5 Group theory

This section is an introduction to abstract algebra. This is a very useful and important subject for those of you who will continue to study pure mathematics.

5.1 Binary operations

5.1.1 Definition and examples

Throughout mathematics, we encounter the following situation: We have a set S, and there is a rule that combines two elements in the set to produce a new element. Let us look at a number of examples:

Example 52. One of the simplest and most well-known examples is perhaps the following. We consider the set $\mathbb{Z}$ and the operation of addition. Using this operation, the numbers 2 and 5 can be combined to give the number 7; the numbers 8 and 3 can be combined to give the number 11, and so on.

Example 53. We could also take the same set $\mathbb{Z}$, and consider the operation of multiplication, or the operation of subtraction.

Example 54. To take a different example, consider the set $M_{2\times 2}$ of 2×2 matrices, with real entries. Two such matrices can be multiplied to produce a new 2×2 matrix.

We make the following definition:

Definition 18. A *binary operation* on a set S is a function from $S \times S$ to S.

(Recall that $S \times S$ is the set of all ordered pairs of elements of S.)

Example 55. The operation of addition is a binary operation on $\mathbb{R}$. It is also a binary operation on $\mathbb{N}$, and also on the set of complex numbers $\mathbb{C}$. It is also a binary operation on the set P_2 of polynomials of degree at most 2. In fact, addition is a binary operation on any vector space.

Example 56. The operation of multiplication is a binary operation on $\mathbb{Z}$. It is also a binary operation on $\mathbb{N}$, and on $\mathbb{R}$, and on $\mathbb{C}$.

Example 57. Consider the set of positive real numbers, which we denote by $\mathbb{R}^+$. The operation of division is a binary operation on this set.

Example 58. Let A be any set, and let S be the set of all functions from A to A. Given two elements f and g of S, we can consider the composition $f \circ g$. Since this is again an element of S, we see that the operation of composition is a binary operation on S.

Example 59. We can define our own binary operations. For example, we can define a binary operations on the set $\mathbb{Z}$ be the formula

$$a * b = ab + 2$$

With this definition, we can compute that $4 * 3 = 14$ and $5 * (-2) = -8$.

Example 60. On the set $\mathbb{Z}$, we can define a binary operation by

$$a * b = \min(a, b)$$

(this means the smallest of a and b, or if they are equal, the common value of a and b.) We can compute

$$\begin{aligned} 5 * 2 &= 2 \\ 10 * 10 &= 10 \\ (-1) * 5 &= -1 \\ 75 * 95 &= 75 \end{aligned}$$

Example 61. Another possible binary operation on $\mathbb{Z}$ is the following:

$$a * b = b$$

In this case we can compute

$$\begin{aligned} 12 * 8 &= 8 \\ 10 * 10 &= 10 \\ (-1) * 5 &= 5 \\ 75 * 95 &= 95 \end{aligned}$$

Example 62. Define a binary operation on $\mathbb{Z}$ by

$$a * b = 3$$

We can compute

$$\begin{aligned} 5 * 2 &= 3 \\ 10 * 10 &= 3 \\ (-1) * (-8) &= 3 \\ 75 * 95 &= 3 \end{aligned}$$

Example 63. We can define a binary operation on the set of points in the plane $\mathbb{R}^2$ as follows: If P and Q are two points, we let $P * Q$ be the midpoint of the segment PQ.

Example 64. On the ring $\mathbb{Z}_n$ defined earlier in the course, we have two binary operations: multiplication mod n and addition mod n.

5.1.2 Examples that are NOT binary operations

There are many examples that look like binary operations but still fail to fit in the definition above. It is important that you understand the following examples, and why they are NOT binary operations[2].

Example 65. Consider the operation of subtraction on the set $\mathbb{N}$ of natural numbers. This is NOT a binary operation, because when you take one natural number minus another one, you don't always get a natural number. For example, $4 - 9$ is not a natural number, because it is negative.
The problem with this operation is that although it is defined for every element of $\mathbb{N} \times \mathbb{N}$, the result does not always lie in $\mathbb{N}$. Remember that a binary operation on $\mathbb{N}$ is a function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$.

Example 66. Consider the set of real numbers $\mathbb{R}$, and the operation of division. This is NOT a binary operation, because it is not defined for every ordered pair in $\mathbb{R} \times \mathbb{R}$. (You cannot divide by zero).

Example 67. Consider the set of all matrices with real entries (of any size). The operation of addition is NOT a binary operation on this set, because you can not always add two matrices (it only works if they are of the same size).

Example 68. Consider again the set $\mathbb{Z}$. If we say that "$a*b$ is some number larger than both a and b", we have NOT defined a binary operation, because the definition is not precise. (What is the value of $5 * 4$?)

5.1.3 Exercises

Do the following rules define a binary operation on the set $\mathbb{Z}$?
E223 $a * b = a - b$
E224 $a * b = a/b$
E225 $a * b = b^2$
E226 $a * b = \frac{a+b}{2}$
E227 $a * b = -1000$

5.1.4 Properties that binary operations can have

In order to study binary operations in a systematic way, we introduce some definitions. In each definition, we consider a binary operation $*$ on a set S.

Definition 19. The binary operation $*$ is called *commutative* if

$$a * b = b * a$$

for all a and b in S.

[2]I might have made a terrible mistake in the lecture. If I told you that $a * b = \frac{ab}{2}$ defines a binary operation on $\mathbb{Z}$, I lied to you, because this expression is not always an integer. It should be $\mathbb{R}$ instead of $\mathbb{Z}$.

Definition 20. The binary operation $*$ is called *associative* if

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

for all a, b, c in S.

Definition 21. An *identity element* for the binary operation $*$ is an element $e \in S$ such that

$$a * e = a \qquad \text{and} \qquad e * a = a$$

for all a in S.

Definition 22. Let $*$ be a binary operation with an identity element e. An *inverse* to an element $b \in S$ is an element $x \in S$ with the property that

$$b * x = e \qquad \text{and} \qquad x * b = e$$

Let us take some examples.

Example 69. Consider the operation $+$ on the set $\mathbb{Z}$. This operation is commutative and associative. It has an identity element, namely 0. Also, every element has an inverse: the inverse of n is the number $-n$.

Example 70. Consider the operation of multiplication on the set $\mathbb{Z}$. This operation is commutative and associative. The operation also has an identity element, namely 1. However, every element does NOT have an inverse. In fact only the elements 1 and -1 have inverses. (1 is the inverse of 1, and -1 is the inverse of -1.)

Example 71. Consider the operation of multiplication on the set $\mathbb{R}$. It is commutative, associative and has an identity element. Every element except 0 has an inverse. (The inverse of a is $\frac{1}{a}$.)

Example 72. Consider the operation of matrix multiplication on the set $M_{2\times 2}$. This binary operation is associative, but NOT commutative. There is an identity element (the identity matrix). Not all elements have an inverse: only the invertible matrices do.

Example 73. Consider the operation on $\mathbb{Z}$ given by

$$a * b = ab - 1$$

Is it associative? To check, we compute

$$a * (b * c) = a * (bc - 1) = abc - a - 1$$

and

$$(a * b) * c = (ab - 1) * c = abc - c - 1$$

so the operation is NOT associative, since these two expressions are not in general equal.
Is the operation commutative? Yes, because

$$ab - 1 = ba - 1$$

for all a and b in $\mathbb{Z}$.
Is there an identity element? This would be an element e such that

$$ea - 1 = a$$

for all $a \in \mathbb{Z}$. This equation can be rewritten as

$$e = \frac{a+1}{a}$$

which clearly cannot be satisfied for all a at once. (In fact, it cannot be satisfied at all when $a = 0$.)
Since the operation does not have an identity element, it doesn't make any sense to ask about if any element has an inverse, since the concept of inverse cannot be defined.

Example 74. We consider the binary operation on $\mathbb{Z}$ given by

$$a * b = \min(a, b)$$

This operation is clearly commutative. It is also associative because $(a*b)*c$ and $a*(b*c)$ are both equal to the smallest of a, b and c. Does the operation have an identity element? Suppose that e is an identity element. Then we would have

$$\min(a, e) = a$$

for all elements a. In other words, we would have $e \geq a$ for every integer a. Clearly there is no such integer e, so there is no identity element for this operation.

Example 75. We define a binary operation on $\mathbb{R}$ by

$$a * b = \frac{ab}{3}$$

This is clearly commutative. Is it associative? We compute

$$a * (b * c) = a * (\frac{bc}{3}) = \frac{abc}{9}$$

and

$$(a * b) * c = (\frac{ab}{3}) * c = \frac{abc}{9}$$

so the operation is associative.
Is there an identity element? This would be an element e such that

$$\frac{ae}{3} = a$$

for all $a \in \mathbb{R}$. We see that $e = 3$ satisfies this condition, so 3 is an identity element.
Which elements have an inverse? An inverse to the element a is an element x such that

$$\frac{ax}{3} = 3$$

in other words, such that $ax = 9$. Hence every element except 0 has an inverse: the inverse of a is $\frac{9}{a}$.

5.1.5 Closedness

Definition 23. Let S be a set with a binary operation $*$, and let T be a subset of S. We sat that T is *closed* under the binary operation, if whenever t_1 and t_2 are in T, then $t_1 * t_2$ is also in T.

Example 76. Consider the set $\mathbb{R}$ with the binary operation of addition. The subset $\mathbb{Z}$ is closed under addition, because the sum of two integers is always an integer. The subset $\mathbb{Z}^+$ is also closed under addition, because the sum of two positive integers is always a positive integer. However, the subset $\mathbb{P}$ (the set of all prime numbers) is NOT closed under addition, because the sum of two primes is not always a prime.

Example 77. Consider the set $M_{2\times 2}$, with the binary operation of matrix multiplication. The set of invertible matrices is closed under this operation, because the product of two invertible matrices is again invertible.

5.1.6 Exercises

On the set $\mathbb{Z}$, we consider the binary operation $a * b = a - b$.
E228 Is this operation commutative?
E229 Is this operation associative?
E230 Does the operation have an identity element?
E231 If the operation has an identity element, which elements have an inverse?
E232 Is the set of even integers closed under this operation?
E233 Is the set of positive integers closed under this operation?
E234 Is the set of prime numbers closed under this operation?
Consider the binary operation in Example 59.
E235 Is this operation commutative?
E236 Is this operation associative?
E237 Does the operation have an identity element?

E238 If the operation has an identity element, which elements have an inverse?
E239 Is the set of even integers closed under this operation?
E240 Is the set of positive integers closed under this operation?
E241 Is the set of prime numbers closed under this operation?
Consider the binary operation in Example 61.
E242 Is this operation commutative?
E243 Is this operation associative?
E244 Does the operation have an identity element?
E245 If the operation has an identity element, which elements have an inverse?
E246 Is the set of even integers closed under this operation?
E247 Is the set of positive integers closed under this operation?
E248 Is the set of prime numbers closed under this operation?
Consider the binary operation in Example 62.
E249 Is this operation commutative?
E250 Is this operation associative?
E251 Does the operation have an identity element?
E252 If the operation has an identity element, which elements have an inverse?
E253 Is the set of even integers closed under this operation?
E254 Is the set of positive integers closed under this operation?
E255 Is the set of prime numbers closed under this operation?

5.1.7 Problems

Consider the binary operation in Example 63.
P26 Is this operation commutative?
P27 Is this operation associative?
P28 Does the operation have an identity element?
P29 If the operation has an identity element, which elements have an inverse?
P30 Let S be the set of points on the line $2x + y = 1$. Is this set closed under the operation?
P31 Is the set of points with integer coordinates closed under this operation?
P32 Is the set of points (x, y) such that $x > 0$ closed under this operation?
Consider the binary operation in Example 58.
P33 Is this operation commutative?
P34 Is this operation associative?
P35 Does the operation have an identity element?
P36 If the operation has an identity element, which elements have an inverse?
P37 Is the set of injective functions closed under this operation?

P38 Is the set of bijective functions closed under this operation?

5.2 Groups: definition and examples

Definition 24. A set S with a binary operation $*$ is called a *group* if the following conditions are satisfied:

- The operation $*$ is associative
- The operation $*$ has an identity element
- Every element of S has an inverse

Definition 25. A group is called *abelian* if the group operation is commutative.

If the group operation is addition, we speak of an *additive* group (this can be addition of numbers, of matrices, of functions, of vectors, etc). If the group operation is some kind of multiplication, we speak of a *multiplicative* group. An additive group is always abelian (this is an unwritten agreement between all mathematicians) but a multiplicative group can be either abelian or nonabelian, depending on the situation.

5.2.1 Examples of groups

Example 78. The set $\mathbb{Z}$, with the operation of addition, is a group. Same is true for the set $\mathbb{R}$ and the set $\mathbb{C}$. However, the set $\mathbb{N}$ is NOT a group under addition, because not every element has an inverse in $\mathbb{N}$.

Example 79. The set $\mathbb{Z}_n$ is a group, with the operation of addition mod n.

Example 80. The set $\mathbb{Z}_n^*$ is a group, with the operation of multiplication mod n.

Example 81. Let A be any set, and let G be the set of bijective functions from A to A. Then G is a group under the operation of composition. If A is a finite set with n elements, the resulting group G is called the *symmetric group* S_n. A bijective function from a finite set to itself is called a *permutation*. A group in which the elements are permutations is called a *permutation* group.

Example 82. We write $GL_2(\mathbb{R})$ for the set of all invertible 2×2 matrices with real entries. This set is a group under matrix multiplication. The letters GL is an abbreviation of "general linear group".

Example 83. We write $SL_2(\mathbb{R})$ for the set of all 2×2 matrices with determinant equal to 1. This set is also a group under matrix multiplication. The letters SL is an abbreviation of "special linear group".

Example 84. The last two examples are examples of so called *Lie groups* (pronounced Lee groups). These groups are very interesting objects, and the focus of much current research. We can also define $GL_n(\mathbb{R})$, as the set of all invertible $n \times n$ matrices, and $SL_n(\mathbb{R})$ as the set of all $n \times n$ matrices with determinant 1, and there are also many other similar groups of matrices, with real or complex entries.

Example 85. Given a geometric object, for example a cube or a rectangular card, we can study the group of *symmetries* of the object.

Example 86. Given any group, we can construct many new groups from it. For example, there is the center of a group, the automorphism group of a group, and the direct product of a group with itself.

5.2.2 Exercises

E256 Check that the set $\mathbb{Z}$ is a group under addition.
E257 Check that the set of positive real numbers is a group under multiplication.
E258 Check that the set $GL_2(\mathbb{R})$ is a group under matrix multiplication.
E259 Is the set $\mathbb{Z}$ a group under the binary operation $a * b = a + b + 1$?
E260 Is the set $M_{2\times 2}$ a group under matrix addition?
E261 Is the set $\mathbb{Z}$ a group under multiplication?

5.3 Answers and solutions

E223 Yes. **E224** No. **E225** Yes. **E226** No. **E227** Yes.
E228 No. **E229** No. **E230** No. There are two conditions on an identity element. The number 0 satisfies one condition but not the other. **E232** Yes.
E233 No. **E234** No.
E235 Yes. **E236** No. **E237** No. **E239** Yes. **E240** Yes. **E241** No.
E242 No. **E243** Yes. **E244**. No. **E246** Yes. **E247** Yes. **E248** Yes.
E249 Yes. **E250** Yes. **E251** No. **E253** No. **E254** Yes. **E255** Yes.
E256 The sum of two integers is an integer, so addition is a binary operation on $\mathbb{Z}$. Addition of integers is associative. The number 0 is the identity element. The inverse of n is $-n$.
E257 The product of two positive real numbers is a positive real number, so we have a binary operation. Multiplication of real numbers is associative. The number 1 is the identity element. The inverse of a is $\frac{1}{a}$.
E258 The product of two invertible matrices is invertible, so we have a binary operation. Matrix multiplication is associative. The identity matrix is the identity element for matrix multiplication. By definition, every invertible matrix has an inverse.
E259 Yes. The operation is associative. The identity element is -1. The inverse of n is $(-2 - n)$.

E260 Yes. The operation is associative. The identity element is the zero matrix, and the inverse of a matrix A is the matrix $-A$.
E261 No. The operation is associative and the number 1 is the identity element, but not every element has an inverse.
P26 Yes. **P27** No. **P28** No.
P30 Yes. If you take two points P, Q on a line, the midpoint of PQ is also on that line.
P31 No. Take for example the points $(0, 0)$ and $(1, 1)$.
P32 Yes.
P33 No. **P34** Yes. **P35** Yes. **P36** The bijective functions. **P37** Yes. (See Problem 4). **P38** Yes. The composite of two bijective functions is also bijective.

5.4 Some basic group theory

This part of the course is covered in the lectures by Mr Nkuubi, so I refer to his lectures for the details. This part of the course will also be on the exam, although it is not in these notes! You are expected to understand the definitions and basic properties of the following concepts:

- Order of an element in a group
- Order of a group
- Homomorphism
- Isomorphism
- Kernel of a homomorphism
- Image of a homomorphism
- Subgroup
- The cyclic subgroup generated by an element
- Coset

I promised earlier in the course that I would prove Euler's theorem, using a general theorem from group theory. Let me give this proof. The general theorem is the following:

Theorem 29 (Lagrange's theorem)**.** Let G be a finite group, and let H be a subgroup of G. Then the order of H divides the order of G.

An immediate consequence of Lagrange's theorem is the following:

Corollary 2. Let G be a finite group of order g. Let e be the identity element of G. Then for every element a of G, we have $a^g = e$.

Proof. Let f be the order of the element a. This is also the order of the cyclic subgroup generated by a. By Lagrange's theorem, f divides g, so $g = nf$ for some positive integer n. We have

$$a^f = e$$

by definition of f. Raising both sides to n gives

$$a^g = e$$

which completes the proof. □

We now recall the formulation of Euler's theorem:
Theorem: Let $n \geq 2$ be an integer, and let a be a positive integer coprime to n. Then the following congruence holds:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Proof. Let r be the remainder when a is divided by n. Since $a \equiv r \pmod{n}$, we also have that

$$a^{\varphi(n)} \equiv r^{\varphi(n)}$$

To prove the theorem, it is sufficient to prove that

$$r^{\varphi(n)} = 1$$

in the ring $\mathbb{Z}_n$. The number a is coprime to n, so r is also coprime to n. Therefore r is in the group $\mathbb{Z}_n^*$. The order of this group is $\varphi(n)$, so be the Corollary above, we can conclude that

$$r^{\varphi(n)} = 1$$

in the group $\mathbb{Z}_n^*$, and hence also in the ring $\mathbb{Z}_n$. □

THE COURSE NOTES END HERE. ALL THE BEST FOR THE EXAM!