Abstract Algebra I

Mario L. Gutierrez Abed

Practice Midterm

(1)

a) Suppose that $*$ is an associative and commutative binary operation on a set X. Show that $H = \{a \in X : a * a = a\}$ is closed under $*$.

Solution:

Let $h,\ g \in H$, so that $h = h * h$ and $g = g * g$ for $h,\ g \in X$.

Then

$$\begin{aligned} h * g &= (h * h) * (g * g) & \\ &= (h * (h * g) * g) & \text{(by associativity)} \\ &= (h * (g * h) * g) & \text{(by commutativity)} \\ &= (h * g) * (h * g) & \text{(by associativity)} \end{aligned}$$

This shows that H is closed under $*$. ✡

b) Give an example of a cyclic group with one generator.

Solution:

$\mathbb{Z}_2 = \{0,\ 1\}$ is such an example, where the generator is 1. That is, $\mathbb{Z}_2$ can be written in the form $\langle 1 \rangle = \{1^n : n \in \mathbb{Z}\} = \{n \cdot 1 : n \in \mathbb{Z}\}$. ✡

c) Explain why $\langle \mathbb{Z}^*,\ + \rangle$ is not a group.

Solution:

It's not a group because it lacks an identity element. That is, there is no $e \in \mathbb{Z}^*$ such that $x * e = e * x = x$ for $x \in \mathbb{Z}^*$. ✡

d) What are the generators of $\mathbb{Z}_6$? How many proper nontivial subgroups does $\mathbb{Z}_6$ have?

Solution:
The generators of $\mathbb{Z}_6$ are the nonzero elements $a \in \mathbb{Z}_6$ such that $\gcd(a, 6) = 1$. The only elements in $\mathbb{Z}_6$ that are relatively prime to 6 are 1 and 5, hence these are the generators.

Now to determine the proper nontivial subgroups of $\mathbb{Z}_6$ we invoke Lagrange's theorem, which says that if H is a subgroup of a finite group G, then the order of H is a divisor of the order of G. We want to use the converse of this theorem, which in fact holds if G (i.e. $\mathbb{Z}_6$ in this case) is abelian. Therefore since $\mathbb{Z}_6$ is abelian, for every divisor of the order of $\mathbb{Z}_6$ (i.e. 6) there is a subgroup of that order. The divisors of 6 are 1,2,3, and 6, so by the converse of Lagrange's theorem (which holds in this case since $\mathbb{Z}_6$ is abelian), we are guaranteed the existence of two nontrivial proper subgroups of order 2 and 3.

e) Explain why $\mathbb{Z}_3$ is not a subgroup of $\mathbb{Z}_6$.

Solution:
In order for a subset H of a group G to be a subgroup of G, H would have to be closed under the same binary operation as G. Since $\mathbb{Z}_3$ is not closed under $+_6$, it follows that $\mathbb{Z}_3$ is not a subgroup of $\mathbb{Z}_6$.
For instance, $1 +_6 2 = 3$ while $1 +_3 2 = 0$.

(2) In each part give an example (with a brief explanation) that satisfies the given conditions or briefly explain why no such example exists:

a) A group having the same order as $\mathbb{Z}_2 \times \mathbb{Z}_2$ but not isomorphic to it.

Solution:
$\mathbb{Z}_4$ is such a group. It is a cyclic group whereas $\mathbb{Z}_2 \times \mathbb{Z}_2$, which is isomorphic to the Klein-4 group, is not cyclic. Therefore $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, even though both groups have the same order.

b) A nonabelian group that is not cyclic.

Solution:
We have a theorem which states that every cyclic group must be abelian. Hence its contrapositive must hold, i.e. if we have a group that is nonabelian then it cannot possibly be cyclic. An example of such groups are the groups of symmetries on n elements S_n for $n \geq 3$.

c) A cyclic group G having a nonabelian subgroup H.

Solution:
No such example exists. We have a theorem which states that every subgroup of a cyclic group is cyclic. Then we have another theorem that tells us that every cyclic group must be abelian. Hence it follows from these two theorems that every subgroup H of a cyclic group G must be abelian.

d) A finite group having no proper nontrivial subgroups.

Solution:
An example of such groups is $\mathbb{Z}_p$ for $2 \leq p < \infty$ a prime. According to a corollary to Lagrange's theorem, every group of prime order is cyclic. By another theorem we know that every cyclic group must be abelian. Hence $\mathbb{Z}_p$ is abelian and the converse of Lagrange's theorem guarantees the existence of subgroups of $\mathbb{Z}_p$ of order that divides p. Since p is prime, only 1 and p itself divide p, hence $\mathbb{Z}_p$ has no nontrivial subgroups. For instance, take $\mathbb{Z}_7$; the only divisors of 7 are itself and 1. Hence there are only two subgroups, one of order 7 and the other of order 1. Thus $\mathbb{Z}_7$ has no nontrivial subgroups.

e) A finite noncyclic group.

Solution:
The Klein-4 group $V = \{e, a, b, ab\}$ with the property $a^2 = b^2 = (ab)^2 = e$ is such an example. This group is not cyclic because there is no element $x \in V$ such that $V = \langle x \rangle = \{x^n : n \in \mathbb{Z}\}$.

f) A group having order 17 containing a subgroup of order 8.

Solution:
No such group can possibly exist. According to Lagrange's theorem, if G is a finite group and H is a

subgroup of G, then the order of H must be a divisor of the order of G. In this case we can see that 8 is clearly not a divisor of 17, which is a prime, therefore no such group can exist.

g) A group having order 8 containing a subgroup of order 4.

<u>Solution:</u>
Such an example is $\mathbb{Z}_8$ with subgroup $H = \{0, 2, 4, 6\}$. To show that H is a subgroup of $\mathbb{Z}_8$, notice that H is closed under the binary operation of $\mathbb{Z}_8$, namely $+_8$. Also the identity 0 of $\mathbb{Z}_8$ is in H and for any element $a \in H$, its inverse is also in H.

h) An abelian group that is not cyclic.

<u>Solution:</u>
The Klein-4 group $V = \{e, a, b, ab\}$ is such an example. We can see that it's abelian since it has the property $a \cdot a = b \cdot b = (ab) \cdot (\text{ab}) = e$. This group is not cyclic because there is no element $x \in V$ such that $V = \langle x \rangle = \{x^n : n \in \mathbb{Z}\}$.

(3) Let $\tau = (2, 5)(3, 4, 7, 8, 9)$ and $\sigma = (1, 2, 5, 3)(4, 8, 7)$.

a) Compute $\tau\sigma\tau^{-1}$.

<u>Solution:</u>

$$\begin{aligned}\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 3 & 4 & 2 & 6 & 7 & 8 & 9 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 4 & 7 & 5 & 6 & 8 & 9 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 7 & 2 & 6 & 8 & 9 & 3 \end{pmatrix}\end{aligned}$$

$$\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 7 & 2 & 6 & 8 & 9 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 9 & 3 & 2 & 6 & 4 & 7 & 8 \end{pmatrix}$$

$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 1 & 4 & 3 & 6 & 7 & 8 & 9 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 3 & 8 & 5 & 6 & 4 & 7 & 9 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 1 & 8 & 3 & 6 & 4 & 7 & 9 \end{pmatrix}\end{aligned}$$

Hence,

$$\tau\sigma\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 7 & 2 & 6 & 8 & 9 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 1 & 8 & 3 & 6 & 4 & 7 & 9 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 9 & 3 & 2 & 6 & 4 & 7 & 8 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 7 & 2 & 6 & 8 & 9 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 9 & 1 & 5 & 6 & 8 & 4 & 7 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 4 & 3 & 1 & 2 & 6 & 9 & 7 & 8 \end{pmatrix}.$$

b) Express $\tau\sigma\tau^{-1}$ of part a) as a product of transpositions. From this result, determine whether $\tau\sigma\tau^{-1}$ is even or odd.

Solution:

$$\tau\sigma\tau^{-1} = (1,\ 5,\ 2,\ 4)\,(7,\ 9,\ 8)$$
$$= (1,\ 4)\,(1,\ 2)\,(1,\ 5)\,(7,\ 8)\,(7,\ 9).$$

Hence $\tau\sigma\tau^{-1}$ is odd.

(4)

a) Let $\phi : G \longrightarrow G'$ be a group homomorphism of G onto G'. Show that if G is abelian, then G' must also be abelian.

Proof:

Let G be abelian and let ϕ be a homomorphism of G onto G'. For $a',\ b' \in G'$, we want to show that $a'\,b' = b'\,a'$. Since ϕ is an onto homomorphism, there exists $a,\ b \in G$ such that $\phi(a) = a'$, $\phi(b) = b'$, and $\phi(a\,b) = \phi(a)\,\phi(b) = a'\,b'$.

But then

$$\begin{aligned} a'\,b' &= \phi(a)\,\phi(b) = \phi(a\,b) \\ &= \phi(b\,a) \quad (\text{since } G \text{ is abelian}) \\ &= \phi(b)\,\phi(a)\ (\text{since } \phi \text{ is a homomorphism}) \\ &= b'\,a'. \end{aligned}$$

Thus we have proven that G' is abelian. ■

b) Let G be a group. Let H be a subset of G consisting of all the elements h of G such that h commutes with every element of G; that is, $H = \{h \in G : hg = gh \ \forall \ g \in G\}$. Prove that H is a subgroup of G.

Proof:

‣ We first show that H is closed under the binary operation of G. For any two elements $h_1, h_2 \in H$, we must then show that $h_1 h_2 \in H$. So let $g \in G$, then we have

$$\begin{aligned}(h_1 h_2) g &= h_1(h_2 g) \quad \text{(by associativity of } G\text{).} \\ &= h_1(g h_2) \quad \text{(by commutative property of } H\text{)} \\ &= (h_1 g) h_2 \quad \text{(by associativity of } G\text{)} \\ &= (g h_1) h_2 \quad \text{(by commutative property of } H\text{)} \\ &= g(h_1 h_2) \quad \text{(by associativity of } G\text{) .}\end{aligned}$$

Since $(h_1 h_2) g = g(h_1 h_2)$, by the definition of H we have $h_1 h_2 \in H$. ✓

‣ Now we show that the identity e is in H. Observe that, $\forall \ g \in G$, we have $e g = g e$. Thus e satisfies the property $\{e \in G : e g = g e \ \ \forall \ g \in G\}$. Hence $e \in H$. ✓

‣ Lastly, we need to show that for $h_1 \in H$, its inverse h_1^{-1} is also in H. For any element $h_1 \in H$, we have $h_1 g = g h_1$. Now let us show that $h_1^{-1} g = g h_1^{-1}$:

$$\begin{aligned} & h_1 g = g h_1 \\ \Longrightarrow \quad & h_1^{-1} h_1 g = h_1^{-1} g h_1 \quad \text{(multiplying on the left by } h_1^{-1}\text{)} \\ \Longrightarrow \quad & g = h_1^{-1} g h_1 \quad (*)\end{aligned}$$

Now, multipliying (*) by h_1^{-1} on the right, we get $g h_1^{-1} = h_1^{-1} g$. This shows that $h_1^{-1} \in H$. ✓

We have proven that H is a subgroup of G, as desired. ■

(5) Any of the following will be chosen:

a) Prove Cayley's theorem: Every group is isomorphic to a group of permutations.

Proof:

Let G be a group. We show that G is isomorphic to a subgroup of S_G. By a previous lemma, we need only define an injective function $\phi : G \longrightarrow S_G$ such that $\phi(x\, y) = \phi(x)\, \phi(y) \ \ \forall \ x, \ y \in G$ (this function will be an isomorphism from G to its image $\phi[G] \subseteq S_G$).

For $x \in G$, let $\lambda_x : G \longrightarrow G$ be defined by $\lambda_x(g) = x\, g \;\; \forall\, g \in G$ (we think of λ_x as performing left multiplication by x). The equation

$$\lambda_x(x^{-1}\, c) = x(x^{-1}\, c) \quad \forall\, c \in G$$

shows that λ_x maps G onto G.
Now

$$\lambda_x(a) = \lambda_x(b) \Longrightarrow x\, a = x\, b \Longrightarrow a = b \quad \text{(by cancellation)}\,.$$

Thus λ_x is also injective, and it's a permutation of G.

We now define $\phi : G \longrightarrow S_G$ by defining $\phi(x) = \lambda_x$ for all $x \in G$. To show that ϕ is injective, suppose that $\phi(x) = \phi(y)$. Then $\lambda_x = \lambda_y$ as functions mapping G into G.
In particular,

$$\lambda_x(e) = \lambda_y(e) \Longrightarrow x\, e = y\, e \Longrightarrow x = y \quad \text{(by cancellation)}\,.$$

Thus ϕ is injective.
We only need to show that $\phi(x\, y) = \phi(x)\, \phi(y)$, that is $\lambda_{xy} = \lambda_x\, \lambda_y$. Now, for any $g \in G$, we have $\lambda_{xy}(g) = (x\, y)\, g$. Permutation multiplication is function composition, so

$$(\lambda_x\, \lambda_y)\,(g) = \lambda_x(\lambda_y(g)) = \lambda_x(y\, g) = x(y\, g) = (x\, y)\, g = \lambda_{xy}.$$

Thus we have that $\lambda_{xy} = \lambda_x\, \lambda_y$, which is the desired homomorphic property, and we have thus proven that every group is isomorphic to a group of permutations. ■

b) Let G be a group and let a be a fixed element of G.

Then,

i) Show that the map $\lambda_a : G \longrightarrow G$, given by $\lambda_a(g) = a\, g$ for $g \in G$, is a permutation of the set G.

Proof:
Let G be a group and fix $a \in G$. Then the map λ_a is given by $\lambda_a(g) = \{a\, g : g \in G\}$. We need to show that this map is bijective:

Showing that the map is injective is trivial; if we pick two images $\lambda_a(g_1) = a\, g_1$ and $\lambda_a(g_2) = a\, g_2$ such that $a\, g_1 = a\, g_2$, we have that $g_1 = g_2$ by the cancellation law, where $g_1,\, g_2 \in G$. Hence λ_a is injective. This map is obviously surjective as well, since by definition for each image $a\, g \in G$ we have a preimage $g \in G$.

Since λ_a is bijection from the group G onto itself, we have that λ_a is a permutation on G. ■

ii) Show that $H = \{\lambda_a : a \in G\}$ is a subgroup of S_G.

Proof:
To show that H is a subgroup of S_G, we need to show that the identity element and inverse element of S_G are in H, and we also need to show that H is closed under the binary operation defined on G (permutation multiplication):

‣ To show closure, let $\lambda_a(g),\ \lambda_b(g) \in H$, where $a,\ b,\ g \in G$. Then,

$$\lambda_a \circ \lambda_b(g) = \lambda_a(\lambda_b(g)) = \lambda_a(b\,g) = a\,b\,g = \lambda_{a\,b}(g) \in H$$

Hence H is closed under permutation multiplication. ✓

‣ Since G is a group, for any $a \in G\ \exists\ a^{-1} \in G$. Thus the map $\lambda_{a\,a^{-1}} = \lambda_e$ represents our identity on H, since $\lambda_e(g) = e\,g = g$. ✓

‣ For $a,\ a^{-1},\ g \in G$ and $\lambda_a \in H$, we have

$$\lambda_a \circ \lambda_{a^{-1}}(g) = \lambda_a(\lambda_{a^{-1}}(g)) = \lambda_a(a^{-1}\,g) = a\,a^{-1}\,g = e\,g = \lambda_e(g).$$

Hence $\lambda_{a^{-1}}$ is the inverse element of H. ✓

Since H is closed under the binary operation defined on S_G, and it contains the identity and inverse elements of S_G, we have that H is a subgroup of S_G. ■

c) Show that any infinite cyclic group G is isomorphic to the group $\langle \mathbb{Z},\ +\rangle$.

Proof:
For all positive integers m, we have that $a^m \neq e$. We claim that no two distinct exponents h and k can give equal elements a^h and a^k of G.
Suppose that $a^h = a^k$ and say $h > k$. Then

$$a^h\,a^{-k} = a^{h-k} = e$$

contrary to our assumption that $a^m \neq e$ for all positive integers m. Hence every element of G can be expressed as a^m for a unique $m \in \mathbb{Z}$. This indicates that the map $\phi : G \longrightarrow \mathbb{Z}$ given by $\phi(a^i) = i$ is thus well defined and is bijective.

Also,

$$\phi(a^i\, a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j).$$

So the homomorphism property is satisfied and ϕ is an isomorphism. ■

d) Let $\phi : G \longrightarrow G'$ be a group homomorphism of G into G'. If e is the identity element in G and e' denotes the identity element in G', show

i) $\phi(e) = e'$.
ii) $\phi(x^{-1}) = \phi(x)^{-1}$, for all $x \in G$.

<u>Proof:</u>
‣ To prove i), let $x \in G$, $\phi(x) \in G'$. Since ϕ is a homomorphism and e is the identity element in G, we have the following:

$$\begin{aligned} & \phi(x\, e) = \phi(x)\, \phi(e) \\ \Longrightarrow \quad & \phi(x) = \phi(x)\, \phi(e) \\ \Longrightarrow \quad & \phi(x)\, e' = \phi(x)\, \phi(e) \\ \Longrightarrow \quad & e' = \phi(e) \quad \text{(by the left cancellation law)} \quad \checkmark \end{aligned}$$

‣ To prove ii), note that since ϕ is a homomorphism, we have $\phi(x)\, \phi(x^{-1}) = \phi(x\, x^{-1}) = \phi(e)$. But by part i), we have that $\phi(e) = e'$.
Hence it follows that $\phi(x^{-1})$ is the inverse element in G', i.e. $\phi(x^{-1}) = \phi(x)^{-1}$. ✓ ■

e) Prove that a group is abelian if every element except the identity has order 2.

<u>Proof:</u>
We are assuming that $a^2 = a \cdot a = 1$ for every element $a \neq 1 \in G$.
For any two elements $a,\ b \in G$, we must show that $a\, b = b\, a$.
Let $a,\ b \in G$. So

$$\begin{aligned} & a^2 = 1 & & & b^2 = 1 \\ \Longrightarrow \quad & a^{-1}\, a^2 = a^{-1}\, 1 & \text{and} \quad & \Longrightarrow & b^{-1}\, b^2 = b^{-1} \cdot 1 \\ \Longrightarrow \quad & a = a^{-1} & & \Longrightarrow & b = b^{-1} \end{aligned}$$

Since a and b are distinct elements of G and G is a group, we have that $a\, b \in G$, hence $(a\, b)^2 = 1$.

Then, by the above argument we have

$$\begin{aligned} a\,b &= (a\,b)^{-1} \\ a\,b &= b^{-1}\,a^{-1} \\ a\,b &= b\,a \qquad \text{(since } b^{-1} = b \text{ and } a^{-1} = a\text{).} \end{aligned}$$

Thus G is abelian. ■

f) Prove that every cyclic group is abelian.

Proof:

Let G be a cyclic group and let a be a generator for G so that $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$. If g_1 and g_2 are any two elements of G, there exist integers r and s such that $g_1 = a^r$ and $g_2 = a^s$.
Then,

$$g_1\,g_2 = a^r\,a^s = a^{r+s} = a^{s+r} = a^s\,a^r = g_2\,g_1.$$

Thus we have proven that G is abelian. ■

g) Show that $\mathbb{R}$ under addition is isomorphic to $\mathbb{R}^+$ under multiplication.

Proof:

We define $\phi : \mathbb{R} \longrightarrow \mathbb{R}^+$ by $\phi(x) = e^x$ for $x \in \mathbb{R}$. Notice that $e^x > 0$ for all $x \in \mathbb{R}$, so indeed we have $\phi(x) \in \mathbb{R}^+$. Now we need to show that ϕ is an isomorphism:

- Notice that

$$\begin{aligned} & \phi(x) = \phi(y) \\ \Longrightarrow\ & e^x = e^y \\ \Longrightarrow\ & \log(e^x) = \log(e^y) \\ \Longrightarrow\ & x = y\,. \end{aligned}$$

Hence ϕ is injective. ✓

- Now if $r \in \mathbb{R}^+$, then $\log(r) \in \mathbb{R}$ and $\phi(\log(r)) = e^{\log(r)} = r$. Thus ϕ is surjective. ✓

- For $x,\ y \in \mathbb{R}$, we have $\phi(x + y) = e^{x+y} = e^x\,e^y = \phi(x) \cdot \phi(y)$. Thus ϕ is homomorphic. ✓

Since ϕ is a bijective homomorphism, it is an isomorphism. Therefore $\langle \mathbb{R}, +\rangle$ is isomorphic to $\langle \mathbb{R}^+, \cdot\rangle$, as we set out to prove. ■

h) Prove that for $n \geq 3$, S_n is nonabelian.

<u>Proof:</u>
Let $\alpha, \beta \in S_n$ be defined by

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & . & . & . \\ 1 & 3 & 2 & . & . & . \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & . & . & . \\ 3 & 2 & 1 & . & . & . \end{pmatrix}.$$

That is, we "permute" the first three elements of both α and β and fix the rest.
Then we have

$$\begin{aligned} \alpha\beta &= \begin{pmatrix} 1 & 2 & 3 & . & . & . \\ 1 & 3 & 2 & . & . & . \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & . & . & . \\ 3 & 2 & 1 & . & . & . \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & . & . & . \\ 2 & 3 & 1 & . & . & . \end{pmatrix} \end{aligned}$$

while

$$\begin{aligned} \beta\alpha &= \begin{pmatrix} 1 & 2 & 3 & . & . & . \\ 3 & 2 & 1 & . & . & . \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & . & . & . \\ 1 & 3 & 2 & . & . & . \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & . & . & . \\ 3 & 1 & 2 & . & . & . \end{pmatrix}. \end{aligned}$$

We can see that $\alpha\beta \neq \beta\alpha$, and this shows that S_n is nonabelian for $n \geq 3$. ■

i) Let H be a subgroup of a group G. Let the relation $\sim_R$ be defined on G by $a \sim_R b$ iff $ab^{-1} \in H$.
Show that $\sim_R$ is an equivalence relation on G.

<u>Proof:</u>
We want to show that $\sim_R$ is an equivalence relation. In order to do this we just need to show that $\sim_R$ satisfies the following three conditions:

- Let $a \in G$. Then $a\,a^{-1} = e$ and $e \in H$ since H is a subgroup. Thus $a \sim_R a$. (Reflexive)
- Suppose $a \sim_R b$. Then $a\,b^{-1} \in H$. Since H is a subgroup, $(a\,b^{-1})^{-1} = b\,a^{-1}$ is in H.
This shows that $b \sim_R a$. (Symmetric)
- Let $a \sim_R b$ and $b \sim_R c$. Then $a\,b^{-1} \in H$ and $b\,c^{-1} \in H$. Since H is a subgroup, $(a\,b^{-1})\,(b\,c^{-1}) = a\,c^{-1}$ is in H, hence $a \sim_R c$. (Transitive) ■