Homework 1 Solutions m31 f 11

(1) a) Prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Pf We must show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ and that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. For the first statement, suppose $x \in A \cap (B \cup C)$. In other words, $x \in A$ and either $x \in B$ or $x \in C$. If $x \in B$, then we have $x \in A \cap B$; if $x \in C$, we have $x \in A \cap C$. Either way, we see that $x \in A \cap (B \cup C) \Rightarrow x \in (A \cap B) \cup (A \cap C)$.

For the second statement, suppose $x \in (A \cap B) \cup (A \cap C)$. Then either $x \in A \cap B$ or $x \in A \cap C$. In either scenario, we have that $x \in A$ and $x \in B \cup C$. Hence $x \in A \cap (B \cup C)$.

Thus, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ and

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$$

so the sets must be equal. ☒

HW1 Solns M31F11

(1) b) Prove that $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$.

Pf We must show that $A\cup(B\cap C)$ is contained in $(A\cup B)\cap(A\cup C)$, and that $(A\cup B)\cap(A\cup C) \subseteq A\cup(B\cap C)$. For the first statement, suppose $x\in A\cup(B\cap C)$. In other words, either $x\in A$ or $x\in B\cap C$. If $x\in A$, then x is in both $A\cup B$ and $A\cup C$; if $x\in B\cap C$, then x is in both B and C, so x is in both $A\cup B$ and $A\cup C$. In either case, $x\in A\cup(B\cap C) \Rightarrow x\in(A\cup B)\cap(A\cup C)$.

For the second statement, suppose that $x\in(A\cup B)\cap(A\cup C)$. In other words, x is in both $A\cup B$ and $A\cup C$. We need to show that either $x\in A$ or $x\in B\cap C$.

Thus, suppose $x\in(A\cup B)\cap(A\cup C)$ but $x\notin A$. Since $x\in A\cup B$, we must have $x\in B$; since $x\in A\cup C$, we must have $x\in C$. Thus, $x\in B\cap C$ if $x\notin A$.

If $x\in A$, then $x\in A\cup(B\cap C)$.

Thus, $x\in(A\cup B)\cap(A\cup C) \Rightarrow x\in A\cup(B\cap C)$.

Since $(A\cup B)\cap(A\cup C)\subseteq A\cup(B\cap C)$ and
$A\cup(B\cap C)\subseteq(A\cup B)\cap(A\cup C)$,
the two sets are equal as claimed. $\blacksquare$

(2) Problem 1.9

To check if the operation is commutative, we need to check that $x * y = y * x$ for every $x, y \in \{a, b, c, d\} = S$. Since the table given is symmetric across the diagonal, and since reflecting across the diagonal takes $x*y$ to $y*x$ for any $x, y \in S$, it follows that $*$ is commutative.

(Alternatively, you could write out all the values of $x*y$ and $y*x$ for $y, x \in S$ and compare them)

(Alternatively, you could observe that the table forms a symmetric matrix, and if $x*y$ is in the (i,j) position, then $y*x$ is in the (j,i) position.)

To check that $*$ is associative, we must check whether $(x*y)*z = x*(y*z)$ for each $x, y, z \in S$.

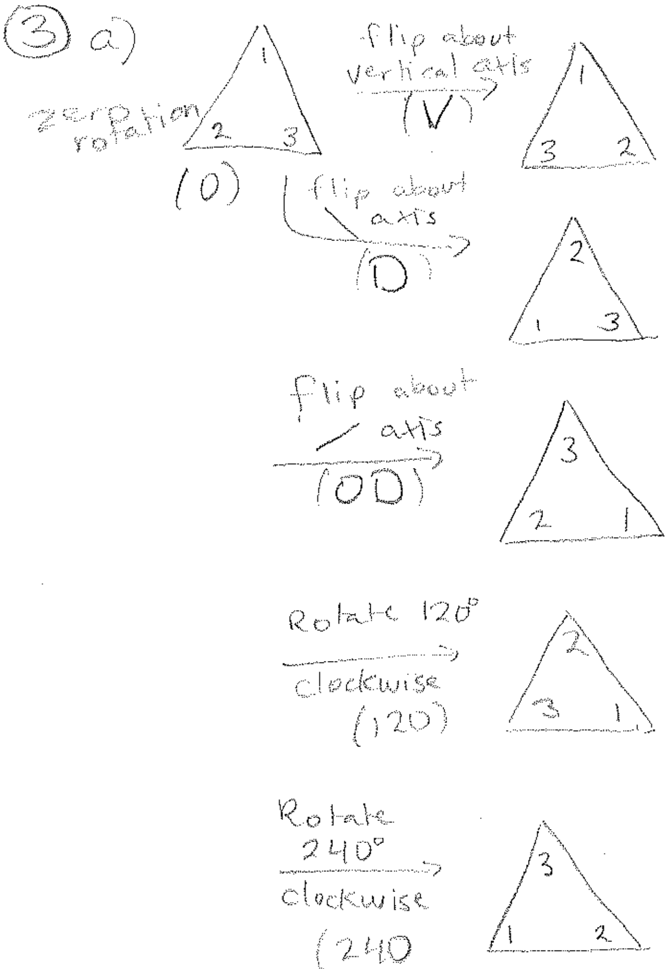
$a*(b*c) = a*d = d$; $(a*b)*c = c*c = a$

So the operation is not associative.

(There are many other triples that show that $*$ is not associative!)

HW 1 Solutions, M31 F11

③ a)



(This is also a vertical flip followed by a 240° rotation)

(This is also a vertical flip followed by a 120° rotation)

There are also other ways to describe the moves!

b)

*	0	120	240	V	D	OD
0	0	120	240	V	D	OD
120	120	240	0	OD	V	D
240	240	0	120	D	OD	V
V	V	D	OD	0	120	240
D	D	OD	V	240	0	120
OD	OD	V	D	120	240	0

c) D_3 is not abelian; for example, $OD * D = 240$ but $D * OD = 120$.

(4)

$*$	1	2	3	4	5	6
1	2	3	4	5	6	1
2	3	4	5	6	1	2
3	4	5	6	1	2	3
4	5	6	1	2	3	4
5	6	1	2	3	4	5
6	1	2	3	4	5	6

Differences between $(\mathbb{Z}_6, \oplus)$ and D_3:

① $\mathbb{Z}_6$ is abelian and D_3 is not

② D_3 has 3 elements (other than the identity) such that $x * x = e$; $\mathbb{Z}_6$ only has one.

Similarities between $(\mathbb{Z}_6, \oplus)$ and D_3:

① The groups have the same number of elements

② Both groups have precisely two elements x such that x isn't the identity, $x * x \neq e$, but $x * x * x = e$ (120 & 240 in D_3, 2 & 4 in $(\mathbb{Z}_6, \oplus)$).

③ In both groups, each element appears exactly once in each row and column of the Cayley table. (This property is actually shared by all groups; can you prove why?)

(5) The set of odd integers does not form a group under addition because it does not contain an identity; If e is an integer such that $e+n=n$ for all odd n, we must have $e=0$, which is not odd.

Also, addition is not a binary operation on the set of odd integers: If a and b are odd, then $a+b$ is even, so $a+b$ is not in the set.

(Alternatively, you could give an example: 7 and 1 are both odd, but $7+1=8$ is not.)

(6) $(P(X), \cap)$ is not a group. The operation $\cap$ is an associative binary operation, and the set X satisfies $A \cap X = A$ for all $A \in P(X)$, so we have an identity, but we do not have inverses for all elements. For example, $\emptyset \cap A = \emptyset$ for any $A \subseteq X$, so ~~there~~ is no set A such that $\emptyset \cap A = X$. In other words, $\emptyset$ has no inverse.

(7) Let $G = \{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R}, a^2 + b^2 \neq 0 \}$. Then G forms a group under matrix multiplication.

Pf We know that matrix multiplication is an associative operation by Example 4 on Page 12 of our text. We need to check the existence of an identity, and of inverses. We also must check that $AB \in G$ for all $A, B \in G$.

Prop The matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is an identity for G.

Proof I satisfies $IA = AI = A$ for any 2×2 matrix A, and hence for any $A \in G$. Since $0 = -0$ and $1^2 + 0^2 = 1 \neq 0$, $I \in G$. Thus, I is the identity in G.

Prop If $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in G$, then the inverse of A,

$$A^{-1} = \frac{1}{a^2+b^2} \begin{bmatrix} a & -b \\ b & a \end{bmatrix},$$

is also in G.

Proof The formula for A^{-1} comes from Example 5 on pp. 18-19 in our text, so we only need to check that $A^{-1} \in G$. But A^{-1} is of the general form of an element of G, (just swap b for $-b$, and multiply a, b by $\frac{1}{a^2+b^2}$) and moreover, $a^2 + (-b)^2 = a^2 + b^2$, which is nonzero by hypothesis.

[cont'd next pg]

Solutions to HW 1, M31 F11

⑦ cont'd | Therefore, $\left(\frac{a}{a^2+b^2}\right)^2 + \left(\frac{(-b)}{(a^2+b^2)}\right)^2 = \frac{a^2+b^2}{(a^2+b^2)^2} = \frac{1}{a^2+b^2}$

is also nonzero, so $A^{-1} \in G$.

To see that matrix multiplication is binary on G, we need to check that $AB \in G$ for any $A, B \in G$. But

$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{pmatrix}$ is of the right form, and

$(ac-bd)^2 + (ad+bc)^2$

$= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2$

$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$

$= (a^2+b^2)(c^2+d^2)$

is nonzero if $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ are in G.

Thus, G is a group. ☒

HW1 Solutions M31 F11

(8) a) [This was a mistake on my part; it's Theorem 3.4 in the book.]

To show that $(a*b)^{-1} = b^{-1}*a^{-1}$, we multiply the 2nd expression by $a*b$:

$$b^{-1}*a^{-1}*(a*b) = b^{-1}*(a^{-1}*a)*b \quad \text{by associativity}$$
$$\left.\begin{aligned} &= b^{-1}*e*b \\ &= b^{-1}*b = e \end{aligned}\right\} \text{by property of inverses.}$$

We must also check the multiplication on the left: $(a*b)*b^{-1}*a^{-1} = a*(b*b^{-1})*a^{-1}$
$$= a*e*a^{-1} = a*a^{-1}$$
$$= e.$$

Thus, by uniqueness of inverses, $(a*b)^{-1} = b^{-1}*a^{-1}$! ⊠

b) Consider the group D_3 and the elements D & OD (see Exercise 3). Then $D*OD = 120$, so $(D*OD)^{-1} = 240$, and $(D*OD)^{-2} = 240*240 = 120$.

However, $(OD)^{-1} = OD$, and $OD*OD = 0$, and similarly $D^{-2} = 0$. Thus,
$$120 = (D*OD)^{-2} \neq (OD)^{-2}*D^{-2} = 0.$$
(There are many other examples!)

HW 1 Solutions, M31 F11

(8)c) The textbook asserts that $(a*b)^{-1} = a^{-1}*b^{-1}$ for all $a,b \in G$ iff G is abelian. I would like you to prove at least the following direction:

Prop If $(G,*)$ is abelian, then $(a*b)^{-1} = a^{-1}*b^{-1}$ for all $a,b \in G$.

Proof We know by Part (a) that $(a*b)^{-1} = b^{-1}*a^{-1}$ always. By definition, if G is abelian, $x*y = y*x$ for all $x,y \in G$. Therefore, in particular,

$$(a*b)^{-1} = b^{-1}*a^{-1} = a^{-1}*b^{-1}$$

for any a,b in an abelian group G. $\boxtimes$

For the other direction:

Prop If $(a*b)^{-1} = a^{-1}*b^{-1}$ for all a,b in a group $(G,*)$, then G is abelian.

Proof We need to show that for all a,b in G,

$a*b = b*a$. Given $a,b \in G$, consider a^{-1} and b^{-1}.

By Part (a), we know that $b^{-1}*a^{-1} = (a*b)^{-1}$, but by hypothesis, $(a*b)^{-1} = a^{-1}*b^{-1}$. Thus $b^{-1}*a^{-1} = a^{-1}*b^{-1}$. Since this is true for every $a,b \in G$ it also must be true that $a*b = b*a$ for every $a,b \in G$, so G is abelian. $\boxtimes$