Math 103A Homework 4

James Holden

February 1, 2019, Winter 2019

Question 1. *Let a, b be two positive integers. Define $H_{ab} = \{am + bn | m, n \in \mathbb{Z}\}$.*

(a) Show that H is a subgroup of $\mathbb{Z}$ with usual addition.

Proof. We want show $H \leq (\mathbb{Z}, +)$.

We need to check subgroup properties.

(i) *Identity*

Identity of $(\mathbb{Z}, +)$ is 0. According to Theorem 5.14 on page 52, we must ensure that the identity of $(\mathbb{Z}, +)$ is also in H. It so happens that the identity in H is 0, and further, for a particular choice of a and b, there are many choices of m and n which will give $e = am + bn = 0$.

Let $h \in H$. For some h as detailed above, $h = am+bn$. To test identity, we would need $h+e = e+h = h$ and substituting in our form for h we get $am + bn + 0 = 0 + am + bn = am + bn = h$. Thus identity exists for $h \in H$ and it is 0.

(ii) Inverse

Let $h = am + bn \in H$. An inverse of h exists such that $h + h^{-1} = e$.

Since $h = am + bn$, we examine $h^{-1} = -(am + bn) = -am - bn$ as the candidte for th additive inverse for h. Indeed, $h + h^{-1} = am + bn - am - bn = 0$.

Thus, for $h \in H$, h^{-1} exists.

(iii) Closure

Let $h_1, h_2 \in H$. $h_1 = am_1 + bn_1$ and $h_2 = am_2 + bn_2$. Therefore, $h_1 + h_2 = a(m_1 + m_2) + b(n_1 + n_2) \in H$ and $m_1 + m_2, n_1 + n_2 \in \mathbb{Z}$.

Thus, H is closed under the same binary operation as $\mathbb{Z}$.

(iv) Associativity

We know H inherits associativity from $\mathbb{Z}$ from the proof of Theorem 5.14 on page 52 of Fraleigh.

Thus $H \leq \mathbb{Z}$.

□

(b) Show that $H = d\mathbb{Z}$ where $d = g.c.d(a, b)$. (Hint the hard direction is a theorem in Math 109). Hint is: Given $a, b \in \mathbb{N}$ such that $gcd(a, b) = d$, then $\exists m, n \in \mathbb{Z}$ such that $d = am + bn$

Proof. We have shown that $H \leq \mathbb{Z}$. We now seek to show that H is generated by $< d >$ where d is the greatest common divisor of (a, b).

We can let $H = j\mathbb{Z} + k\mathbb{Z}$. We have $a, b \in \mathbb{Z}$ such that d is divisible by both a and b since this is a cyclic group. If we take a natural number r such that r is divisible by both a and b, then for any $j, k \in \mathbb{Z}$, $H = a\mathbb{Z} + b\mathbb{Z} = rj\mathbb{Z} + rk\mathbb{Z} \in r\mathbb{Z}$.

$H = d\mathbb{Z} \in r\mathbb{Z}$ and r divisible by d, so $d = gcd(a, b)$.

□

Question 2. *(Exercises 4: Question 29 (Page 48)) Show that if G is finite group with identity e and with an even number of elements, then there is $a \neq e$ in G such that $a * a = e$.*

Proof. For an example of a group like this, consider $C_4 = (\{e, r, r^2, r^3\}, *)$. In this example, we have $r^2 * r^2 = e$. There are elements a in C_4 for which $a * a = e$ does not hold, for example r and it's inverse r^3 because $r * r = r^2$ and $r^3 * r^3 = r^2$, and for some completeness we'll just point out that $r * r^3 = e$.

We want to show $a * a = e$ for some $a \in G$ and we'll do this by showing that if it is not true, that this leads to a contradiction.

(Note that $a * a = e$ implies $a^{-1} = a$.)

(I) Assuming the conclusion is not true, we say that for all $a \in G$ where $a \neq e$ that $a * a \neq e$. This would imply $a \neq a^{-1}$ for all $a \in G$.

By Theorem 4.17 of Fraleigh, page 42, the inverse of an element not the identity is unique, in other words there is only one of them, therefore let us try to pair every element with its unique inverse like so (a, a^{-1}). This pairing leaves the identity element paired with itself (e, e) but because we have an even number of elements, this leave one other non-identity element b paired with itself, (b, b), meaning $b * b = e$. Thus, we have shown $b \in G$ exists such that $b * b = e$.

Therefore we have contradicted our previous statement(I) because we have shown such a element of G exists. □

Question 3. *(Exercises 5: Question 11 (Page 55)) Determine whether the set of invertible $n \times n$ matrices with real number entries is a subgroup of $GL(n, \mathbb{R})$.*

$n \times n$ matrices with determinant -1.

Proof. Not a subgroup. Let A and B be $n \times n$ matrices and let $det(A) = -1$ and $det(B) = -1$. For any two $n \times n$ matrices A and B we have $det(AB) = det(A)det(B)$ but $det(A)det(B) = 1$ and therefore this set of matrices is not closed under matrix multiplication. □

Question 4. *(Exercises 5: Question 12 (Page 55)) Determine whether the given set of invertible $n \times n$ matrices with real number entries is a subgroup of $GL(n, \mathbb{R})$.*

$n \times n$ matrices with determinant -1 or 1.

Proof. We let H be the set of $n \times n$ matrices with determinant -1 or 1. We want to prove that $H \leq GL(n, \mathbb{R})$ or that H is not a subgroup of $GL(n, \mathbb{R})$.

H is a subgroup of $GL(n, \mathbb{R})$ if and only if:

(i) *Closure :* H is closed under the binary operation of $GL(n, \mathbb{R})$

Let $A, B \in H$. We see that $det(AB) = det(A)det(B) = 1$ or $det(AB) = det(A)det(B) = -1$ which are both determinants within the set of possible determinants. Thus H is closed under matrix multiplication

(ii) Identity: the identity element of $GL(n, \mathbb{R})$ is also in H

The identity element of $GL(n, \mathbb{R})$ is I_n, the $n \times n$ identity matrix. Let $h \in H$. We see $h * I_n = I_n * h = h$. Therefore, $I_n \in H$.

(iii) Inverse: for all $A \in H$ it is true that $A^{-1} \in H$. First note that matrix A is invertible because $det(A) \neq 0$. We should consider two cases.

Case 1: Let $A \in H$ and $det(A) = 1$. We have $1 = det(I_n) = det(A^{-1}A) = det(A^{-1}) * det(A) = det(A^{-1}) * 1$. So $det(A^{-1}) = 1$.

Case 2: Let $A \in H$ and $det(A) = -1$. We have $-1 = -det(I_n) = -det(A^{-1}A) = -det(A^{-1}) * det(A) = -det(A^{-1}) * -1$. So $det(A^{-1}) = -1$.

(iv) Associativity:

We know that matrix multiplication is associative and H inherits this property from $GL(n, \mathbb{R})$. Associativity is inherent in the group operation.

Thus $H \leq G$. □

Question 5. *(Exercises 5: Question 13 (Page 55)) Determine whether the given set of invertible $n \times n$ matrices with real number entries is a subgroup of $GL(n, \mathbb{R})$.*

The set of all $n \times n$ matrices A such that $A^T A = I_n$ ie. the orthogonal matrices.

Proof. We want to find out whether or not $H \leq GL(n, \mathbb{R})$.

H is a subgroup of $GL(n, \mathbb{R})$ if and only if:

(i) Closure: H is closed under the binary operation of $GL(n, \mathbb{R})$

Suppose $(A^T)A = I_n$ and $(B^T)B = I_n$. Then we have $(AB)^T AB = B^T(A^T A)B = B^T I_n B = B^T B = I_n$

Therefore the set of these matrices is closed under the $GL(n, \mathbb{R})$ multiplication.

(ii) Identity: the identity element of $GL(n, \mathbb{R})$ is also in H

Since $I_n^T = I_n$ and $I_n I_n = I_n$, the set contains the identity, which is I_n.

(iii) Inverses: for all $a \in H$ it is true that $a^{-1} \in H$

For each A in the set, the equation $(A^T)A = I_n$ shows that the inverse of A is A^T.

(iv) Associativity

We know that matrix multiplication is associative and H inherits this property from $GL(n, \mathbb{R})$. Associativity is inherent in the group operation.

□

Question 6. *(Exercises 5: Question 33 (Page 57)) Find the order of the cyclic subgroup generated by the indicated element.*

The subgroup of the multiplicative group G of invertible 4×4 matrices generated by

$$g = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Proof. Generating a group from g by applying g until we arrive at identity:

$$g^2 = g * g = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} * \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = e$$

Therefore $|< g >| = 2$. □

Question 7. *(Exercises 5: Question 41 (Page 58)) Let $\phi : G \to G'$ be an isomorphism of a group $< G, * >$ with a group $< G', *' >$. Write out a proof to convince a skeptic of the intuitively clear statement:*

If H is a subgroup of G, then $\phi[H] = \{\phi(h) | h \in H\}$ is a subgroup of G'. That is, an isomorphism carries subgroups into subgroups.

Proof. In order to prove that $\phi[H] \leq G'$ when $H \leq G$ and ϕ is an isomorphism.

(i) Closure:

For all $a, b \in H$ we have $\phi(a), \phi(b) \in \phi[H]$. We know $a * b \in H$ because $H \leq G$. Since ϕ is an isomorphic function, $\phi(a) *' \phi(b) = \phi(a * b) \in \phi[H]$ because $a * b \in H$ and the definition of $\phi[H]$ so $\phi[H]$ is closed under $*'$.

(ii) Identity:

We know $e' \in \phi[H]$ because $\phi[H] \leq G'$. Since ϕ is an isomorphism, $\phi(e) = e' \in \phi[H]$. Therefore, the isomorphism carries the identity element of G to G'.

(iii) Inverse:

Let $a \in H$ such that $\phi(a) \in \phi[H]$. Since $H \leq G$, we know $a^{-1} \in H$.

We have $e' = \phi(e) = \phi(a^{-1} * a) = \phi(a^{-1}) *' \phi(a)$. So $\phi(a)^{-1} = \phi(a^{-1}) \in \phi[H]$

(iv) Associativity:

The subgroup $\phi[H]$ inherits associativity from the group G'.

□

Question 8. *(Exercises 5: Question 48 (Page 58)) Repeat Ex. 47 for the general situation of the set H of all solutions x of the equation $x^n = e$ for a fixed integer $n \geq 1$ in an Abelian group G with identity e.*

Proof. (i) Closure:

Let $a, b \in H$. Since G is abelian, $ab = ba$. Therefore we take $(ab)^n = a^n b^n = ee = e$ where the first equity arises from the commutative nature of Abelian groups and the second equation arises from the fact that all $x^n = e$ for all elements of H, so $ab \in H$ and H is closed under $*$.

(ii) Identity:
Because $e^n = e$, we have the identity of G as the identity of H.
(iii) Inverse:
For $a \in H, a^n = e$ so inverse of a is a^{n-1}. We know $a^{n-1} \in H$ because $a^{n-1} * a = e$.
(iv) Associativity:
The subgroup H inherits associativity from the group G.
Therefore H is a subgroup of G.

□