Section 6.2 Introduction to the Algebraic Group

1. Do the following sets with given binary operations form a group? If it does, give the identity element and the inverse of each element. If it does not form a group, say why.

a) All even integers, addition
Ans: Yes, the identity is 0 and the inverse of $2n$ is $-2n$ for $n \in \mathbb{Z}$.

b) $\{-1,1\}$, multiplication
Ans: Yes, the identity is 1 and the inverse of -1 is -1.

c) All nonzero complex numbers, multiplication
Ans: Yes, the identity is 1 and the inverse of z is $1/z$

d) All nonzero rational numbers, multiplication
Ans: Yes, the identity is 1 and the inverse of p/q is q/p.

e) All positive rational numbers, multiplication
Ans: Yes, the identity is 1 and the inverse of p/q is q/p.

f) The four numbers $1,-1,i,-i$ where $i=\sqrt{-1}$ is the unit complex number, the binary operation is ordinary multiplication.
Ans: Yes, the unit is 1, the inverse of -1 is itself, the inverse of i is $-i$, and the inverse of $-i$ is i.

g) The set of positive irrational numbers together with 1 with the operation of multiplication.
Ans: No, it does satisfy all the properties of a group except closure. The product
$\sqrt{2}\ \sqrt{2}=2$ does not belong to the group.

h) The set of integers under subtraction.
Ans: No, the operation is not associative. That is $a-(b-c)\neq(a-b)-c$.

2. **(Odd Integers Under Addition)** Give two reasons why the odd integers under addition do not
constitute a group?

Ans: No identity and not closed under addition; i.e 1 + 3 = 4 is not in the group.

3. **(Finish the Group)** Complete the following Cayley table for a group of order three.

$*$	e	a	b
e	e	a	b
a	a		
b	b		

Ans:

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

4. **(Finish the Group)** Complete the following Cayley table for a group of order four without looking at the Cayley tables of the Klein 4- group or the cyclic group of order 4 in the text.

$*$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

Ans: The cyclic group of order 4 and the Klein 4-group are given in the text.

5. **(Verification of a Group)** Do the nonzero integers with the operation of multiplication form a group?
Ans: No, integers other than 1 and -1 do not have inverses.

6. **(Group You are Well Familiar)** Show that $\{\mathbb{Z},+\}$ is a group (i.e. the integers with the operation of addition) is a group.
Ans: We leave this simple demonstration for the reader.

7. **(Property of a Group)** Verify that for all elements a,b in a group the identity $(ab)^{-1}=b^{-1}a^{-1}$ holds. Hint: Show that $(ab)\left(b^{-1}a^{-1}\right)$ is the identity.

Ans: Since $(ab)\left(b^{-1}a^{-1}\right)=a\left(bb^{-1}\right)a^{-1}=aea^{-1}=aa^{-1}=e$ this means ab is the inverse of $b^{-1}a^{-1}$, which we write as $(ab)^{-1}=b^{-1}a^{-1}$.

8. **(General Properties of Groups)** Show that a group has exactly one identity.
Ans: If e and f are two identities for a group. Then $e=ef=f$.

9. **(More General Properties of Groups)** Show that every element in a group has no more than one inverse.
Ans: Suppose an element a of the group has has two inverses l and r. Then we have $l = le = l(ar) = (la)r = er = r$.

10. **(Heisenberg Group)** A group that plays an important role in quantum mechanics is the Heisenberg group which consists of matrices of the form

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

where x, y, z are real numbers and the group operation matrix multiplication. Show this is a group.

Ans: The product of two upper-triangular matrices with 1s down the diagonal is

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+x' & y+y'+xz' \\ 0 & 1 & z+z' \\ 0 & 0 & 1 \end{pmatrix}$$

which has the desired form. The 3×3 identity matrix belongs to the set of upper triangular matrices with 1s down the diagonal ($x = y = z = 0$) and plays the role of the identity element of the group. Also every matrix in the set has a unique inverse since the determinant of each member of the group is 1, and the inverse of an upper triangular matrix with 1's down the diagonal is

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix}$$

which has the desired form.

11. **(Direct Product of Groups)** When we think of the real numbers $\mathbb{R}$ as a set, then the cartesian product $\mathbb{R}\times\mathbb{R} = \{(x, y) : x \in \mathbb{R}, y \in \mathbb{R}\}$ as the set. However, if we think of $\mathbb{R}$ as a group with a the group operation, say addition, then the **direct product**[1] $\mathbb{R}\times\mathbb{R} = \{(x, y) : x \in \mathbb{R}, y \in \mathbb{R}\}$ is *still* a set, but now it is a group where we define the group operation $\oplus$ as $(a,b)\oplus(c,d) = (a+c, b+d)$. Define the direct product of the

[1] Although the group operation is addition, we still call $\mathbb{R}\times\mathbb{R}$ the direct product.

group $\mathbb{Z}_2=\{0,1\}$ with itself as $\mathbb{Z}_2^2=\mathbb{Z}_2\times\mathbb{Z}_2=\{(a,b):a,b\in\mathbb{Z}_2\}$ where the binary operation is defined as $(a,b)\oplus(c,d)=(a+c,b+d)$. Show that $\mathbb{Z}_2\times\mathbb{Z}_2$ is a group under this operation. This group and other direct sums of groups play an important role in coding theory.

Ans: The direct product (or sum) $\mathbb{Z}_2\times\mathbb{Z}_2$ consists of the four pairs of binary numbers

$$\mathbb{Z}_2\times\mathbb{Z}_2=\{(a,b):a,b\in\mathbb{Z}_2\}=\{(0,0),(0,1),(1,0),(1,1)\}$$

We can construct the addition table for $\mathbb{Z}_2\times\mathbb{Z}_2$ (using mod 2 arithmetic).

$\oplus$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

We can see from this Cayley table the direct sum is a group. Note if we associate $e=(0,0)$, $R_{180}=(0,1)$, $V=(1,0)$, $H=(1,1)$ we see this group is isomorphic (the same) to the Klein 4-group.

12. **(Mod 3 Multiplication)** Create the multiplication table for the integers 1,2 where multiplication defined as $\text{mod}(3)$ arithmetic.

Ans:

$\otimes$	1	2
1	1	2
2	2	1

13. **(Mod 4 Multiplication)** Create the multiplication table for the integers 1,2,3 for modular arithmetic $\text{mod}(4)$ and show that this does not define a group. In other that the numbers $1,2,...,n-1$ forms a group under $\text{mod}(n)$ multiplication, it must be true that n is a prime number.

Ans: The multiplication is not closed since $2\cdot 2=0$ which is not in the group.

$\otimes$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

14**. (Mod 5 Multiplication)** Create the multiplication table for the integers 1,2,3,4 where multiplication defined as $\mathrm{mod}(5)$ arithmetic.

Ans:

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

15. **(Relative Prime Group $U(10)$)** For each positive integer n the set of positive integers 1,2,…, n that are relatively prime[2] with n is denoted by $U(n)$. For example, $U(10)=\{1,3,7,9\}$. The set $U(n)$ is a group under multiplication modulo n.

a) Draw the Cayley table for $U(10)$.
b) Is the group Abelian?
c) What is the inverse of each element?

Ans: a)

$\otimes$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

b) The group is Abelian.
c) The inverse of 1 is 1, the inverse of 9 is itself, and 3 and 7 are inverses of each other.

13. **(Relative Prime Group $U(8)$**
For each positive integer n the set of positive integers 1,2,…, n that are relatively prime with n is denoted by $U(n)$. For example, $U(8)=\{1,3,5.7\}$. The set $U(n)$ is a group under multiplication modulo n.

d) Draw the Cayley table for $U(8)$.
e) Is the group Abelian?
f) What is the inverse of each element?

[2] Two numbers are relatively prime if and only if the greatest common divisor of both numbers is 1

Ans: a)

$\otimes$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

b) The group is abelian.
c) Every element of the group is its own inverse. The group is isomorphic to the Klein 4-group.

14. **(Isomorphic Groups)** Show that Group C and Group D are isomorphic by interchanging the 3rd and 4th columns of C, and then the 3rd and 4th rows to get D.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Group C

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Group D

Ans: Simply carry out the operations. Make sure you relabel the members of the group when you are done; the 0 is renamed 1, 1 is renamed 2, and 3 and 4 are interchanged.

15. **(Infinite Group)** Show that the set of all rational numbers x in the interval $x \in [0,1)$ forms an infinite group if the group operation is defined as

$$x + y = \begin{cases} x + y & \text{if } 0 \le x + y < 1 \\ x + y - 1 & \text{if } x + y \ge 1 \end{cases}$$

Ans: The group identity is 0. The reminder of the axioms are straightforward to verify.

16. **(Groups and Latin Squares)** The Cayley table for a group forms what is called a **Latin square.** That is, every element of the group occurs exactly once in each row and exactly once in each column. The converse is not true however, there are Latin squares that do not form groups. Find a Latin square for the numbers $\{0,1,2\}$ that do not form a group.

Ans: The following Latin square does not form a group since it does not contain an identity element**.**

$\otimes$	0	1	2
0	1	2	0
1	0	1	2
2	2	0	1

17. **(Modular Fun)** Compute the following sums and products in the cyclic group $\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$.

a) $\mathbb{Z}_4$: $1+7$ and 3×7
b) $\mathbb{Z}_5$: $9+7$ and 5×7
c) $\mathbb{Z}_6$: $10+7$ and 2×7
d) $\mathbb{Z}_9$: $11+20$ and 3×7
e) $\mathbb{Z}_{10}$: $100+7$ and 30×10
f) $\mathbb{Z}_{11}$: $11+11$ and 11×7
g) $\mathbb{Z}_{11}$: $12+7$ and 10×10
h) $\mathbb{Z}_{15}$: $14+1$ and 3×6

Ans:

a) $\mathbb{Z}_4$: $1+7=0,\ 3\times 7=1$
b) $\mathbb{Z}_5$: $9+7=1,\ 5\times 7=0$
c) $\mathbb{Z}_6$: $10+7=5,\ 2\times 7=2$
d) $\mathbb{Z}_9$: $11+20=4,\ 3\times 7=3$
e) $\mathbb{Z}_{10}$: $100+7=7,\ 30\times 10=0$
f) $\mathbb{Z}_{11}$: $11+11=0,\ 11\times 7=0$
g) $\mathbb{Z}_{11}$: $12+7=8,\ 10\times 10=1$
h) $\mathbb{Z}_{15}$: $14+1=0,\ 3\times 6=3$

18. **(Modular Group)** The set of all 2×2 matrices

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

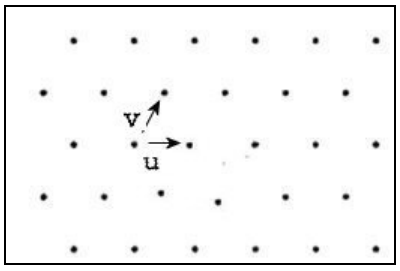
whose entries are all integers and whose determinant $|A|=ad-bc$ with group operation matrix multiplication is called the **modular group** and plays an important role in many areas of mathematics. One reason for its importance is that it is the symmetry group for 2-dimensional **lattices**, which are infinitely large wire meshes which are all vectors of the form $a\hat{u}+b\hat{v}\in\mathbb{R}^2$ where $\hat{u},\hat{v}$ are two fixed basis vectors (each pair of basic vectors determines a mesh) and a,b range over the integers .

a) Draw the mesh for the basis vectors $\hat{u}=(1,0),\hat{v}=(1,1)$.
b) Show that the member of the modular group

$$\begin{bmatrix} 1 & 3 \\ 0 & 2 \end{bmatrix}$$

distorts the plane but is a symmetry for the mesh; i.e. it maps the mesh into itself.

Ans: a)



b) Grid points can be represented by

$$a\begin{pmatrix}1\\0\end{pmatrix}+b\begin{pmatrix}1\\1\end{pmatrix}=(a+b)\begin{pmatrix}2\\1\end{pmatrix}=c\begin{pmatrix}2\\1\end{pmatrix}$$

where c is an integer. Multiplying this vector by A gives

$$\begin{aligned}(a+b)\begin{bmatrix}1&3\\0&2\end{bmatrix}\begin{pmatrix}2\\1\end{pmatrix}&=(a+b)\begin{pmatrix}5\\2\end{pmatrix}\\&=(a+b)\left[3\begin{pmatrix}1\\0\end{pmatrix}+2\begin{pmatrix}1\\1\end{pmatrix}\right]\\&=(3a+3b)\begin{pmatrix}1\\0\end{pmatrix}+(2a+2b)\begin{pmatrix}1\\1\end{pmatrix}\end{aligned}$$

which is a point in the lattice. The matrix A distorts the plane as can be seen from the fact it maps the unit square with opposite corners $(0,0),(1,1)$ into a non-square parallelogram.

ΟΠΧΝΞΩΨ