MATH 315 Assignment 1

Instructor: Dr. Thomas Bitoun
Name: Yifeng Pan
UCID: 30063828

Winter 2020

1 Let $(G, *), (G_1, *_1), (G_2, *_2)$ be groups. Show the following.

1.1 $(G_1 \times G_2, \star)$ with $(g_1, g_2) \star (h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2)$ is a group.

Let $(a_1, a_2), (b_1, b_2), (c_1, c_2), \in G_1 \times G_2$.

$$\begin{aligned}((a_1, a_2) \star (b_1, b_2)) \star (c_1, c_2) &= (a_1 *_1 b_1, a_2 *_2 b_2) \star (c_1, c_2) \\ &= ((a_1 *_1 b_1) *_1 c_1, (a_2 *_2 b_2) *_2 c_2) \\ &= (a_1 *_1 (b_1 *_1 c_1), a_2 *_2 (b_2 *_2 c_2)) \\ &= (a_1, a_2) \star (b_1 *_1 c_1, b_2 *_2 c_2) \\ &= (a_1, a_2) \star ((b_1, b_2) \star (c_1, c_2)).\end{aligned}$$

Therefore $\star$ is associative.

Let e_1 be the identity of $(G_1, *_1)$, and e_2 be the identity of $(G_2, *_2)$.

$$\begin{aligned}(e_1, e_2) \star (a_1, a_2) &= (e_1 *_1 a_1, e_2 *_2 a_2) \\ = (a_1, a_2) &= (a_1 *_1 e_1, a_2 *_2 e_2) \\ &= (a_1, a_2) \star (e_1, e_2).\end{aligned}$$

Therefore $(e_1, e_2) \in G_1 \times G_2$ is an identity.

Let a_1^{-1} be the inverse of a_1 for the $(G_1, *_1)$ group, and a_2^{-1} be the inverse of a_2 for the $(G_2, *_2)$ group.

$$\begin{aligned}(a_1, a_2) \star (a_1^{-1}, a_2^{-1}) &= (a_1 *_1 a_1^{-1}, a_2 *_2 a_2^{-1}) \\ = (e_1, e_2) &= (a_1^{-1} *_1 a_1, a_2^{-1} *_2 a_2) \\ &= (a_1^{-1}, a_2^{-1}) \star (a_1, a_2).\end{aligned}$$

Therefore $\forall (a_1, a_2) \in G_1 \times G_2, \exists$ an inverse (a_1^{-1}, a_2^{-1}).

Now, $(a_1, a_2) \star (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2)$, where $a_1 *_1 b_1 \in G_1, a_2 *_2 b_2 \in G_2$;
Therefore $\star$ is a closed binary operation on $G_1 \times G_2$.

Therefore $(G_1 \times G_2, \star)$ is a group.

1.2 The center of $(G_1 \times G_2, \star)$ is $Z(G_1) \times Z(G_2)$, where $Z(G_i)$ is the center of G_i, for $i \in \{1, 2\}$.

Suppose $(z_1, z_2) \in Z(G_1 \times G_2)$. So $\forall (a_1, a_2) \in G_1 \times G_2$,

$$\begin{aligned}&(z_1, z_2) \star (a_1, a_2) = (a_1, a_2) \star (z_1, z_2) \\ \Rightarrow\ &(z_1 *_1 a_1, z_2 *_2 a_2) = (a_1 *_1 z_1, a_2 *_2 z_2) \\ \Rightarrow\ &z_1 *_1 a_1 = a_1 *_1 z_1 \text{ and } z_2 *_2 a_2 = a_2 *_2 z_2 \\ \Rightarrow\ &z_1 \in Z(G_1) \text{ and } z_2 \in Z(G_2) \\ \Rightarrow\ &(z_1, z_2) \in Z(G_1) \times Z(G_2)\end{aligned}$$

□

Suppose $z_1 \in Z(G_1)$ and $z_2 \in Z(G_2)$, where $(z_1, z_2) \in Z(G_1) \times Z(G_2)$. So $\forall a_1 \in G_1$ and $\forall a_2 \in G_2$.

$$\begin{aligned}&z_1 *_1 a_1 = a_1 *_1 z_1 \text{ and } z_2 *_2 a_2 = a_2 *_2 z_2 \\ \Rightarrow\ &(z_1 *_1 a_1, z_2 *_2 a_2) = (a_1 *_1 z_1, a_2 *_2 z_2) \\ \Rightarrow\ &(z_1, z_2) \star (a_1, a_2) = (a_1, a_2) \star (z_1, z_2) \\ \Rightarrow\ &(z_1, z_2) \in Z(G_1 \times G_2)\end{aligned}$$

□

Therefore $Z(G_1 \times G_2) \subseteq Z(G_1) \times Z(G_2)$, and $Z(G_1) \times Z(G_2) \subseteq Z(G_1 \times G_2)$.

1.3 A non-empty subset S of G is a subgroup if and only if $\forall s_1, s_2 \in S, s_1 * s_2^{-1} \in S$.

Suppose S is a subgroup of G. Let $s_1, s_2 \in S$. Since S is a group, s_2 has an inverse s_2^{-1}. Since $*$ is closed on S, $s_1 * s_2^{-1} \in S$. □

Suppose $S \subseteq G$ is non-empty, and $\forall s_1, s_2 \in S, s_1 * s_2^{-1} \in S$.

Since $S \neq \varnothing$, let $s_1 = s_2 = s, e = s * s^{-1} \in S$. Therefore S contains the identity e.

Now, let $s_1 = e$. So $\forall s_2 \in S, e * s_2^{-1} = s_2^{-1} \in S$. Therefore every element in S is invertible.

$(S, *)$ inherits associativity from $(G, *)$.

Let $a, b \in S$. Since b has an inverse in S, let $s_1 = a, s_2 = b^{-1}$. So $a * b = s_1 * b^{-1^{-1}} = s_1 * s_2^{-1} \in S$. Therefore $*$ is closed on S.

Therefore S is a group. Since $S \subseteq G$, S is a subgroup of G. □

2 Let S_4 be the symmetric group of degree 4, i.e. $S_4 = S_{\{1,2,3,4\}}$.

2.1 Using the cycle notation, list all elements of order 2 of S_4.

$\{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\}$

2.2 Show that the subset $H = \{\sigma \in S_4 | \sigma(1) = 1\}$ is a subgroup.

Since $\sigma(1) = 1$ holds true for the identity, H contains the identity. H inherits associativity from S_4.

All elements of H has the form $\left[\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & & & \\ 0 & & \tau & \\ 0 & & & \end{array}\right]$ for some $\tau \in S_3$. when written as permutation matrices. Since the transpose of a permutation matrix is its inverse, every element of H has an inverse. Since the transpose has the same form, the inverse is in H.

The block matrix form of H retains its form after matrix multiplication with any two elements of H. Therefore H is closed.

Therefore H is a group. Since $H \subseteq S_4$, it is a subgroup of S_4.

2.3 Assuming (2.2), show that $gHg^{-1} = \{g \circ h \circ g^{-1} | h \in H\}$ is a subgroup of S_4, for all $g \in S_4$.

Let e be the identity, which is $\in H$. So $e = gg^{-1} = (ge)g^{-1} = geg^{-1} \in gHg^{-1}$. gHg^{-1} inherits associativity.

Let $gag^{-1} \in gHg^{-1}$, where $a \in H$. We know $\exists a^{-1} \in H$, so $ga^{-1}g^{-1} \in gHg^{-1}$. Now,

$$\begin{aligned} gag^{-1}ga^{-1}g^{-1} &= gaea^{-1}g^{-1} \\ &= gaa^{-1}g^{-1} \\ &= geg^{-1} \\ &= gg^{-1} \\ = e &= ga^{-1}ag^{-1} \\ &= ga^{-1}eag^{-1} \\ = ga^{-1}g^{-1}gag^{-1} & \end{aligned}$$

Therefore every element of gHg^{-1} has an inverse in gHg^{-1}.

Let $gag^{-1}, gbg^{-1} \in gHg^{-1}$, where $a, b \in H$. So $gag^{-1}gbg^{-1} = gabg^{-1}$. Since $ab \in H$, $gabg^{-1} \in gHg^{-1}$. Therefore gHg^{-1} is closed.

Therefore gHg^{-1} is a group. Since $gHg^{-1} \subseteq S_4$, it is a subgroup.

3 Let n be the natural number $\in \{1, 2, 3, \ldots\}$. An nth root of unity is a complex number z such that $z^n = 1$.

3.1 Prove that the nth roots of unity form a cyclic subgroup H_n of $\mathbb{C}^\times$ of order n. (Recall that $\mathbb{C}^\times = \mathbb{C} - \{0\}$, with the complex multiplication.)

Let $n \in \{1, 2, 3, \ldots\} = \mathbb{N}$. Let $Z_n = \{z | z \in \mathbb{C} \wedge z^n = 1\}$. Let the group H_n be Z_n under complex multiplication. Since there are n solution to $z \in \mathbb{C}, z^n = 1$, the order of H_n is n.

H_n inherits associativity from $\mathbb{C}^\times$.

H_n contains the identity 1, as $1^n = 1, \forall n \in \mathbb{N}$.

Let $a, b \in H_n$. Now, $(ab)^n = a^n b^n = 1 \times 1 = 1$. Therefore $ab \in H_n$, and H_n is closed.

Let $a \in H_n$. a^{n-1} is the inverse, as $aa^{n-1} = a^{n-1}a = a^n = 1$. Now, $\left(a^{n-1}\right)^n = (a^n)^{n-1} = 1^{n-1} = 1$. Therefore every element of H_n has an inverse in H_n.

Therefore H_n is a subgroup of $\mathbb{C}^\times, \forall n \in \mathbb{N}$. □

Now, since all elements of H_n are on the unit circle on the complex plane centered at $(0, 0)$, all elements of H_n can be written in the form $\exp(ix)$. (Assume reduced form where $x = x \mod 2\pi$.)

Let $n \geq 2$. ($n = 1$ is the trivial case.)

Let $m = \exp(ix) | (x \neq 0 \wedge \exp(ix) \in H_n) \wedge \forall \exp(iy) \in H_n, x \leq y$. (If m is not unique, then H_n is not a set. Therefore m is unique.)

Let Y_n be the cyclic subgroup generated from $m \in \mathbb{C}^\times$.

Let $y \in Y_n$. So $y = m^z$ for some $z \in \mathbb{Z}$. Now, since $m \in H_n$, $y^n = m^{z^n} = m^{n^z} = 1^z = 1$. Therefore $y \in H_n$.

Now we find the order of $Y_n = \left|\{m^0, m^1, m^{-1}, m^2, m^{-2}, \ldots\}\right|$. Let $z \in Z$. Let $z = qn + r | q \in \mathbb{Z}, r \in [0, n) \cap \mathbb{Z}$. (The solution to q, r is unique.)

Now $m^z = m^{qn} m^r = 1^q m^r = m^r$. Therefore $Y_n = \{m^0, m^1, m^2, \ldots, m^{n-1}\} = \{m^r\}$.

Now we prove $m^0, \ldots, m^{n-1}$ are distinct. Due to the cancellation law derived from the inverse property of groups, it is sufficient to prove that $m^0 \neq m^k, \forall 0 < k < n, k \in \mathbb{N}$.

By contradiction: Suppose $\exists k \in (0, n) \cap \mathbb{N}$, where $m^k = 1$. Since $\exp(i\frac{xk}{n})^n = \exp(\frac{ixkn}{n}) = \exp(ixk) = m^k = 1$, therefore $\exp(i\frac{xk}{n}) \in H_n$. Since $\frac{k}{n} < 1$, $x > \frac{xk}{n}$. This is a contradiction from the construction of x. Therefore there exists no such m^k.

Therefore $m^0, \ldots, m^{n-1}$ are distinct, and $|Y_n| = n$.

Therefore Y_n and H_n have the same order, and since $Y_n \subseteq H_n, Y_n = H_n$.

Therefore H_n is a cyclic subgroup of $\mathbb{C}^\times$. □

3.2 Determine the product of all the nth roots of unity.

-1 if n is even, 1 if n is odd.

Let $a \in H_n$. If a and a^{-1} are distinct elements, then they cancel out to the identity. The only cases where $a = a^{-1}$ is $a \in \{1, -1\}$. We can ignore the identity. And $-1 \in H_n \leftrightarrow n$ is even.

3.3 Show that if the only subgroups of H_n are the trivial subgroups $\{1\}$ and H_n, then $n = 1$ or n is a prime number.

We prove the contrapositive. Suppose $n \neq 1$ and n is not prime. So $\exists a, b \in \mathbb{N}$ such that $ab = n \geq 4, a > 1, b > 1$.

(The following two paragraphs are a repeat of (3.1):)

Now, since all elements of H_n are on the unit circle on the complex plane centered at $(0, 0)$, all elements of H_n can be written in the form $\exp(ix)$. (Assume reduced form where $x = x \mod 2\pi$.)

Let $m = \exp(ix) | (x \neq 0 \wedge \exp(ix) \in H_n) \wedge \forall \exp(iy) \in H_n, x \leq y$. (If m is not unique, then H_n is not a set. Therefore m is unique.)

Let Y_n be the cyclic subgroup generated from $m^a \in \mathbb{C}^\times$.

We've proven in (3.1) that $m^a \neq m^0 = 1$. Therefore $Y_n \neq \{1\}$.

Now we prove $m \notin Y_n$ by contradiction (Note: Y_n is generated from m^a.): Suppose $m \in Y_n$. So $\exists z \in \mathbb{Z}, m^1 = m^{az}$. Therefore $az \equiv 1 \pmod n$, or $az = kn + 1$ for some $k \in Z$. So $az = kab + 1$ and $a(z - kb) = 1$. Therefore $a \in \{-1, 1\}$, which is a contradiction as $a > 1$ by construct. Therefore $m \notin Y_n$. Since $m \in H_n$, $Y_n \neq H_n$.

Therefore if $n \neq 1$ and n is a non-prime, then we can construct Y_n to be a non-trivial subgroup of H_n.

4 Recall the group $GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0 \right\}$, with matrix multiplication.

4.1 Show that the subset $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in \mathbb{Z} \text{ and } ad - bc \neq 0 \right\}$ is not a subgroup.

Let H be the above subset. Let $a = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, a \in H$. So $a^{-1} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}, a^{-1} \notin H$. Therefore H is not a group, and therefore not a subgroup.

4.2 Show that the subset $SL_2(\mathbb{Z})$ of invertible matrices with integer coefficients and determinant 1, i.e.

$$\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\}$$

is a subgroup.

We know $I_2 \in SL_2(\mathbb{Z}) \subseteq GL_2(\mathbb{R})$ and matrix multiplication is associative.

Let $A, B \in SL_2(\mathbb{Z})$. Now, $\det(AB) = \det(A)\det(B) = 1 \times 1 = 1$. Since AB is an integer matrix, $AB \in SL_2(\mathbb{Z})$. Therefore $SL_2(\mathbb{Z})$ is closed.

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$. We know $A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$, which is an integer matrix with $\det(A^{-1}) = da - (-c)(-b) = ad - bc = 1$. Therefore A^{-1} exists and is in $SL_2(\mathbb{Z})$.

Therefore $SL_2(\mathbb{Z})$ is a group and a subgroup of $GL_2(\mathbb{R})$.

4.3 Let $SL_2(\mathbb{Z}/3\mathbb{Z})$ be $SL_2(\mathbb{Z})$ with the matrix entries interpreted modulo 3. It is a group. What is the order of $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in SL_2(\mathbb{Z}/3\mathbb{Z})$?

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \neq I_2$ and $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \neq I_2$ and $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$ under $SL_2(\mathbb{Z}/3\mathbb{Z})$.

Therefore the peroid of $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in SL_2(Z/3\mathbb{Z})$ is 3, as 3 is the smallest positive integer with this property. □

Citations

"Algebra" by Michael Artin (ISBN 13: 9780132413770).

Proofread by Devin Kwok (UCID: 10016484).