the elements are in field F, by additive closure of field F the sum of the elements should also be in F, then the resulting matrices belong to $H(F)$. Thus, the $H(F)$ is closed under matrix multiplication.

2. $I_n = XX^{-1}$, let $X^{-1} = Y$ then:

$$XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$$

but $I_n = XY$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$$

(a) $d + a = 0 \implies d = -a$

(b) $f + c = 0 \implies f = -c$

(c) $e + af + b = 0 \implies e = -a(-c) - b = ac - b$

$$Y = X^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

$\implies$ for any $X, \exists X^{-1} \in H(F) \implies H(F)$ is closed under inverses.

3. To see if $H(F)$ is associative, consider three matrices

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}, Z = \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}$$

then

$$(XY)Z = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a+g & h+i(d+a)+e+af+b \\ 0 & 1 & f+c+i \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$X(YZ) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & g+d & h+di+e \\ 0 & 1 & i+f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+g+d & h+di+e+a(i+f)+b \\ 0 & 1 & c+f+i \\ 0 & 0 & 1 \end{pmatrix}$$

By associativity of F, and commutativeness of the multiplicative group operation:

(a) d + a + g = a + g + d

(b) f + c + i = c + f + i

(c) h + id + ia + e + af = h + di + e + ai + af + b

$\implies (XY)Z = X(YZ) \implies H(F)$ is associative.

From subparts 1, 2, and 3, we know that $H(F)$ is associative, and is closed under matrix multiplication, and has inverses for all $X \in H(F)$. It's can also be trivially seen that $I_n \in H(F) : a, b, c = 0$. So $H(F)$ is a group.
The order of a group is its cardinality. For any $X \in H(F)$, X can have any combination of $a, b, c : a, b, c \in F$. If the order of the F is $\mid F \mid$ then a, b, c can each have $\mid F \mid$ possible values $(\mid F \mid \cdot \mid F \mid \cdot \mid F \mid)$. So the order of $\mid H(F) \mid = \mid F \mid^3$.

4. Let $X \in H(\mathbb{Z}/2\mathbb{Z}) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$. And we know that $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$. Then,

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a & b+ac+b \\ 0 & 1 & c+c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod 2$$

If $a = 0$ or $c = 0$, $\mid X \mid = 2$. Else,

$$\begin{pmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$\mid X \mid \leq 4 \implies \mid X \mid \big| 4$ but we know that $1, 2 \neq \mid X \mid \implies \mid X \mid = 4$.
Also if $X = I_n \implies \mid X \mid = 1$ The order of elements in $H(\mathbb{Z}/2\mathbb{Z}) = \{1, 2, 4\}$.

5. Let $X \in H(\mathbb{R}) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$.

If $a = b = c = 0$ then $\mid X \mid = 1$. Else, let $\mid X \mid = n$, where n is some positive integer and y is any integer. Then by working out X^n for $n = 1, 2, 3, \ldots$ we can observe the following pattern:

$$X^n = \begin{pmatrix} 1 & na & nb + yac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}$$

For $\mid X \mid = n$, $na = nc = nb + yac = 0$. So we have the following cases:

(a) If $a \neq 0$ or $c \neq 0$ then na and nc respectively cannot be zero for any $x \in \mathbb{R} \implies \mid X \mid = \infty$

(b) If $a = 0$ and $c = 0$ then $na = nc = yac = 0$. Still, for the resulting matrix to be an identity matrix $nb = 0$. If $b \neq 0$ then nb cannot be zero for any $x \in \mathbb{R} \implies \mid X \mid = \infty$

So X only has finite order if $a = b = c = 0$ but if that is the case then X is an identity matrix. Thus, all nonidentity elements of the group $H(\mathbb{R})$ have infinite order.

Problem 9. If $\varphi : G \to H$ is an isomorphism, prove that $\mid \varphi(x) \mid = \mid x \mid$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if φ is only assumed to be a homomorphism?

Solution.
If $\varphi : G \to H$ is an isomorphism then we know that $ker(\varphi) = \{e_G\} \implies \varphi(e_G) = e_H$. Now, let $\mid g \mid = n, g \in G$. Then,

$$\varphi(g^n) = \varphi(e_G) = e_H$$

But by definition of a homomorphism we also know,

$$\varphi(g^n) = \varphi(\underbrace{g \dots g}_{n-times}) = \underbrace{\varphi(g) \dots \varphi(g)}_{n-times} = (\varphi(g))^n$$

$$\implies \varphi(g^n) = (\varphi(g))^n = e_H$$
$$\implies \mid \varphi(g) \mid \leq \mid g \mid$$

Also, because $\varphi : G \to H$ is an isomorphism we know that $\exists \varphi^{-1} : H \to G$ and let $\mid \varphi(g) \mid = m$. Then

$$\varphi^{-1}((\varphi(g))^m) = e_H = g^m$$
$$\implies m \geq \mid g \mid$$

Now we have, $m \geq n$ and $n \geq m \implies m = n, \forall g \in G$.

Isomorphic groups are bijective, so if G has x elements of order n, and all elements of G that have order n are mapped to elements of H that have order n, then G and H have x elements of of order n.

The result is not necessarily true if φ is only assumed to be an homomorphism because φ doesn't have an inverse, so we only know that $m \leq n$.

> **Problem 10**. Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.

Solution.
We know from Q9 that if $\varphi : G \to H$ is an isomorphism then $|\varphi(g)| = |g|$. Let $G = \mathbb{R} - \{0\}$ and $H = \mathbb{C} - \{0\}$. We know that for $i \in \mathbb{C}, |i| = 4$. So if the groups are isomorphic, there must exist an element $x \in \mathbb{R}$ such that $|x| = 4$. But for $\mathbb{R}$:

1. $|x| = 1$ only for the identity element

2. $|x| = 2$ if $x = -1$.

3. $\forall x \in \mathbb{R}, x > 1$, and $n \in \mathbb{Z}^+, x^n = 1$.
   But $x^n = \underbrace{x \dots x}_{n-times}$ and we can see that if $x > 1 \implies x^n > 1 \implies x^n \neq 1$ So there $\nexists n : x^n = 1 \implies |x| = \infty$.

4. $\forall x \in \mathbb{R}, x < -1$, and $n \in \mathbb{Z}^+, x^n = 1$.
   But $x^n = \underbrace{x \dots x}_{n-times}$ and we can see that if $x < -1, x^n$ alternates between being $x^n > 1$ (for even powers) and $x^n < -1$(for odd powers). In both cases $x^n \neq 1$ So there $\nexists n : x^n = 1 \implies |x| = \infty$.

5. $\forall x \in \mathbb{R}, -1 < x < 1$, and $n \in \mathbb{Z}^+, x^n = 1$.
   But $0^n = 0$ always, and the absolute value of everything else raised to any positive integer n would be smaller than the original value.

   $$abs(x) > abs(x^n) \implies 1 - x^n > 1 - x$$

   So there $\nexists n : x^n = 1 \implies |x| = \infty$.

Hence $|x| = \{1, 2, \infty\}, x \in \mathbb{R}$. So there does not exist any element in $\mathbb{R}$ with order 4, and thus σ cannot be an isomorphism.

Problem 11. Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

Solution.
Suppose $\mathbb{Z}$ and $\mathbb{Q}$ are isomorphic, and $\mathbb{Z} = \langle 1 \rangle$, where $\mathbb{Z}$ can be generated by adding/subtracting 1 multiple times to itself. Then there must exist some p/q such that $\mathbb{Q} = \langle p/q \rangle$. But $\exists p/2q \in \mathbb{Q}$ that cannot be generated from p/q by adding/subtracting multiple times it from itself ($p/2q$ is not an integral multiple of p/q). Hence, $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

Problem 12. Prove that D_{24} and S_4 are not isomorphic.

Solution.
We know from Q9 that if $\varphi : G \to H$ is an isomorphism then $\mid \varphi(g) \mid = \mid g \mid$. But from the presentation of a dihedral group we know that that $r, s \in D_{24} : r^{12} = s^2 = e \implies \mid r \mid = 12$. However, the maximum length an m-cycle in S_4 can have is 4, thus the maximum order an element in S_n can have is 4. Thus, in $\varphi : D_{24} \to S_4$, $\exists g \in D_{24} : \mid \varphi(g) \mid \neq \mid g \mid \implies \varphi$ is not isomorphic.

Problem 13. Let $d \in \mathbb{Z}$ nonsquare. Prove that $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$ is a field under addition and multiplication of complex numbers. Hint: You can take for granted that $\sqrt{d}$ is irrational.

Solution.

We know that $\mathbb{Q}(\sqrt{d}) \in \mathbb{C}$. So $\mathbb{Q}(\sqrt{d})$ inherits associativity and commutativity from the field $\mathbb{C}$. Then we only need to show that $\mathbb{Q}(\sqrt{d})$ is closed under inverses, multiplication, and addition to prove that $\mathbb{Q}(\sqrt{d})$ is a field.

1. if $a, b = 0$
   $a + b\sqrt{d} = 0 + 0 = 0$
   $\implies 0 \in \mathbb{Q}(\sqrt{d})$

   if $a = 1, b = 0$
   $a + b\sqrt{d} = 1 + 0 = 1$
   $\implies 1 \in \mathbb{Q}(\sqrt{d})$
   Hence, $\mathbb{Q}(\sqrt{d})$ is closed under inverses.

2. Let $x + y\sqrt{d}$ be the additive inverse of $a + b\sqrt{d}$ then,

$$\begin{aligned} a + b\sqrt{d} + x + y\sqrt{d} &= 0 \\ a + x + b\sqrt{d} + y\sqrt{d} &= 0 \\ (a + x)1 + (b + y)\sqrt{d} &= 0 \\ \implies a &= -x \\ \implies b &= -y \end{aligned}$$

   $a, b \in \mathbb{Q}$, so the additive inverse of $a + b\sqrt{d}$ is $(-a - b\sqrt{d})$. Thus, $(\mathbb{Q}\sqrt{d})$ is closed under addition.

3. Let x be the multiplicative inverse of $a + b\sqrt{d}$ then,

$$\begin{aligned}
(a+b\sqrt{d})(x+y\sqrt{d}) &= 1 \\
x+y\sqrt{d} &= 1/(a+b\sqrt{d}) \\
x+y\sqrt{d} &= \frac{1}{a+b\sqrt{d}} \cdot \frac{a-x+y\sqrt{d}\sqrt{d}}{a-b\sqrt{d}} \\
x+y\sqrt{d} &= \frac{a-b\sqrt{d}}{a^2-b^2d} \\
x+y\sqrt{d} &= \frac{a}{a^2-b^2d} + \frac{-b}{a^2-b^2d} \cdot \sqrt{d} \\
\implies x = \frac{a}{a^2-b^2d}, &\qquad y = \frac{-b}{a^2-b^2d}
\end{aligned}$$

We can see that $x, y \in \mathbb{Q}$ because $a, b \in \mathbb{Q}$. So,

$$(a+b\sqrt{d})^{-1} = \frac{a}{a^2-b^2d} + \frac{-b}{a^2-b^2d} \cdot \sqrt{d} \in \mathbb{Q}(\sqrt{d})$$

Thus, $\mathbb{Q}(\sqrt{d})$ is closed under multiplication.

Hence, $\mathbb{Q}(\sqrt{d})$ is a field under addition and multiplication of complex numbers.

Problem 14. Remind yourself (or learn about) the field of complex numbers $\mathbb{C} = \{z = x+iy : x+y \in \mathbb{R}, i^2 = -1\}$. Prove that the complex conjugation $z = x+iy \mapsto \bar{z} = x-iy$ is a homomorphism of the additive group $\mathbb{C} \mapsto \mathbb{C}$ and the multiplicative group $\mathbb{C}^\times \mapsto \mathbb{C}^\times$. Prove that the absolute value $z \mapsto \mid z \mid = \sqrt{z\bar{z}}$ is a homomorphism of the multiplicative groups $\mathbb{C}^\times \mapsto \mathbb{R}^\times$. Let $U = \{z \in \mathbb{C} : \mid z \mid = 1\}$ be the unit circle. Prove that the map $\mathbb{R} \mapsto U$ defined by $\theta \mapsto e^{i\theta}$ is a group homomorphism.

Solution.

1. To show that $\sigma : \mathbb{C} \to \mathbb{C}$ are holomorphic where σ is complex conjugation we need to show that $\varphi(ab) = \varphi(a)\varphi(b)$ where $a, b \in \mathbb{C}$. Let $a = x + yi, b = p + qi$.

$$\begin{aligned}
\varphi(ab) &= \varphi(a)\varphi(b) \\
\varphi(x + yi + p + qi) &= \varphi(x + yi) + \varphi(p + qi) \\
\varphi((x + p) + (y + q)i) &= (x - yi) + (p - qi) \\
(x + p) - (y + q)i &= (x + p) - (y + q)i
\end{aligned}$$

   Thus, σ is a homomorphism from $\mathbb{C} \to \mathbb{C}$.

2. To show that $\sigma : \mathbb{C}^\times \to \mathbb{C}^\times$ are homomorphic where σ is the absolute value of z we need to show that $\varphi(ab) = \varphi(a)\varphi(b)$ where $a, b \in \mathbb{C}$. Let $a = x + yi, b = p + qi$.

$$\begin{aligned}
\varphi(ab) &= \varphi(a)\varphi(b) \\
\varphi((x + yi)(p + qi)) &= \varphi(x + yi) \cdot \varphi(p + qi) \\
\varphi(xp + pyi + xqi - yq) &= (x - yi) \cdot (p - qi) \\
\varphi((xp - yq) + (py + xq)i) &= (x - yi) \cdot (p - qi) \\
\varphi((xp - yq) + (py + xq)i) &= xp - pyi - xqi - yq \\
xp - yq - pyi - xqi &= xp - pyi - xqi - yq
\end{aligned}$$

   Thus, σ is a homomorphism from $\mathbb{C}^\times \to \mathbb{C}^\times$.

3. To show that $\sigma : \mathbb{C}^\times \to \mathbb{R}^\times$ are holomorphic where σ is the absolute value of z we need to show that $\varphi(ab) = \varphi(a)\varphi(b)$ where $a, b \in \mathbb{C}$. Let $a = x + yi, b = p + qi$.

$$\begin{aligned}
\varphi(ab) &= \varphi(a)\varphi(b) \\
\varphi((x + yi)(p + qi)) &= \varphi(x + yi) \cdot \varphi(p + qi) \\
\varphi(xp + pyi + xqi - yq) &= (x^2 + y^2) \cdot (p^2 + q^2) \\
\varphi((xp - yq) + (py + xq)i) &= (x^2 + y^2) \cdot (p^2 + q^2) \\
(xp - yq)^2 + (py + xq)^2 &= (x^2 + y^2) \cdot (p^2 + q^2) \\
x^2p^2 + y^2q^2 - 2xypq + p^2y^2 + x^2q^2 + 2xypq &= x^2p^2 + y^2p^2 + x^2q^2 + y^2q^2 \\
x^2p^2 + y^2q^2 + p^2y^2 + x^2q^2 &= x^2p^2 + y^2p^2 + x^2q^2 + y^2q^2
\end{aligned}$$

Thus, σ is a homomorphism from $\mathbb{C}^\times \to \mathbb{R}^\times$.

4. To show that $\sigma : \mathbb{R} \to U$ are homomorphic where $\sigma(\theta) = e^{i\theta}$ we need to show that $\varphi(ab) = \varphi(a)\varphi(b)$ where $a, b \in \mathbb{R}$.

$$\begin{aligned} \varphi(ab) &= \varphi(a)\varphi(b) \\ \varphi(a+b) &= e^{ia}e^{ib} \\ e^{i(a+b)} &= e^{ia+ib} \\ e^{ia+ib} &= e^{ia+ib} \end{aligned}$$

Thus, σ is a homomorphism from $\mathbb{R} \to U$.