Chapter 5 Algebraic Systems

§5.1. Binary Operations

Definition: Let A and B be two nonempty sets. A binary operation on A is a function $f: A\times A\to B$. That is, for any ordered pair of elements a, b of A, there is a unique element c of B such that $c=f(a, b)$.

Notation: Usually we use $*$ to denote a binary operation. Also, instead of writing $*(a, b)$, we write $a*b$ to denote the element in B that is mapped by (a, b) under $*$.

Definition: Let $*$ be a binary operation defined on A and mapped to B (i.e. $*: A\times A\to B$). The operation $*$ is said to be closed on A (or A is closed under $*$) iff $a*b\in A\ \forall a, b\in A$. In other words, $*$ is closed on A iff $\text{Ran}(*)\subseteq A$.

Examples

1) The usual addition (+), subtraction (−), multiplication ($\cdot$), and division (/) are binary operations on $\mathbb{R}$ (or $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{Z}^+$, etc.).
   Unless otherwise stated, +, −, $\cdot$, and / will denote these usual operations on a set of real numbers.

2) + is closed on $\mathbb{Z}$, i.e. the sum of two integers is also an integer. + is also closed on $\mathbb{Z}^+$.
   − is closed on $\mathbb{Z}$, but − is not closed on $\mathbb{Z}^+$ ($\because 2, 3\in\mathbb{Z}^+$ but $2-3=-1\notin\mathbb{Z}^+$).
   $\cdot$ is closed on $\mathbb{Z}$, but / is not closed on $\mathbb{Z}$ ($\because 1, 2\in\mathbb{Z}$ but $1/2=\frac{1}{2}\notin\mathbb{Z}$).

3) + is closed on $\mathbb{Q}$ $\because \frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}\in\mathbb{Q}$, where $a, b, c, d\in\mathbb{Z}$, $b\neq 0$ and $d\neq 0$.
   Similarly it can be shown that − and $\cdot$ are closed on $\mathbb{Q}$.
   / is not closed on $\mathbb{Q}$ $\because \frac{9}{0}$ is undefined. However, / is closed on $\mathbb{Q}-\{0\}$.

4) Let $\mathbb{I}=\mathbb{R}-\mathbb{Q}$ (i.e. $\mathbb{I}$ is the set of all irrational numbers). Then + is not closed on $\mathbb{I}$.
   Proof: Let $a=\sqrt{2}$ and $b=2-\sqrt{2}$.
   It is proved in Chapter 1 that $\sqrt{2}\notin\mathbb{Q}$. It can be proved that $2-\sqrt{2}\notin\mathbb{Q}$ (for details, see remark i/ below).
   Thus $a, b\in\mathbb{I}$. However, $a+b=\sqrt{2}+(2-\sqrt{2})=2\in\mathbb{Q}$, i.e. $a+b\notin\mathbb{I}$.
   Remark i/. Proof of $2-\sqrt{2}\notin\mathbb{Q}$: Suppose $2-\sqrt{2}\in\mathbb{Q}$. Then $2-\sqrt{2}=\frac{m}{n}$ for some $m, n\in\mathbb{Z}^+$. But this implies that $\sqrt{2}=2-\frac{m}{n}=\frac{2n-m}{n}\in\mathbb{Q}$, which is a contradiction. $\therefore 2-\sqrt{2}\notin\mathbb{Q}$.
   ii/. Same argument shows that if $a\in\mathbb{Q}$ and $b\notin\mathbb{Q}$, then $a+b$, $a-b$, $a\cdot b$, a/b, and b/a (provided $a\neq 0$) are all irrational.

5) $\cdot$ is not closed on $\mathbb{I}$ $\because \sqrt{2}\cdot\sqrt{2}=2\notin\mathbb{I}$.

6) Union ($\cup$), intersection ($\cap$), difference (−), and symmetric difference ($\oplus$) are binary operations on sets of sets.
   Remark The complement operation ^{c} is not a binary operation because it is performed on a single set. This kind of operation is called a unary operation.

7) Conjunction ($\wedge$), disjunction ($\vee$), conditional ($\to$), and biconditional ($\leftrightarrow$) are binary operations on sets of propositions. Negation ($\sim$) is another example of a unary operation.

8) Matrix addition, matrix subtraction, and matrix multiplication are binary operations on sets of matrices. In this chapter, we will mainly consider 2×2 matrices.

9) We may define an operation on a finite set by a table, like the following.

$*$	α	β
α	α	α
β	β	β

   This table defines an operation $*$ on the set $\{\alpha, \beta\}$ with

$$\alpha*\alpha=\alpha,\quad \alpha*\beta=\alpha,$$
$$\beta*\alpha=\beta,\quad \beta*\beta=\beta.$$

   Here, the operation $*$ is closed on the set $\{\alpha, \beta\}$.

10) Define a binary operation $*$ on $\mathbb{Z}^+$ by

$$a*b=a^b+b^a,$$

where the operations involved on the RHS are the usual exponentiation and the usual addition.
Find $2*3$, $2*5$, and $3*4$. If $2*x=100$ for some $x\in\mathbb{Z}^+$, find x.

Solution: $2*3=2^3+3^2=8+9=17$, $2*5=2^5+5^2=32+25=57$, $3*4=3^4+4^3=81+64=145$.

If $2*x=100$ for some $x\in\mathbb{Z}^+$, then $2^x<100 \Rightarrow x\le 6$. If $x\le 5$, then $2*x=2^x+x^2\le 2^5+5^2=2*5=57$.

$\therefore$ The only possible solution of $2*x=100$ is $x=6$.

In fact, $2*6=2^6+6^2=64+36=100$.

$\therefore$ $2*x=100$ has a unique solution, viz. $x=6$.

Remark Same argument shows that the only possible solution of $2*x=101$ ($x\in\mathbb{Z}^+$) is $x=6$. However, $x=6$ is not a solution of $2*x=101$. This means that $2*x=101$ has no solution in $\mathbb{Z}^+$.

§5.2. Properties of Operations

Associative

Definition: Let $*$ be a binary operation on a set A. $*$ is said to be associative iff

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

for all elements a, b, c of A (whenever $a*b$ and $b*c$ are both in A).

Commutative

Definition: Let $*$ be a binary operation on a set A. $*$ is said to be commutative iff

$$a*b=b*a$$

for all elements a, b of A.

Examples

1) It is well known that + and $\cdot$ are both associative and commutative.
– is neither associative nor commutative.
/ is neither associative nor commutative.

2) It is known in Chapter 1 that $\cup$ (union) and $\cap$ (intersection) are both associative and commutative.
It can be readily seen that – (set difference) is neither associative nor commutative.
It is obvious that $\oplus$ (symmetric difference) is commutative. Moreover, it can be shown that $\oplus$ is associative.

3) It is known in Chapter 2 that $\wedge$ (conjunction) and $\vee$ (disjunction) are both associative and commutative.
$\rightarrow$ (conditional) is neither associative (see the table) nor commutative.
It is obvious that $\leftrightarrow$ (biconditional) is commutative. Moreover, it can be shown that $\leftrightarrow$ is associative.

$(p$	$\rightarrow$	$q)$	$\rightarrow$	r	p	$\rightarrow$	$(q$	$\rightarrow$	$r)$
F	T	F	F	F	F	T	F	T	F

4) It is obvious that matrix addition is both associative and commutative.
It is also obvious that matrix subtraction is neither associative nor commutative.
It is known that **matrix multiplication is associative but not commutative**.

5) Let $*$ be the operation on $A=\{\alpha, \beta\}$ defined by the right table.
Here $\alpha*\beta=\alpha$ and $\beta*\alpha=\beta$. $\therefore$ $*$ is not commutative.
Note that $*$ has the property that $x*y=x$ $\forall x, y\in A$.
It follows that $\forall a, b, c\in A$, $(a*b)*c=a*c=a$ and $a*(b*c)=a$.
$\therefore$ $*$ is associative.

$*$	α	β
α	α	α
β	β	β

6) Let $*$ be the operation on $\mathbb{Z}^+$ defined by $a*b=a^b+b^a$ ($a, b\in\mathbb{Z}^+$).
Since + is commutative, we have $b*a=b^a+a^b=a^b+b^a=a*b$. $\therefore$ $*$ is a commutative.
Since $(2*2)*1=(4+4)*1=8*1=8+1=9$
and $2*(2*1)=2*(2+1)=2*3=8+9=17$,
we have $(2*2)*1\ne 2*(2*1)$.
$\therefore$ $*$ is not associative.

§5.3. Algebraic Systems

Definition: A set together with a number of operations on the set is called an algebraic system.

When there is only one operation, the algebraic system is usually denoted by $(A, *)$, where A is a set and $*$ is an operation defined on A. Here we will mainly discuss algebraic systems of the form $(A, *)$.

When $*$ is closed on A, $(A, *)$ is said to be a closed algebraic system. When $*$ is commutative, $(A, *)$ is said to be a commutative algebraic system.

Examples

1) $(\mathbb{Z}, +)$, $(\mathbb{Z}, -)$, and $(\mathbb{Z}, \cdot)$ are closed algebraic systems.
   $(\mathbb{Z}, +)$ and $(\mathbb{Z}, \cdot)$ are commutative, but $(\mathbb{Z}, -)$ is not.

2) $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, +)$, and $(\mathbb{R}, \cdot)$ are all commutative closed algebraic systems.
   $(\mathbb{Q}, -)$ and $(\mathbb{R}, -)$ are not commutative.

3) Let A be the set of all 2×2 matrices with real entries, i.e.
$$A = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}.$$
   Let $+$ and $\cdot$ denote matrix addition and matrix multiplication respectively.
   Then $(A, +)$ is commutative, but $(A, \cdot)$ is not.

4) Let $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$ (i.e. A is the set of all 2×2 diagonal matrices with real entries), and let $\cdot$ denote matrix multiplication.
   Since
$$\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix}\begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & 0 \\ 0 & b_1b_2 \end{pmatrix} = \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix}\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix},$$
   $(A, \cdot)$ is a commutative closed algebraic system.

§5.4. Semigroups

Definition: An algebraic system $(A, *)$ is said to be a semigroup iff it satisfies the following conditions:

i/. $*$ is closed on A

ii/. $*$ is associative

Examples

1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z}^+, +)$, $(\mathbb{Q}^+, +)$, and $(\mathbb{R}^+, +)$ are all commutative semigroups.
   $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{Z}^+, \cdot)$, $(\mathbb{Q}^+, \cdot)$, and $(\mathbb{R}^+, \cdot)$ are all commutative semigroups.
   $(\mathbb{R}, -)$ and $(\mathbb{R}-\{0\}, /)$ are not semigroups $\because$ the operations are not associative.
   Let $\mathbb{I} = \mathbb{R} - \mathbb{Q}$.
   $(\mathbb{I}, +)$ and $(\mathbb{I}, \cdot)$ are not semigroups $\because$ the operations are not closed on $\mathbb{I}$ (see Examples 4 and 5 of §5.1).

2) Let $*$ be the operation on $A = \{\alpha, \beta\}$ defined by the right table.

$*$	α	β
α	α	α
β	β	β

   Note that the algebraic system $(A, *)$ here is the same as the one mentioned in Example 5 of §5.2.
   From this example, we conclude that $(A, *)$ is a semigroup.

3) Let $A = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$, and let $\cdot$ denote matrix multiplication.
   Since
$$\begin{pmatrix} 1 & a_1 \\ 0 & b_1 \end{pmatrix}\begin{pmatrix} 1 & a_2 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} 1 & a_2 + a_1b_2 \\ 0 & b_1b_2 \end{pmatrix},$$
   we see that $\cdot$ is closed on A.
   It is known that $\cdot$ is associative.
   $\therefore$ $(A, \cdot)$ is a semigroup.

§5.5. Identity

Definition: Let $(A, *)$ be an algebraic system. An element e of A is called an identity of $(A, *)$ iff $e*x=x*e=x\ \forall x\in A$.

Theorem

If $(A, *)$ has an identity, then it must be unique.

Proof: Suppose e_1 and e_2 are identities of $(A, *)$.
Since e_1 is an identity of $(A, *)$, $e_1*e_2=e_2$. Since e_2 is an identity of $(A, *)$, $e_1*e_2=e_1$.
$\therefore e_2=e_1*e_2=e_1$.

Examples

1) 0 is the identity of $(\mathbb{Z}, +)$ (or $(\mathbb{Q}, +)$ or $(\mathbb{R}, +)$) $\because 0+x=x+0=x\ \forall x\in\mathbb{Z}$.
$(\mathbb{Z}^+, +)$ has no identity $\because$ if the identity exists, then it must be 0 ($\because e+x=x \Rightarrow e=0$); but $0\notin\mathbb{Z}^+$.

2) 1 is the identity of $(\mathbb{Z}, \cdot)$ (or $(\mathbb{Q}, \cdot)$ or $(\mathbb{R}, \cdot)$ or $(\mathbb{Z}^+, \cdot)$) $\because 1\cdot x=x\cdot 1=x\ \forall x\in\mathbb{Z}$.
$(\mathbb{Z}^-, \cdot)$ has no identity $\because 1\notin\mathbb{Z}^-$.

3) Even though $x-0=x\ \forall x\in\mathbb{Z}$, $(\mathbb{Z}, -)$ has no identity $\because 0-x\neq x$ whenever $x\neq 0$.
This example reminds us that we need to consider **both** $e*x$ and $x*e$.

4) Let $A=\left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix}\middle| a, b, c, d\in\mathbb{R}\right\}$, and let $\cdot$ denote matrix multiplication.

Then the matrix $I=\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}$ is the identity of $(A, \cdot)$, i.e. $IM=MI=M$ for all $M\in A$.

This is why $\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}$ is called an identity matrix (of order 2) in matrix theory.

5) Suppose $(A, *)$ has e as the identity. Let x, y, and z be elements of A such that at least one of them is e. Prove that $(x*y)*z=x*(y*z)$.

Proof: Case 1: $x=e$. LHS$=(e*y)*z=y*z$. RHS$=e*(y*z)=y*z$. $\therefore$ LHS$=$RHS.
Case 2: $y=e$. LHS$=(x*e)*z=x*z$. RHS$=x*(e*z)=x*z$. $\therefore$ LHS$=$RHS.
Case 3: $z=e$. LHS$=(x*y)*e=x*y$. RHS$=x*(y*e)=x*y$. $\therefore$ LHS$=$RHS.
In all cases, $(x*y)*z=x*(y*z)$.

Remark This example shows that if an algebraic system $(A, *)$ has an identity e, when we want to determine whether $(A, *)$ is associative, we need only to consider the expressions $(x*y)*z$ and $x*(y*z)$ for those cases in which x, y, and z are all different from e.

§5.6. Monoids

Definition: An algebraic system $(A, *)$ is said to be a monoid iff it satisfies the following conditions:

i/. $*$ is closed on A
ii/. $*$ is associative
iii/. $(A, *)$ has an identity

Examples

1) $(\mathbb{Z}, +)$, $(\mathbb{Z}_+, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{R}, +)$ are all commutative monoids with 0 as the identity.
$(\mathbb{Z}^+, +)$ is a semigroup but not a monoid.

2) $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}^+, \cdot)$, $(\mathbb{Q}, \cdot)$, and $(\mathbb{R}, \cdot)$ are all commutative monoids with 1 as the identity.

3) Let $A=\left\{\begin{pmatrix} 1 & a \\ 0 & b\end{pmatrix}\middle| a, b\in\mathbb{Z}\right\}$, and let $\cdot$ denote matrix multiplication.

From Example 3 of §5.4, we know that $\cdot$ is closed on A and $\cdot$ is associative.

Note that $I=\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}$ is of the form $\begin{pmatrix} 1 & a \\ 0 & b\end{pmatrix}(a, b\in\mathbb{Z})$. That is, $I\in A$.

According to Example 4 of §5.5, I is the identity of $(A, \cdot)$.
Note also that $(A, \cdot)$ is not commutative (see the equation in Example 3 of §5.4).
Conclusion: $(A, \cdot)$ is a non-commutative monoid with I as the identity.

4) Let $A=\left\{\begin{pmatrix}1 & 0\\ 0 & a\end{pmatrix}\middle| a\in\mathbb{Z}\right\}$, and let $\cdot$ denote matrix multiplication.

Since $\begin{pmatrix}1 & 0\\ 0 & a_1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & a_2\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & a_1a_2\end{pmatrix}$, $\cdot$ is closed on A.

It is known that $\cdot$ is associative.

Since $I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\in A$, I is the identity of $(A, \cdot)$.

Further, observe that $\begin{pmatrix}1 & 0\\ 0 & a_1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & a_2\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & a_1a_2\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & a_2a_1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & a_2\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & a_1\end{pmatrix}$.

Conclusion: $(A, \cdot)$ is a commutative monoid with I as the identity.

5) Let $A=\mathbb{R}$, and define a binary operation on A by $a*b=a+b-1$.

Obviously, $*$ is closed on A, and $*$ is commutative.

Since for any $a, b, c\in A$,

$$(a*b)*c=(a+b-1)*c=(a+b-1)+c-1=a+b+c-2$$

and $$a*(b*c)=a*(b+c-1)=a+(b+c-1)-1=a+b+c-2,$$

we see that $*$ is associative.

Since $1*x=x*1=x+1-1=x$ (don't forget $*$ is commutative) for any $x\in A$, 1 is the identity of $(A, *)$.

Conclusion: $(A, *)$ is a commutative monoid with 1 as the identity.

§5.7. Groups

Inverse of an Element

Definition: Let $(A, *)$ be an algebraic system with an identity, say e.
Let $a\in A$. An element $b\in A$ is said to be an inverse of a iff $b*a=a*b=e$.

Theorem

Let $(A, *)$ be an associative algebraic system with e as the identity. Every element of A can have at most one inverse.

Proof: Let $a\in A$. Suppose b_1 and b_2 are inverses of a.
Then $b_2=b_2*e=b_2*(a*b_1)=(b_2*a)*b_1=e*b_1=b_1$.

Group

Definition: An algebraic system $(A, *)$ is said to be a group iff it satisfies the following conditions:

i/. $*$ is closed on A
ii/. $*$ is associative
iii/. $(A, *)$ has an identity
iv/. Every element of A has an inverse

Notes

a/. In what follows, we will mainly consider associative algebraic systems. Due to the above theorem, we can say the inverse of a if it exists. This unique inverse of a (if exists) is denoted by a^{-1}.

b/. A commutative group is also called an abelian group.

Examples

1) $(\mathbb{Z}, +)$ is an abelian group with 0 as the identity, and $-x$ is the inverse of x ($\because (-x)+x=0$) for all $x\in\mathbb{Z}$.
Similarly, $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are abelian groups with 0 the identity, and $-x$ the inverse of x.
However, $(\mathbb{Z}_+, +)$ is a monoid but not a group $\because$ 1 has no inverse (note that $1+x>0$ for all $x\in\mathbb{Z}_+$).

2) $(\mathbb{Z}, \cdot)$ is a monoid with 1 as the identity, but it is not a group $\because$ 2 has no inverse (note that $2x\neq 1$ for all integers x).
$(\mathbb{Q}, \cdot)$ is a monoid (with 1 as the identity) but not a group $\because$ 0 has no inverse (note that $0\cdot x=0\neq 1$ for all rational numbers x).
Actually, for the monoid $(\mathbb{Q}, \cdot)$, 0 is the only element of $\mathbb{Q}$ that has no inverse as we can see from the next example.

3) $(\mathbb{Q}-\{0\}, \cdot)$ is an abelian group because

i/. the product of 2 nonzero rational numbers is still a nonzero rational number (i.e. $\cdot$ is closed on $\mathbb{Q}-\{0\}$);

ii/. it is known that $\cdot$ is associative and commutative;

iii/. 1 is the identity ($1 \in \mathbb{Q}-\{0\}$ and we know already that $1 \cdot x = x \cdot 1 = x \ \forall x \in \mathbb{Q}$);

iv/. if $x \in \mathbb{Q}-\{0\}$, then $\frac{1}{x}$ is defined and is also a nonzero rational number, i.e. $\frac{1}{x} \in \mathbb{Q}-\{0\}$. Since $x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$, $\frac{1}{x}$ is the inverse of x.

§5.8. Subgroups

Definition: Let $(A, *)$ be a group, and let $B \subseteq A$. $(B, *)$ is called a subgroup of $(A, *)$ if $(B, *)$ itself is a group.

Theorem

Let $(A, *)$ be a group with identity e.
Let $B \subseteq A$. Then $(B, *)$ is a subgroup of $(A, *)$ if the following three conditions are satisfied.

a/. $*$ is closed on B

b/. $e \in B$

c/. $b^{-1} \in B$ for all $b \in B$.

Examples

1) Let $(A, *)$ be a group with identity e.
Then, according to the above theorem, $(\{e\}, *)$ and $(A, *)$ are subgroups of $(A, *)$. These two subgroups are called the trivial subgroups of $(A, *)$.

2) Let $B_1 = \{n \in \mathbb{Z} \mid n \text{ is even}\}$, and $B_2 = \{n \in \mathbb{Z} \mid n \text{ is odd}\}$. Is $(B_1, +)$ a group? Is $(B_2, +)$ a group?

Solution: Note that B_1 and B_2 are both subsets of $\mathbb{Z}$, and that $(\mathbb{Z}, +)$ is a group with identity 0.
Since the sum of two even integers is still even, $+$ is closed on B_1.
Since the sum of two odd integers is odd, $+$ is not closed on B_2.
Since 0 is even, $0 \in B_1$ and $0 \notin B_2$.
If x is even, then $-x$ is also even. Thus, $-x \in B_1$ for all $x \in B_1$ (recall that $-x$ is the inverse of x here).
By the above theorem, $(B_1, +)$ is a subgroup of $(\mathbb{Z}, +)$, and hence $(B_1, +)$ itself is a group.
Since $+$ is not closed on B_2, $(B_2, +)$ is not a group.

3) Let $A = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{Q} \right\}$, and let $\cdot$ denote matrix multiplication.

(a) Is $(A, \cdot)$ a group?

(b) If not, find a subset B of A such that $B \neq \{I\}$ (I is the identity matrix) and $(B, \cdot)$ is a group.

Solution: (a) For any $a_1, a_2, b_1, b_2 \in \mathbb{Q}$, we have

$$\begin{pmatrix} 1 & a_1 \\ 0 & b_1 \end{pmatrix}\begin{pmatrix} 1 & a_2 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} 1 & a_2 + a_1 b_2 \\ 0 & b_1 b_2 \end{pmatrix} \quad \text{---------- (1).}$$

From (1), we see that $\cdot$ is closed on A.

It is known that $\cdot$ is associative and $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in A$ is the identity of $(A, \cdot)$.

From (1), we also see that for any $a, b \in \mathbb{Q}$,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix} \neq I .$$

This means that $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, which is an element of A, has no inverse.

$\therefore$ $(A, \cdot)$ is a monoid but not a group.

(b) It is known in matrix theory that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible iff $ad - bc \neq 0$ and in that case,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \text{inverse of} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

$\therefore \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$ has an inverse $\Leftrightarrow 1 \cdot b - a \cdot 0 \neq 0 \Leftrightarrow b \neq 0$. In that case,

$$\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}^{-1} = \frac{1}{b}\begin{pmatrix} b & -a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -a/b \\ 0 & 1/b \end{pmatrix} \quad \text{---------- (2).}$$

Thus it is natural to consider the set $B = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{Q}, \text{ and } b \neq 0 \right\}$.

From (1), we see that $\cdot$ is closed on B.

Obviously $I \in B$.

From (2), we see that $\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}^{-1} \in B$ for all $\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \in B$.

It follows from the subgroup theorem that $(B, \cdot)$ is a group.

Remark Since $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$ (note that these matrices are in B), the group $(B, \cdot)$ mentioned in (b) is non-abelian.

4) Let $A = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{Q}, \text{ and } b \neq 0 \right\}$, and let $\cdot$ denote matrix multiplication. Find a subset B of A such that $B \neq \{I\}$ and $(B, \cdot)$ is an abelian group.

Solution: From the previous example, we know that $(A, \cdot)$ is a non-abelian group.

Let $B = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \middle| b \in \mathbb{Q} \text{ and } b \neq 0 \right\}$.

Since $\begin{pmatrix} 1 & 0 \\ 0 & b_1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & b_1 b_2 \end{pmatrix}$ and $b_1 b_2 \neq 0$ if $b_1 \neq 0$ and $b_2 \neq 0$, $\cdot$ is closed on B and $(B, \cdot)$ is commutative.

Note that $I \in B$.

Note also that if $b \neq 0$ ($b \in \mathbb{Q}$), then $\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1/b \end{pmatrix} \in B$ for all $\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \in B$.

It follows from the subgroup theorem that $(B, \cdot)$ is a group.

Since $(B, \cdot)$ is commutative, $(B, \cdot)$ is an abelian group.

Remark The above answer is not unique.

For example, if $B' = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$, then $(B', \cdot)$ is also an abelian group (exercise).