Chapter 2 Homework

Spencer

October 23, 2015

Problem 3

Show that $\{1, 2, 3\}$ under multiplication modulo 4 is not a group but that $\{1, 2, 3, 4\}$ under multiplication modulo 5 is a group.

The former is not a group since $2 \cdot 2 \equiv 0 \pmod 4$ and $0 \notin \{1, 2, 3\}$.

Since for all $x \in \{1, 2, 3, 4\}$, we have $\gcd(x, 5) = 1$, we have for all $x, y \in \{1, 2, 3, 4\}$, $\gcd(xy, 5) = 1$. Since no such xy is divisible by 5, we'll have $0 < xy < 5$ when we take xy to be the least non-negative residue modulo 5. This shows closure for the latter set under multiplication modulo 5. Associativity follows from the associativity of modular multiplication. The identity here is 1. The inverse of 1 is 1, the inverse of 2 is 3, the inverse of 3 is 2, and the inverse of 4 is 4.

Problem 4

Show that the gruop $GL(2, \mathbb{R})$ of Example 9 is non-Abelian by exhibiting a pair of matrices A and B in $GL(2, \mathbb{R})$ such that $AB \neq BA$.

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

This can be checked by straight-forward computation, or more easily by seeing that one is a 90 degree rotation counter-clockwise, while the other is a reflection about the y-axis. Now consider transforming the point $(1, 0)$ by each composition.

Problem 7

Translate each of the following multiplicative expression into its additive counterpart. Assume that addition is commutative.

Part a

$$a^2 b^3 = 2a + 3b$$

Part b

$$a^{-2}(b^{-1}c)^2 = -2a + 2(-b + c)$$

Part c

$$(ab^2)^{-3}c^2 = e = 0 = -3(a + 2b) + 2c$$

Problem 11

Prove that the set of all 2×2 matrices with entires from $\mathbb{R}$ and determinent $+1$ is a group under matrix multiplication.

Closure of this set under the operation of matrix multiplication is easily verified by the fact that for any two matrices A and B in the set, $(\det A)(\det B) = (+1)(+1) = +1 = \det AB$ while AB is yet another 2×2 matrix having real entries. Then associativity follows from the associativity of matrix multiplication. The identity of the group is...

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

...and clearly its determinent is $+1$. Then since all matrices have a determinent of $+1$, they all have inverses. What remains to be shown is that all of these inverses have a determinent of $+1$. Let the following matrix be in the set.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Then we have $ad - bc = 1$. It's inverse is given by...

$$\frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Then the scalar of the matrix obviously goes away and the determinent is calculated as $ad - (-b)(-c) = ad - bc = 1$, which is just what we wanted.

problem 14

Let G be a group with the following property: Whenever a, b, and c belong to G and $ab = ca$, then $b = c$. Prove that G is Abelian.

Let $x, y \in G$. Choose $b = xy \in G$, $c = yx \in G$, and $a = x^{-1} \in G$. It follows that $ab = y = ca$. Then, by the property given, we see that $b = c$ and therefore $xy = yx$. Since we let x and y be any two elements in G, the group G must be Abalian.

Problem 15

Let a and b be elements of an Abelian group and let n be any integer. Show that $(ab)^n = a^n b^n$. Is this also true for non-Abelian groups?

First consider the case where $n = 0$. Since we define any element of a group to the zeroth power to be the identity, this case holds.

Now consider the case where $n > 0$. Since we have an Abelian group, we can swap any pair of adjacent elements in any one of the expressions on either side of the equation. Because of this we can swap any two elements in the expression by using a sequence of adjacent swaps of adjacent elements. Using this fact, we have...

$$\begin{aligned} a^n b^n &= aba^{n-1}b^{n-1} \\ &= (ab)^2 a^{n-2} b^{n-2} \\ &= (ab)^3 a^{n-3} b^{n-3} \\ &\cdots \\ &= (ab)^n a^{n-n} b^{n-n} \\ &= (ab)^n \end{aligned}$$

Let's now consider the case when $n < 0$. The equation becomes...

$$((ab)^{-1})^{|n|} = (b^{-1}a^{-1})^{|n|} = (a^{-1}b^{-1})^{|n|} = (a^{-1})^{|n|}(b^{-1})^{|n|}$$

Reading from left to right, the first equality holds by Problem 16, and the second holds by the fact that we have an Abelian group. We now notice that this reduces to the $n > 0$ case, and therefore holds as well.

Now suppose a non-Abelian group satisfies this property. Consider the case $n = 2$. Then, for all a, b in the group, we have $abab = aabb$. But now left multiply this by a^{-1} and right multiply this by b^{-1} and we get $ba = ab$, showing that the group operator commutes. But this means that the group is Abelian. By contradiction, non-Abilian groups do now hold the property for all integers n.

Problem 16

In a group, prove that $(ab)^{-1} = b^{-1}a^{-1}$. Find an example that shows that it is possible to have $(ab)^{-2} \neq b^{-2}a^{-2}$. Find distinct nonidentity elements a and b from a non-Abelian group with the property that $(ab)^{-1} = a^{-1}b^{-1}$.

Let $x = b^{-1}a^{-1}$. To show that $x^{-1} = ab$, we need only show that $xab = b^{-1}a^{-1}ab = b^{-1}b = e$, and $abx = abb^{-1}a^{-1} = aa^{-1} = e$. The identity now follows from the fact that an element and its inverse are inverses of one another. Thus, $x = (ab)^{-1}$, and we have $(ab)^{-1} = b^{-1}a^{-1}$ as desired.

Suppose $(ab)^{-2} = b^{-2}a^{-2}$ for all $a, b \in G$ where G is any group. We can rearrange this to get...

$$\begin{aligned}((ab)^{-1})^2 &= b^{-2}a^{-2}\\ (b^{-1}a^{-1})^2 &= (b^{-1})^2(a^{-1})^2\\ b^{-1}a^{-1}b^{-1}a^{-1} &= b^{-1}b^{-1}a^{-1}a^{-1}\\ a^{-1}b^{-1} &= b^{-1}a^{-1}\end{aligned}$$

This rearranges to $ab = ba$ and even just implies it directly. Therefore, any counter example can be found by finding $a, b \in G$ where the operation on a and b doesn't commute. In D_3 choose $a = F_0$ and $b = R_{120}$.

We now want to find distinct nonidentity elements a and b of a group such that their inverses commute, since $b^{-1}a^{-1} = (ab)^{-1}$ and we want $(ab)^{-1} = a^{-1}b^{-1}$. But this is just equivilant to finding two nonidentity elements of a group that commute. That is, let $x = a^{-1}$ and $y = b^{-1}$, and we just want to find nonidentity elements x and y such that $xy = yx$. Just let x be any nonidentity element and let y be the inverse of x. Here we're exploiting the fact that elements of groups commute with their inverses. We know that $y \neq e$ since if it was, then this would imply that x is the identity, but it's not. In D_3 choose $a = R_{120}$ and $b = R_{240}$.

Problem 17

Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

Using the result proven in Problem 16, we have...

$$(ab)^{-1} = a^{-1}b^{-1} \iff b^{-1}a^{-1} = a^{-1}b^{-1} \iff e = aba^{-1}b^{-1} \iff ba = ab$$

Problem 18

In a group, prove that $(a^{-1})^{-1} = a$ for all a.

Here we're being asked to prove that the inverse of the inverse of any element of a group is itself. This is clear from...

$$a^{-1}a = e$$

...where e is the identity. From the definition of an inverse, this shows that the inverse of a^{-1} is a and that the inverse of a is a^{-1}.

Problem 19

For any elements a and b from a group and any integer n, prove that...

$$(a^{-1}ba)^n = a^{-1}b^n a$$

The case $n = 0$ is clear since $(a^{-1}ba)^0 = e = a^{-1}a = a^{-1}b^0a$. Now suppose $n > 0$.

$$\begin{aligned}
(a^{-1}ba)^n &= a^{-1}ba(a^{-1}ba)^{n-1} \\
&= a^{-1}baa^{-1}ba(a^{-1}ba)^{n-2} \\
&= a^{-1}b^2a(a^{-1}ba)^{n-2} \\
&= a^{-1}b^3a(a^{-1}ba)^{n-3} \\
&= a^{-1}b^4a(a^{-1}ba)^{n-4} \\
&\dots \\
&= a^{-1}b^n a(a^{-1}ba)^{n-n} \\
&= a^{-1}b^n a
\end{aligned}$$

Now consider the case when $n < 0$. The LHS then becomes...

$$((a^{-1}ba)^{-1})^{|n|} = (a^{-1}b^{-1}a)^{|n|}$$

Using the result found in the $n > 0$ case we see that the RHS is...

$$(a^{-1}b^{-1}a)^{|n|} = a^{-1}(b^{-1})^{|n|}a = a^{-1}b^n a$$

...which is just what we wanted.

Problem 20

If $a_1, a_2, \dots, a_n$ belong to a group, what is the inverse of $a_1a_2 \dots a_n$?

It is easy to see that the answer is $a_n^{-1}a_{n-1}^{-1} \dots a_1^{-1}$. But let's go ahead and show it...

$$\begin{aligned}
e &= a_1a_1^{-1} \\
&= a_1a_2a_2^{-1}a_1^{-1} \\
&= a_1a_2a_3a_3^{-1}a_2^{-1}a_1^{-1} \\
&= \dots \\
&= a_1a_2 \dots a_na_n^{-1} \dots a_2^{-1}a_1^{-1}
\end{aligned}$$

Problem 23

Prove that every group table is a Latin square.

Suppose that the same element appears at least twice in the same row or column. This would mean that for some elements a, b, c, and d in the group, with $a \neq b$, that $ac = d$ and $bc = d$. This implies that $ac = bc$. Right multiplication by the inverse of c on both sides of this equation gives us $a = b$. By contradiction, no element can appear more than once in the same row or column.

Problem 24

Construct a Cayley table for $U(12)$.

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Problem 26

Prove that if $(ab)^2 = a^2b^2$ in a group G, then $ab = ba$.

The proof follows from the following steps.

$$\begin{aligned} abab &= aabb \\ a^{-1}ababb^{-1} &= a^{-1}aabbb^{-1} \\ ba &= ab \end{aligned}$$

Problem 27

Let a, b, and c be elements of a group. Solve the equation $axb = c$ for x. Solve $a^{-1}xa = c$ for x.

For the former equation, $x = a^{-1}cb^{-1}$, for the latter, $x = aca^{-1}$.

Problem 28

Prove that the set of all rational numbers of the form 3^m6^n, where m and n are integers, is a group under multiplication.

Associativity follows directly from that of multiplication. The following shows closure.

$$(3^m6^n)(3^i6^j) = 3^m3^i6^n6^j = 3^{m+i}6^{n+j}$$

The identity is the element with $m = n = 0$. This suggests the following inverse.

$$(3^m6^n)(3^{-m}6^{-n}) = 3^{m-m}6^{n-n} = 3^06^0 = 1$$

Problem 29

Let G be a finite group. Show that the number of elements x of G such that $x^3 = e$ is odd. Show that the number of elements x of G such that $x^2 = e$ is even.

Consider the set $S = \{x \in G : x(x^2) = e\}$. That is, the set of all elements of G whose square is their inverse. This set has at least one member since $e(e^2) = e$. Suppose $x \in S$ and $x \neq e$. Then $x^{-1} = x^2$ and $(x^2)^{-1} = x$ are distinct pairs of elements of S that are inverses of one another since $x^2 = x$ if and only if $x = e$. Notice that $(x^2)^3 = (x^3)^2 = e^2 = e$. We used the property here that if a is the inverse of b, then b is the inverse of a. Since additions to S must come in pairs, except for e, the set S must have an odd number of elements.

A similar argument works for the second part of the question. Now let $S = \{x \in G : x^2 = e\}$. That is, the set of all elements of G that are their own inverses. Err...

Problem 31

Suppose that G is a group with the property that for every choice of elements in G, $axb = cxd$ implies $ab = cd$. Prove that G is Abelian.

Consider the case where $c = b$, $d = a$, and $x = a^{-1}$. Clearly, $axb = cxd$ in this case, and so it follows that $ab = cd = ba$. We could have also chosen $x = b^{-1}$.

Problem 33

Prove that if G is a group with the property that the square of every element is the identity, then G is Abelian.

The property given here says that every element is its own inverse. Using this and the result proven in Problem 16, we see that...

$$ab = a^{-1}b^{-1} = (ba)^{-1} = ba$$

Problem 37

Let $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in \mathbb{R}, a \neq 0 \right\}$. Show that G is a group under matrix multiplication. Explain why each element of G has an inverse even though the matrices have 0 determinent.

Associativity follows from the associativity of matrix multiplication. Closure is verified by the following check.

$$\begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix}$$

Note that $2ab \neq 0$ since $a \neq 0$ and $b \neq 0$. This check suggests the following identity.

$$\begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$$

Given any element of the set, we can now formulate its inverse.

$$\begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} 1/(4a) & 1/(4a) \\ 1/(4a) & 1/(4a) \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$$

The determinent of a matrix determines whether the matrix has a multiplicative inverse with respect to a different identity matrix than the one we're using here.