FFHS - Fernfachhochschule Schweiz
BsC in Cyber Security

2024

Discrete Mathematics

David

Table of contents

1 Glossary of Mathematical Symbols

This is a glossary of the mathematical symbols used in this document.

1.1 Set Theory

Symbol	Usage	Interpretation
$\emptyset$	$\{\}$	The empty set
$\{\}$	$\{a, b, c...\}$	A set containing elements a, b, and c (and so on)
$\mid$	$\{a \mid T(a)\}$	The set of all a such that $T(a)$ is true
$:$	$\{a : T(a)\}$	The set of all a such that $T(a)$ is true

1.2 Set Operations

Symbol	Usage	Interpretation
$\cup$	$\{A \cup B\}$	The union of sets A and B
$\cap$	$\{A \cap B\}$	The intersection of sets A and B
$\uplus$	$\{A \uplus B\}$	Union of disjoint sets A and B

1.3 Set Relations

Symbol	Usage	Interpretation
$\in$	$\{a \in A\}$	The element a is in the set A
$\notin$	$\{a \notin A\}$	The element a is not in the set A
$\subset$	$\{A \subset B\}$	The set A is a subset of the set B
$\subseteq$	$\{A \subseteq B\}$	The set A is a subset of or equal to the set B
$\neq$	$\{A \neq B\}$	The set A is not equal to the set B

1.4 Blackboard bold

Symbol	Interpretation
$\mathbb{N}$	The set of natural numbers
$\mathbb{Z}$	The set of integers
$\mathbb{Z}p$	The set of integers where p is a prime number

1.5 Equality, equivalence and similarity

Symbol	Usage	Interpretation
$=$	$a = b$	The elements a and b are equal
$\neq$	$a \neq b$	The elements a and b are not equal
$\equiv$	$a \equiv b$	The elements a and b are equivalent
$\not\equiv$	$a \not\equiv b$	The elements a and b are not equivalent

1.6 Comparison

Symbol	Usage	Interpretation
$<$	$a < b$	The element a is less than b
$>$	$a > b$	The element a is greater than b
$\leq$	$a \leq b$	The element a is less than or equal to b
$\geq$	$a \geq b$	The element a is greater than or equal to b

1.7 Divisibility

Symbol	Usage	Interpretation
$\mid$	$a \mid b$	The element a divides b
$\nmid$	$a \nmid b$	The element a does not divide b

1.8 Relations

Symbol	Usage	Interpretation
$\circ$	$R \circ S$	The composition of relations R and S
$\leq$	$a \leq b$	Order relation between elements a and b
$\sim$	$a \sim b$	Equivalence relation between elements a and b
$[]$	$[a]$	The equivalence class of element a
$^{-1}$	R^{-1}	The inverse of relation R
$^{+}$	R^{+}	The transitive closure of relation R
*	R^{*}	The reflexive-transitive closure of relation R

1.9 Logical Operators

Symbol	Usage	Interpretation	Colloquially
$\wedge$	$a \wedge b$	The logical conjunction of a and b	Both a and b
$\vee$	$a \vee b$	The logical disjunction of a and b	Either a or b or both
$\neg$	$\neg a$	The logical negation of a	Not a
$\Leftrightarrow$	$a \Leftrightarrow b$	The logical implication from a to b and b to a	If a then b and if b then a
$\Rightarrow$	$a \Rightarrow b$	The logical implication from a to b	If a then b

1.10 Quantifiers

Symbol	Usage	Interpretation
$\forall$	$\forall a$	For all elements a
$\exists$	$\exists a$	There exists an element a
$\exists!$	$\exists! a$	There exists exactly one element a
$\nexists$	$\nexists a$	There does not exist an element a

2 Relation

2.1 Cartesian product

The Cartesian product of two sets A and B is the set of all ordered pairs (a, b) where a is an element of A and b is an element of B.
$A * B = \{(a, b) \mid a \in A \land b \in B\}$

The Cartesian product of the sets $A = \{1, 2\}$ and $B = \{3, 4\}$ is:
$A * B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$.

A relation R from a set A to a set B is a subset of the Cartesian product $A * B$.
$R \subseteq A * B$

Let $A = \{1, 2\}$ and $B = \{3, 4\}$. The relation $R = \{(1, 3), (2, 4)\}$ is a relation from A to B.

For $(a, b) \in R$, we write aRb, and say that a is in relation R to b.

2.2 Inverse relation

The inverse relation $R^{\{-1\}}$ of a relation R is the relation that contains the ordered pairs of R in reverse order.
$R^{\{-1\}} = \{(b, a) \mid (a, b) \in R\}$

Let $R = \{(1, 3), (2, 4)\}$. The inverse relation $R^{\{-1\}}$ is:
$R^{\{-1\}} = \{(3, 1), (4, 2)\}$.

2.3 Composition of relations

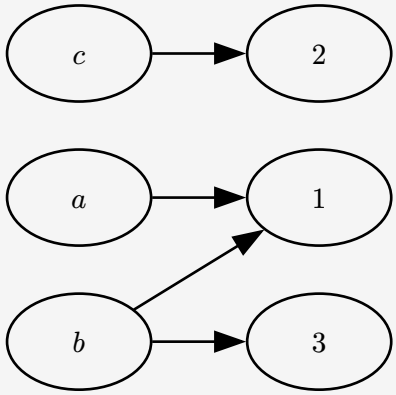
Given the relation $R \subseteq A * B$ and $S \subseteq B * C$, the composition of $R \circ S$ is the relation from A to C defined by:

$R \circ S = \{(a, c) \mid \exists b \in B, (a, b) \in R \land (b, c) \in S\}$

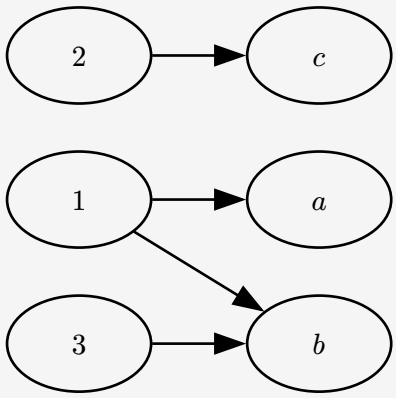
2.4 Representation of relations

Relations can be represented in different ways, one way is by using a directed graph.

$R = \{(a,1),(b,1),(b,3),(c,2)\} \subseteq A * B$ when $A = \{a,b,c\}$ and $B = \{1,2,3\}$.



or $R^{\{-1\}} = \{(1,a),(1,b),(3,b),(2,c)\}$.



2.5 Relations $R \subseteq A * A$

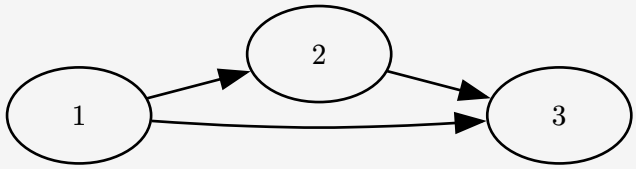
Relations that are subsets of the Cartesian product of a set with itself are called relations on the set. They can have the following properties:

Reflexive: $(a, a) \in R \forall a \in A$.

The relation $R = \{(1, 1), (2, 2)\} \subseteq A * A$ is reflexive.

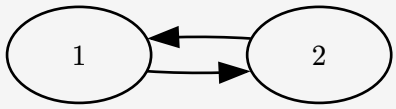
Transitive: $\forall a, b, c \in A, (a, b) \in R \land (b, c) \in R \Rightarrow (a, c) \in R$.

The relation $R = \{(1, 2), (2, 3), (1, 3)\} \subseteq A * A$ is transitive.



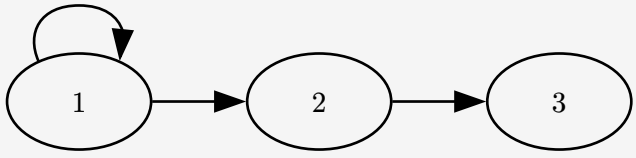
Symmetric: $\forall a, b \in A, (a, b) \in R \Rightarrow (b, a) \in R$.

The relation $R = \{(1, 2), (2, 1)\} \subseteq A * A$ is symmetric.



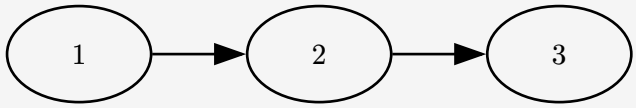
Antisymmetric: $\forall a, b \in A, (a, b) \in R \land (b, a) \in R \Rightarrow a = b$.
or equivalently: $\forall a, b \in A, (a, b) \in R \land a \neq b \Rightarrow (b, a) \notin R$.

The relation $R = \{(1, 2), (2, 3), (1, 1)\} \subseteq A * A$ is antisymmetric.



Asymmetric: $\forall a, b \in A, (a, b) \in R \Rightarrow (b, a) \notin R$.

The relation $R = \{(1, 2), (2, 3)\} \subseteq A * A$ is asymmetric.



A relation R on a set A is called an equivalence relation if it is **reflexive**, **symmetric**, and **transitive**.
For $(a, b) \in R$, we say that a is **equivalent** to b and write $a \equiv b$.

2.6 Equivalence classes

Given an equivalence relation R on a set A, the equivalence class of an element $a \in A$ is the set of all elements in A that are equivalent to a.
$[a]_R = \{b \in A \mid a \equiv b\}$

Given the relation R is an equivalence relation on the set A then the following properties hold:

1. The equivalence classes of R form a partition of A.

2. A partition of a set A is a collection of nonempty, mutually disjoint subsets of A whose union is A.

2.7 Order Relations

A relation R on a set A is called a order(relation) if it is **reflexive**, **antisymmetric** and **transitive**.
Often denoted by $a \leq b$.

For each order there also exists a strict order. A strict order is the result of removing the reflexive property from the order relation.

2.7.1 Strict order

A relation R on a set A is called a strict order if it is **antisymmetric** and **transitive** and **not reflexive**.

From each order relation R there exists a strict order relation S such that $aRb \iff aSb \wedge a \neq b$. From each strict order a order relation can be derived by adding the reflexive property.

$A \leq B$ is a order relation on the set A.
$A < B$ is a strict order relation on the set A.

2.8 Comparability

Two elements a and b in a set A are said to be comparable with respect to a relation R if either aRb or bRa.

2.8.1 Total order

A relation R on a set A is called a total order if it is a partial order and for all $a, b \in A$ either aRb or bRa.

Total means that for any elements a and b in A, they are always related (they can always be compared) with respect to $R \iff aRb \vee bRa$.

2.8.2 Partial order

A relation R on a set A is called a partial order if it is **reflexive**, **antisymmetric** and **transitive**.

Partial means that for any elements a and b in A, they are not always related (they can not always be compared) with respect to $R \iff aRb \vee bRa$.

2.9 closures

Closure of a relation R is the smallest relation that contains R and has a certain property.

2.9.1 Reflexive closure

The reflexive closure of a relation R on a set A is the smallest relation that contains R and is reflexive.
A relation R is reflexive if for all $a \in A$, $(a, a) \in R$.

The reflexive closure of a relation R is $R \cup \{(a, a) \mid a \in A\}$.
Often denoted by $[R]^{\text{refl}}$.

Let $R = \{(1, 2), (2, 3)\} \subseteq A * A$.
The reflexive closure of R is $R \cup \{(1, 1), (2, 2), (3, 3)\}$.

2.9.2 Transitive closure

The transitive closure of a relation R on a set A is the smallest relation that contains R and is transitive.
A relation R is transitive if for all $a, b, c \in A$, $(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$.

The transitive closure of a relation R is the intersection of all transitive relations that contain R.

Often denoted by $[R]^{\text{trans}}$.
$[R]^{\text{trans}} = R \cup \{(a, c) \mid \exists b \in A, (a, b) \in R \wedge (b, c) \in R\}$.

Let $R = \{(1, 2), (2, 3)\} \subseteq A * A$.
The transitive closure of R is $R \cup \{(1, 3)\}$.

2.9.3 Symmetric closure

The symmetric closure of a relation R on a set A is the smallest relation that contains R and is symmetric.
A relation R is symmetric if for all $a, b \in A$, $(a, b) \in R \Rightarrow (b, a) \in R$.

The symmetric closure of a relation R is $R \cup \{(b, a) \mid (a, b) \in R\}$.
Often denoted by $[R]^{\text{sym}}$.

Let $R = \{(1, 2), (2, 3)\} \subseteq A * A$.
The symmetric closure of R is $R \cup \{(2, 1), (3, 2)\}$.

3 Modular arithmetic

Modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" upon reaching a certain value called the modulus.

A common example of modular arithmetic is the 12-hour clock, where the hours are represented by numbers from 1 to 12. When the clock reaches 12, it wraps around to 1. If the time now is 10 o'clock and we add 5 hours, the result is 10 + 5 = 3, because 10 + 5 = 15, and 15 modulo 12 is 3.

Two integers a and b are said to be congruent modulo m if m divides their difference. This is denoted as $a \equiv b \bmod(m)$.

In other words, a and b leave the same remainder when divided by m.

$7 \equiv 19 \bmod(6)$ because 6 divides $19 - 7 = 12$.
or equivalently, $7 \bmod(6) = 1$ and $19 \bmod(6) = 1$. So, $7 \equiv 19 \bmod(6)$.

3.1 Ring of integers modulo m

The ring of integers modulo m, denoted as $\mathbb{Z}/m\mathbb{Z}$, is the set of integers from 0 to $m-1$.

The ring of integers modulo 3, denoted as $\mathbb{Z}/3\mathbb{Z}$, is the set $\{0,1,2\}$. Since the possible numbers are limited to $0,1,2$ its easy to create a table of addition and multiplication for all possible combinations.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Table 1: Addition table

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Table 2: Multiplication table

3.2 Digit sum

The digit sum of a number is the sum of its digits.

The digit sum of 123 is $1+2+3=6$.

We can use the digit sum to determine if a number is divisible by $3 \vee 9$.

3.2.1 Digital root

The digital root of a number is the single-digit number obtained by repeatedly summing the digits of the number until a single-digit number is obtained.

The digital root of 123 is $1+2+3=6$.
The digital root of 12345 is $1+2+3+4+5=15$, and $1+5=6$.

3.3 Neutral element

The neutral element is an element, that when combined with another element using a binary operation, leaves the other element unchanged.

The neutral element for addition is 0, because $a+0=a \forall a \in \mathbb{Z}$.
The neutral element for multiplication is 1, because $a*1=a \forall a \in \mathbb{Z}$.

3.3.1 Inverse element

The inverse element is an element, that when combined with another element using a binary operation, results in the neutral element.

The inverse element for addition is the negative of the element, because $a+(-a)=0 \forall a \in \mathbb{Z}$.

The inverse element for multiplication is the reciprocal of the element, because $a*\left(\frac{1}{a}\right)=1 \forall a \in \mathbb{Z}$.

3.4 Neutral and inverse elements in modular arithmetic

Neutral and inverse elements can also be defined in modular arithmetic.

3.4.1 Subtraction

In order to subtract b from a in the ring of integers modulo m, find the inverse of b and add it to a.

The inverse of b is the element x such that $b + x = 0 \bmod(m)$.

Every element in the ring of integers modulo m has an inverse element therefore **subtraction is always possible.**

If we take the ring of integers modulo 6 ($\mathbb{Z}/6\mathbb{Z}$), we get the following addition table:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

In this table, each row and column contains all the elements of the ring of integers modulo 6. Figures like this are called Latin squares.

Since subtraction can be defined as addition of the inverse element $a + (-b)$, its possible to subtract by finding the inverse element.

For example: $5 - 4 \in \mathbb{Z}/6\mathbb{Z}$
1. Find the inverse of 4: $4 + x = 0 \bmod(6)$. The inverse of 4 is 2.
2. Add the inverse to 5: $5 + 2 = 1 \bmod(6)$.

3.4.2 Division

In order to divide a by b in the ring of integers modulo m, find the inverse of b and multiply it by a.

The inverse of b is the element x such that $b * x = 1 \mod(m)$.

Not every element in the ring of integers modulo m has an inverse element therefore **division is not always possible.**

If we take the ring of integers modulo 6 ($\mathbb{Z}/6\mathbb{Z}$), we get the following multiplication table:

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

In this table, not every element has a reciprocal element. For example, 2 does not have a reciprocal element.

therefore, division is only possible for the elements $1, 5$ in the ring of integers modulo 6.

In order to find a ring of integers modulo m where division is possible for all elements, m must be a prime number.

7 ($\mathbb{Z}/7\mathbb{Z}$), we get the following multiplication table, that shows that every element has a reciprocal element.

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

For smaller numbers, its easy to find the inverse element by trial and error or by writing out the multiplication table. For larger numbers, the Extended Euclidean Algorithm can be used to find the inverse element.

In order for a to have an inverse element x in the ring of integers modulo m, a and m must be coprime. This means that the greatest common divisor of a and m must be 1 ($\gcd(a, m) = 1$).

Since a and m are coprime, there exists integers x and y such that $ax + my = 1$.

To find the inverse element x, we can use the Extended Euclidean Algorithm.

4 Greatest Common Divisor

Each number has at least two divisors: 1 and itself.

$$d \mid a \Rightarrow a = d * k \text{ for some integer } k.$$

This means the divisors d can not be larger than a itself.

The divisors of 12 are $1, 2, 3, 4, 6, 12$.

$1 * 12 = 12,\ 2 * 6 = 12,\ 3 * 4 = 12,\ 4 * 3 = 12,\ 6 * 2 = 12,\ 12 * 1 = 12.$

A common divisor of two numbers is a number that divides both numbers. This means a common divisor of a and b is a number d that divides both a and b.

The common divisors of 12 and 18 are $1, 2, 3, 6$.

$1 * 12 = 12,\ 2 * 6 = 12,\ 3 * 4 = 12,\ 6 * 2 = 12.$

$1 * 18 = 18,\ 2 * 9 = 18,\ 3 * 6 = 18,\ 6 * 3 = 18.$

The greatest common divisor of two numbers is the largest number that divides both numbers denoted as $\gcd(a, b)$.

In order to find the greatest common divisor of two numbers, the Euclidean Algorithm can be used.

4.1 Euclidean Algorithm

The Euclidean Algorithm is an efficient method to find the greatest common divisor of two numbers. It is based on the fact that a common divisor of two numbers is also a divisor of their sum and difference.

$a = 42,\ b = 66.$

A common divisor of 42 and 66 is for example 3. $3 * 14 = 42$ and $3 * 22 = 66$.

For sum and difference the following holds:

$108 = 42 + 66 = 3 * 14 + 3 * 22 = 3 * (14 + 22) = 3 * 36.$

$24 = 66 - 42 = 3 * 22 - 3 * 14 = 3 * (22 - 14) = 3 * 8.$

4.1.1 Algorithm

The Euclidean algorithm works as follows:

$\gcd(400, 225)$

$400 - 225$	$400 - 225 = 175$
$225 - 175$	$225 - 175 = 50$
$175 - 50$	$175 - 50 = 125$
$125 - 50$	$125 - 50 = 75$
$75 - 50$	$75 - 50 = 25$
$50 - 25$	$50 - 25 = 25$
$25 - 25$	$25 - 25 = 0$

$\gcd(400, 225) = 25.$

$$d \mid (\alpha * a + \beta * b) \quad \forall \alpha, \beta \in \mathbb{Z}.$$

Every term of the form $\alpha * a + \beta * b$ is a multiple of d if both a and b are multiples of d. Such terms are called **linear combinations** of a and b.

4.2 Extended Euclidean Algorithm

The Extended Euclidean Algorithm calculates in addition to the greatest common divisor (gcd) of integers a and b, also the coefficients of Bézout's identity, which are integers x and y such that

$$a * x + b * y = \gcd(a, b).$$

Given the same example as before: $a = 400$, $b = 225$.

The Extended Euclidean Algorithm calculates the coefficients x and y such that $a * x + b * y = \gcd(a, b)$.

$$\begin{aligned}
&400 - 225 \\
&\quad 225 - 175 \\
&\quad\quad 175 - 50 \\
&\quad\quad 125 - 50 \\
&\quad\quad 75 - 50 \\
&\quad\quad\quad 50 - 25 \\
&\quad\quad\quad 25 - 25
\end{aligned}$$

$\gcd(400, 225) = 25$.

Now the coefficients x and y can be calculated by working backwards:

$$\begin{aligned}
&25 = 50 - 25 \\
&= 50 - (75 - 50) = 2 * 50 - 75 \\
&= 2 * 50 - (125 - 50) = 3 * 50 - 125 \\
&= 3 * 50 - (175 - 50) = 4 * 50 - 175 \\
&= 4 * (225 - 175) - 175 = 4 * 225 - 5 * 175 \\
&= 4 * 225 - 5 * (400 - 225) \\
&= 9 * 225 - 5 * 400
\end{aligned}$$