MATH 4107 (Prof. Heil) PRACTICE PROBLEMS WITH SOLUTIONS Spring 2018

Here are a few practice problems on groups. **You should first work through these WITHOUT LOOKING at the solutions!** After you write your own solution, you can compare to my solution. Your solution does not need to be identical to mine—there are often many ways to solve a problem—but it does need to be CORRECT.

1. Show that if A is a subgroup of a group G and $g \in G$, then $gAg^{-1} = \{gag^{-1} : a \in A\}$ is a subgroup of G.

Solution

Let A be a subgroup of G and let $g \in G$ be a fixed element. We must show that gAg^{-1} is a subgroup of G.

Note that gAg^{-1} is nonempty since $e = geg^{-1} \in gAg^{-1}$.

To show that $gAg{-}1$ is closed under compositions, suppose that x, y are any two elements of gAg^{-1}. By definition, this means that $x = gag^{-1}$ and $y = gbg^{-1}$ for some a, $b \in A$. Since $ab \in A$, we therefore have that

$$xy \;=\; gag^{-1}gbg^{-1} \;=\; g(ab)g^{-1} \;\in\; gAg^{-1}.$$

To show that gAg^{-1} is closed under inverses, suppose that $x \in gAg^{-1}$. Then $x = gag^{-1}$ for some element $a \in A$. Since $a^{-1} \in A$, we therefore have that

$$x^{-1} \;=\; (gag^{-1})^{-1} \;=\; (g^{-1})^{-1}a^{-1}g^{-1} \;=\; ga^{-1}g^{-1} \;\in\; gAg^{-1}. \quad \square$$

2. Let $\varphi\colon G \to H$ be a homomorphism of groups with kernel N. For a, $x \in G$, show that the following statements are equivalent (i.e., each one implies the other).

i. $\varphi(a) = \varphi(x)$.
ii. $a^{-1}x \in N$.
iii. $aN = xN$.

Solution

i $\Rightarrow$ ii. Suppose that $\varphi(a) = \varphi(x)$. Then

$$\varphi(a^{-1}x) \;=\; \varphi(a)^{-1}\varphi(x) \;=\; e,$$

so $a^{-1}x \in \ker(\varphi) = N$.

ii $\Rightarrow$ iii. Suppose that $a^{-1}x \in N$. Then $n = a^{-1}x \in N$. Suppose that $z \in aN$. Then $z = am$ for some $m \in N$. Therefore $z = xx^{-1}am = xn^{-1}m \in xN$ since $n^{-1}m \in N$. Thus $aN \subseteq xN$, and the reverse inclusion is similar.

iii $\Rightarrow$ ii. Suppose that $aN = xN$. Then $a = ae \in aN = xN$, so $a = xn$ for some $n \in N$. Therefore $n = x^{-1}a$, so $a^{-1}x = n^{-1} \in N$.

iii $\Rightarrow$ i. Your turn, find the proof. $\square$

3. Let G be a group. Define $a \sim b$ if there exists a $g \in G$ such that $b = gag^{-1}$. Prove that $\sim$ is an equivalence relation.

Solution

Since $a = aaa^{-1}$, we have $a \sim a$.

If $a \sim b$ then $b = gag^{-1}$ for some $g \in G$. Therefore $a = g^{-1}bg = g^{-1}b(g^{-1})^{-1}$. Since $g^{-1} \in G$, we have $b \sim a$.

If $a \sim b$ and $b \sim c$ then $b = gag^{-1}$ and $c = hbh^{-1}$ for some g, $h \in H$. Therefore $c = hbh^{-1} = hgag^{-1}h^{-1} = (hg)a(hg)^{-1}$. Since $hg \in G$, we have $a \sim c$. □

4. Let $x \in \mathbb{R}^3$ be a fixed vector. The *stabilizer* of x is the set

$$G_x \;=\; \{A : A \text{ is an invertible } 3 \times 3 \text{ matrix and } Ax = x\}.$$

(a) Prove that G_x is a group if the group operation is matrix multiplication.

Solution

G_x is closed under matrix multiplication. Suppose that A, $B \in G_x$. Then A and B are invertible 3×3 matrices which have the property that $Ax = x$ and $Bx = x$. The product of invertible matrices is invertible, so AB is an invertible 3×3 matrix. Further,

$$(AB)x \;=\; A(Bx) \;=\; Ax \;=\; x,$$

so $AB \in G_x$.

The group operation is associative. The group operation is matrix multiplication, and we know that matrix multiplication is associative.

G_x contains an identity. The 3×3 identity matrix I is in G_x because it is invertible and satisfies $Ix = x$.

G_x is closed under inverses. Suppose that $A \in G_x$. Then A is an invertible 3×3 matrix which has the property that $Ax = x$. The inverse matrix A^{-1} is also an invertible 3×3 matrix. Further, if we multiply both sides of the equation $x = Ax$ by A^{-1}, we see that

$$A^{-1}x \;=\; A^{-1}Ax \;=\; x.$$

Hence $A^{-1} \in G_x$. □

(b) Explicitly compute the stabilizer of the vector $x = (1, 0, 0)$. What is the order of G_x?

Solution

Let A be any matrix in G_x. Let v_1, v_2, v_3 be the three columns of A. Then:

$$x \;=\; Ax \;=\; \begin{bmatrix} | & | & | \\ v_1 & v_2 & v_3 \\ | & | & | \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \;=\; 1v_1 + 0v_2 + 0v_3 \;=\; v_1.$$

Hence the first column of A must be the vector $x = (1, 0, 0)$. This shows that

$$G_x \;\subseteq\; \{A : A \text{ is invertible with first column } x\}.$$

Suppose on the other hand that A is an invertible matrix whose first column is x. Let v_2, v_3 be the other two columns. Then

$$Ax \;=\; \begin{bmatrix} | & | & | \\ x & v_2 & v_3 \\ | & | & | \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \;=\; 1x + 0v_2 + 0v_3 \;=\; x.$$

Therefore $A \in G_x$. This shows that

$$\{A : A \text{ is invertible with first column } x\} \subseteq G_x.$$

The combination of these two inclusions implies that

$$G_x = \{A : A \text{ is invertible with first column } x\}.$$

We can be still a little more specific about the matrices that lie in G_x. Let $v_2 = (a, b, c)$ and $v_3 = (d, e, f)$. Then since a matrix is invertible if and only if it has a nonzero determinant, we need

$$\det(A) = \det \begin{bmatrix} 1 & a & d \\ 0 & b & e \\ 0 & c & f \end{bmatrix} = bf - ce$$

to be nonzero. Hence

$$G_x = \left\{ \begin{bmatrix} 1 & a & d \\ 0 & b & e \\ 0 & c & f \end{bmatrix} : bf \neq ce \right\}.$$

Since there are infinitely many such matrices, the order of G_x is infinity. □

QUESTION: Does our answer to problem 4(b) imply that if x is ANY element of $\mathbb{R}^3$ then G_x will consist simply of those invertible 3×3 matrices whose first column is x? NO!! (Why?? What would the stabilizer of $x = (1, 1, 0)$ be?)

5. Recall that $S_n = A\big(\{1, \ldots, n\}\big)$ is the group of all bijections of $\{1, \ldots, n\}$ onto itself, under the operation of composition of functions.

Suppose that $n \geq 3$. Show that if $f \in S_n$ commutes with every $g \in S_n$, then $f = e$, the identity bijection.

Solution

Suppose that f commutes with every g, but that $f \neq e$. Then there is some $i \in \{1, \ldots, n\}$ such that $f(i) = j \neq i$. Since $n \geq 3$, there must be a third number k that is distinct from both i and j. Let g be the bijection that exchanges i and k and leaves all other numbers alone. In particular, since j is different from both i and k, we have $g(j) = j$. Therefore,

$$(g \circ f)(i) = g(f(i)) = g(j) = j = f(i)$$

and

$$(f \circ g)(i) = f(g(i)) = f(k) = f(g(i)) = f(k).$$

But $g \circ f = f \circ g$, so this implies $f(i) = f(k)$. Since f is a bijection, this implies $i = k$, which is a contradiction. Therefore it cannot be true that f commutes with every $g \in S_n$. □

6. Let f be the following permutation of $\{1, 2, 3, 4, 5, 6, 7\}$ given in two-line notation:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 6 & 3 & 7 & 4 & 1 \end{pmatrix}.$$

Explain the meaning of this notation, and explain how to compute the inverse of f.

Solution

The word "permutation" is a synonym for a bijection of a set onto itself. So f is a bijection

of $\{1,2,3,4,5,6,7\}$ onto itself, and the two-line notation means that $f(1) = 2$, $f(2) = 5$, and so forth. To find the inverse, you simply have to trace the permutation backwards. For example, since f maps the number 1 to the number 2, the inverse of this permutation must map 2 back to 1. Hence if we write the inverse in two-line notation then the number 1 must appear on the second line immediately under the number 2. We do the same computation for each of the other numbers, arriving finally at the conclusion that the inverse permutation is

$$f^{-1} \;=\; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 4 & 6 & 2 & 3 & 5 \end{pmatrix}. \qquad \square$$

7. Let $\varphi\colon G \to H$ be a homomorphism of a group G *onto* a group H. If N is a normal subgroup of G, show that $\varphi(N)$ is a normal subgroup of H.

Solution

Recall the definition that $\varphi(N) = \{\varphi(n) : n \in N\}$.

The fact that $\varphi(N)$ is a subgroup of H is an exercise in the book, but let's go ahead and give a proof of this anyway. We know that $e_H = \varphi(e_G) \in \varphi(N)$, so $\varphi(N)$ is not empty.

Next let's show that $\varphi(N)$ is closed under compositions. Suppose that x, $y \in \varphi(N)$. Then by definition of $\varphi(N)$, we must have $x = \varphi(a)$ and $y = \varphi(b)$ for some a, $b \in N$. Since φ is a homomorphism, we therefore have

$$xy \;=\; \varphi(a)\varphi(b) \;=\; \varphi(ab).$$

However, since N is a subgroup of G, we know that $ab \in N$. Therefore $xy = \varphi(ab) \in \varphi(N)$, so $\varphi(N)$ is closed under compositions.

Finally, let's show that $\varphi(N)$ is closed under inverses. Suppose that $x \in \varphi(N)$. Then by definition of $\varphi(N)$, we must have $x = \varphi(a)$ for some $a \in N$. Since φ is a homomorphism, we therefore have

$$x^{-1} \;=\; \varphi(a)^{-1} \;=\; \varphi(a^{-1}).$$

However, since N is a subgroup of G, we know that $a^{-1} \in N$. Therefore $x^{-1} = \varphi(a^{-1}) \in \varphi(N)$, so $\varphi(N)$ is closed under inverses.

Thus $\varphi(N)$ is a subgroup of H. Now let's show that it is a *normal* subgroup. To do this, we must show that $h\varphi(N)h^{-1} \subseteq \varphi(N)$ for every $h \in H$. So, choose any particular $h \in H$. Then since φ is SURJECTIVE (this is important!), we know that $h = \varphi(g)$ for some $g \in G$.

Suppose now that $x \in h\varphi(N)h^{-1}$. This means that $x = h\varphi(a)h^{-1}$ for some $a \in N$. Therefore

$$x \;=\; h\varphi(a)h^{-1} \;=\; \varphi(g)\varphi(a)\varphi(g)^{-1} \;=\; \varphi(g)\varphi(a)\varphi(g^{-1}) \;=\; \varphi(gag^{-1}).$$

However, N is a NORMAL subgroup of G, so $gNg^{-1} = N$. Therefore $gag^{-1} \in gNg^{-1} = N$. Hence $x = \varphi(gag^{-1}) \in \varphi(N)$. Thus, we have shown that $h\varphi(N)h^{-1} \subseteq \varphi(N)$, so $\varphi(N)$ is normal. $\square$

8. Prove that a group G is abelian if and only if the function $f\colon G \to G$ defined by $f(a) = a^{-1}$ is a homomorphism.

Solution

"$\Rightarrow$." Suppose that G is abelian, i.e., $ab = ba$ for every a, $b \in G$. Then

$$f(ab) \;=\; (ab)^{-1} \;=\; b^{-1}a^{-1} \;=\; a^{-1}b^{-1} \;=\; f(a)\,f(b).$$

Therefore f is a homomorphism.

"$\Leftarrow$." Suppose that f is a homomorphism, and let a, b be any two elements of G. Then

$$ab \;=\; f(a^{-1})\,f(b^{-1}) \;=\; f(a^{-1}b^{-1}) \;=\; f((ba)^{-1}) \;=\; ((ba)^{-1})^{-1} \;=\; ba.$$

Therefore G is abelian. $\square$

9. The set $G = \{2^n : n \in \mathbb{Z}\}$ is a group under the operation of ordinary multiplication of numbers. Prove that G is isomorphic to the group of integers $\mathbb{Z}$ under the operation of addition of numbers.

Solution

Define a function $f\colon \mathbb{Z} \to G$ by $f(n) = 2^n$. I will leave it to you to show that f is a bijection (do it!). If m, $n \in \mathbb{Z}$, then

$$f(m+n) \;=\; 2^{m+n} \;=\; 2^m 2^n \;=\; f(m)f(n),$$

so f is a homomorphism. Since f is both a bijection and a homomorphism, it is an isomorphism. $\square$

10. Define

$$G \;=\; \mathbb{Z}_6 \times \mathbb{Z}_4 \;=\; \{(m,n) : m \in \mathbb{Z}_6,\, n \in \mathbb{Z}_4\},$$

i.e., $\mathbb{Z}_6 \times \mathbb{Z}_4$ is the set of all ordered pairs of elements from $\mathbb{Z}_6$ and $\mathbb{Z}_4$. I will not prove it, but you should be able to show that this set is a group under the operation

$$(m_1, n_1) \oplus (m_2, n_2) \;=\; ((m_1 + m_2) \bmod 6,\; (n_1 + n_2) \bmod 4).$$

a. Compute the cyclic subgroup $H = \langle (1,2) \rangle$, i.e., give a list of all the elements in H.

Solution

Just start computing the "powers" of the element $(1,2)$. Since this is an additive group, "powers" means adding $(1,2)$ to itself over and over. We usually call these the "multiples" of $(1,2)$ rather than "powers." The multiples are:

$$\begin{aligned}
0 \cdot (1,2) \;&=\; (0,0),\\
1 \cdot (1,2) \;&=\; (1,2),\\
2 \cdot (1,2) \;&=\; (1,2) \oplus (1,2) \;=\; (2,0),\\
3 \cdot (1,2) \;&=\; (2,0) \oplus (1,2) \;=\; (3,2),\\
4 \cdot (1,2) \;&=\; (3,2) \oplus (1,2) \;=\; (4,0),\\
5 \cdot (1,2) \;&=\; (4,0) \oplus (1,2) \;=\; (5,2),\\
6 \cdot (1,2) \;&=\; (5,2) \oplus (1,2) \;=\; (0,0).
\end{aligned}$$

That is, adding $(1,2)$ to itself six times yields the identity $(0,0)$. The element $(1,2)$ has order six, and the cyclic subgroup that it generates is

$$H \;=\; \langle (1,2) \rangle \;=\; \big\{(0,0),\; (1,2),\; (2,0),\; (3,2),\; (4,0),\; (5,2)\big\}. \quad \square$$

b. Compute the coset $(2,3) + H$.

Solution

We simply have to add the element $(2,3)$ to each of the elements of H:

$$(2,3) + H \;=\; \big\{(2,3),\ (3,1),\ (4,3),\ (5,1),\ (0,3),\ (1,1)\big\}. \quad \square$$

c. Compute $[G : H]$.

Solution

The group G contains 24 elements: there are six choices for the first coordinate of any element and four choices for the second coordinate, yielding 24 distinct elements in $G = \mathbb{Z}_6 \times \mathbb{Z}_4$. The subgroup H contains 6 elements. Therefore the index is $[G : H] = 4$. The 24 elements of the group are divided into 4 cosets, each containing 6 elements. $\square$

11. Let G be a finite group with K normal in G. If $(|K|, [G : K]) = 1$, prove that K is the unique subgroup of G having order $|K|$.

Hint: Suppose H is a subgroup of G such that $|H| = |K|$. You must show that $H = K$. To do this, think about the order $o(Ka)$ of the coset Ka in the group G/K when a is an element of H.

Solution

The hint suggests thinking about the order of some cosets Ka in the quotient group G/K, specifically those cosets Ka which come from elements $a \in H$. By Lagrange's Theorem, we know that the order of an element must divide the order of the group. In this case the element is the coset Ka and the group is G/K. Now, the order of the group G/K is $|G/K| = [G : K]$. Therefore, $o(Ka)$ must divide $[G : K]$. If we could show that $o(Ka)$ must also divide $|K|$, then we could conclude that $o(Ka) = 1$, because we are given that the greatest common divisor of $|K|$ and $[G : K]$ is 1.

Now, what we have to work with is that $a \in H$. Therefore, the order of a must divide $|H|$, which equals $|K|$. That is, $o(a)$ divides $|K|$. However, that isn't what we want, because we want to show that $o(Ka)$ divides $|K|$. So, we need to think about how $o(a)$ and $o(Ka)$ are related.

So, let $k = o(a)$. By definition, $a^k = e$. Since K is normal, this implies that

$$(Ka)^k \;=\; (Ka)(Ka)\cdots(Ka) \;=\; K(aa\cdots a) \;=\; K(a^k) \;=\; Ke \;=\; K.$$

But K is the identity element of G/K, so the order of Ka in G/K must divide k. Thus $o(Ka)$ divides k, but we know that $k = o(a)$ divides $|H| = |K|$, so we conclude that $o(Ka)$ divides $|K|$.

Thus, we have shown that $o(Ka)$ divides both $|K|$ and $[G : K]$. Since these two numbers are relatively prime, we must have $o(Ka) = 1$. Hence Ka is the identity element in G/K, i.e., $Ka = K$. But this implies $a \in K$. Thus we have shown that every element $a \in H$ is also in K. Hence $H \subseteq K$. But H and K contain the same number of elements, so H must in fact be all of K, i.e., $H = K$. Hence K is the only subgroup of G with this order. $\square$