THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2070A Algebraic Structures 2019-20
Tutorial 1
Date: 11th September 2019

Revision: A binary operation $*$ on a set S is a function mapping form $S \times S$ to S.

Remark:

1. Exactly one element is assigned to each possible ordered pair of elements of S.
2. For each ordered pair of elements of S, the element assigned to it is again in S.

Problems:

1. Let $M(\mathbb{R})$ be the set of all matrices with real entries. Is the usual matrix addition $+$ a binary operation on $M(\mathbb{R})$?

   Solution. No. $A+B$ is not defined for an ordered pair (A, B) of matrices having different sizes.

   ◀

2. On $\mathbb{Z}^+$, define $*$ by $a * b = c$ where c is at least 2 more than $a + b$. Is $*$ a binary operation on $\mathbb{Z}^+$?

   Solution. No. More than one element can be assigned to $1*1$. In fact any positive integer at least 4 can be assigned to $1 * 1$.

   ◀

3. On $\mathbb{Z}^+$, define $*$ by $a * b = a/b$. Is $*$ a binary operation on $\mathbb{Z}^+$?

   Solution. No. $1 * 3 (= 1/3)$ is not in $\mathbb{Z}^+$.

   ◀

4. On $\mathbb{Q}$, define a binary operator $*$ by $a * b = ab + 1$. Is $*$ commutative? Is $*$ associative?

Solution. It is commutative because $ab+1 = ba+1$ for all $a, b \in \mathbb{Q}$. It is not associative because

$$(1 * 2) * 3 = 3 * 3 = 10 \neq 8 = 1 * 7 = 1 * (2 * 3).$$

◀

5. Let $SL(2, \mathbb{Z})$ be the set of $n \times n$ matrices of determinant 1 with integral entries. Prove that

$$\Gamma_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}) : a \text{ and } d \text{ are odd}, b \text{ and } c \text{ are even} \right\}$$

is a group with the group operation given by matrix multiplication.

Solution.

- We first show that matrix multiplication is a well-defined binary operation on Γ_2, which means for any $g, h \in SL(2, \mathbb{Z})$, we wish to show that $gh \in \Gamma_2$. First of all, $det(gh) = det(g) \cdot det(h) = 1 \cdot 1 = 1$. Writing $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $h = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ where a, d, e, h are odd and b, c, f, g are even, their product $gh = \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix}$. Note that $a\alpha + b\gamma$ and $c\beta + d\delta$ are both odd and $a\beta + b\delta$ and $c\alpha + d\gamma$ are both even, so $gh \in \Gamma_2$.
- Γ_2 is a subset of the set $M_{2\times 2}(\mathbb{R})$ of 2×2 matrix. Since matrix multiplication is associative, $\cdot$ is associative on Γ_2.
- Clearly we have $I \in \Gamma_2$. It is clear that $IA = AI = A$ for all $A \in \Gamma_2$. Hence, Γ_2 has identity element.
- Given $g \in \Gamma_2$, $g = (\begin{matrix} a & b \\ c & d \end{matrix})$. And note that we have that a, d are odd, b, c are even, and $ad - cb = 1$. Let $g' = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ and check directly that $gg' = I$. So $g' \in \Gamma_2$. Hence every element in Γ_2 has inverse element.

◀

6. Let $S = \mathbb{R} \setminus \{-1\}$. Define $*$ on S by

$$a * b = a + b + ab.$$

   (a) Find $20 * 70$.

   (b) Is $*$ a binary operation on S?

   (c) Show that $(G, *)$ is an abelian group.

   (d) Find the solution of the equation $1490 * x = 2020$ in S.

   (e) Find the solution of the equation $20 * x * 70 = 2020$ in S.

Solution. (a) $20 * 70 = 20 + 70 + (20)(70) = 1490.$.

(b) Yes. We need to show that S is closed under $*$, that is, that for any $a, b \in S$, $a*b \in S$ which means that $a + b + ab \neq -1$. Now note that $a + b + ab = -1$ if and only if $0 = ab + a + b + 1 = (a + 1)(b + 1)$. This is the case if and only if $a = -1$ or $b = -1$, which is not the case for $a, b \in S$.

(c)
- Associativity: By direct checking, one gets

$$(a * b) * c = (a + b + ab) * c = a + b + c + ab + ac + bc + abc$$

and

$$a * (b * c) = a * (b + c + bc) = a + b + c + ab + ac + bc + abc.$$

- 0 serves as identity element for $*$, for $0 * a = a * 0 = a$.
- For any $a \in S$, $\frac{-a}{a+1}$ serves as inverse of a because

$$a * \frac{-a}{a+1} = a - \frac{a}{a+1} - \frac{a^2}{a+1} = 0$$

and

$$\frac{-a}{a+1} * a = \frac{-a}{a+1} + a - \frac{a^2}{a+1} = 0.$$

- It is clear that $*$ is commutative.

(d) The inverse of 1490 is $-1490/1491$ (see the above). So the solution is given by

$$x = -1490/1491 * 2020 = 530/1491.$$

(e) Because the operation is commutative, we have $20 * x * 70 = 20 * 70 * x = 1490 * x$. One arrives at $1490 * x = 2020$, Part (d) yields $x = 530/1491$.
Alternatively, the solution can be obtained by $x = \frac{-20}{21} * 2020 * \frac{-70}{71} = 530/1491$ as 20 and 70 have respective inverses $\frac{-20}{21}$ and $\frac{-70}{71}$.

◀

7. Let G be a group of order 4 and e be the identity. Does the equation $x^3 = e$ have no non-trivial solution (i.e. $x \neq e$)?

Solution. Yes. It has no non-trivial solution. Suppose $a \neq e$ and $a^3 = e$. Then a, a^2, a^3 are distinct elements in G, because

- if $a = a^2$, then $a^{-1}a = a^{-1}a^2$ implies $a = e$ (contradicting to $a \neq e$);
- if $a = a^3$, then $a^2 = e$ which implies $a = aa^2 = a^3 = e$;
- if $a^2 = a^3$, then $a = e$ again!

Let $G = \{a, a^2, a^3 = e, b\}$ where $b \neq a, a^2, a^3$. (Note G is of order 4, so G carries 4 elements.)
But then $ab \notin G$ because

- if $ab = e$, then $a^3 b = a^2(ab) = a^2 e = a^2$ imples $b = a^2$ recalling $a^3 = e$;
- if $ab = a$, then $b = e$;
- if $ab = b$, then $a = e$;
- if $ab = a^2$, then $b = a$.

The consequence $ab \notin G$ gives a contradiction as G is a group. So $a^3 \neq e$. $\blacktriangleleft$

Optional Part

1. Let X be a set. For any subsets U, V of X, we define
$$U \setminus V = \{x \in U : x \notin V\} \quad \text{and} \quad U \Delta V = (U \setminus V) \cup (V \setminus U).$$
Note that we have $U \Delta V = (U \cup V) \cap \left(\overline{U} \cup \overline{V}\right)$ and $U \Delta V = \left(U \cap \overline{V}\right) \cup \left(\overline{U} \cap V\right)$. Let $P(X)$ be the set of all subsets of X. Show that $P(X)$ with Δ as the operation is a group.

Solution.

- The binary operation Δ is well-defined on $P(X)$, because $U - V$ and $V - U$ are subsets of X and so is their union.
- **Associativity**: You may check from the following two facts: $U \Delta V = (U \cup V) \cap \left(\overline{U} \cup \overline{V}\right)$ and $U \Delta V = \left(U \cap \overline{V}\right) \cup \left(\overline{U} \cap V\right)$, the distributive law, and DeMorgan's law, so the details are left to you. We demonstrate that for any $U, V, W \in P(X)$,
$$\begin{aligned}
& (U \Delta V) \Delta W \\
= \; & \left(\left((U \cap \overline{V}) \cup (\overline{U} \cap V)\right) \cap \overline{W}\right) \cup \left(\overline{(U \Delta V)} \cap W\right) \\
= \; & \left(\left((U \cap \overline{V}) \cup (\overline{U} \cap V)\right) \cap \overline{W}\right) \cup \left(\overline{\left((U \cup V) \cap \left(\overline{U} \cup \overline{V}\right)\right)} \cap W\right) \\
= \; & \left(U \cap \overline{V} \cap \overline{W}\right) \cup \left(\overline{U} \cap V \cap \overline{W}\right) \cup \left(\left(\overline{(U \cup V)} \cup \overline{\left(\overline{U} \cup \overline{V}\right)}\right) \cap T\right) \\
= \; & \left(U \cap \overline{V} \cap \overline{W}\right) \cup \left(\overline{U} \cap V \cap \overline{W}\right) \cup \left(\left((\overline{U} \cap \overline{V}) \cup (U \cap V)\right) \cap W\right) \\
= \; & \left(U \cap \overline{V} \cap \overline{W}\right) \cup \left(\overline{U} \cap V \cap \overline{W}\right) \cup \left(\overline{U} \cap \overline{V} \cap W\right) \cup (U \cap V \cap W)\,.
\end{aligned}$$
In a similar way, we can also find that (leave it to you!)
$$U \Delta (V \Delta W) = \left(U \cap \overline{V} \cap \overline{W}\right) \cup \left(\overline{U} \cap V \cap \overline{W}\right) \cup \left(\overline{U} \cap \overline{V} \cap W\right) \cup (U \cap V \cap W)\,.$$
- **Identity**: Take $\emptyset$ (the empty set) to be the identity element e. You will be able to verify the condition.
- **Inverse**: Check that the inverse of U is U itself. Indeed
$$U \Delta U = (U \setminus U) \cup (U \setminus U) = \emptyset.$$

$\blacktriangleleft$