SMA205: Introduction to Algebra

Welcome to the course SMA205 - Introduction to Algebra.

- Summaries of all lectures will be distributed, with page numbers so that you will know if you are missing some page.
- The exam will most probably be given in December. There will be more information on the exam later.
- With the summaries there will also be exercises and problems. The exercises will be easy, and will serve only as a help for you to check that everything is clear. The problems will be harder and will require some thought. The student who attempts all problems will be well prepared for the exam.
- You are encouraged to ask questions whenever something is unclear. You can ask during the lectures, after the lectures, in my office, or by email.

The outline of the course is as follows:

- Review of sets, relations and functions
- Elementary number theory
- Applications to cryptography
- Introduction to abstract algebra

There will soon be a course web page:

`www.andreasholmstrom.org/sma205`

Here you will find copys of the lecture notes and additional online references for further reading. Nothing of this is necessary for the exam, but for those who want to learn more, it is a good starting point.

You can always email me at `andreas.holmstrom@gmail.com` if you have any questions.

1 Review of sets, relations and functions

You will already be familiar with the notions of set, relation and function, but since these are absolutely fundamental to everything that follows, we will quickly review them.

1.1 Sets

We can think of a *set* as any collection of objects. Most often these objects will be numbers. The objects that belong to a set are called *members* or *elements* of the set. A set can be either *finite* or *infinite*. We will use capital letters, mainly A, B, C, S, T, to denote sets, and small letters (a, b, c, . . .) for the elements of a set. We use the notation

$$a \in S$$

to say that a is a member of the set S. We also write $a \notin S$ if a is not a member of S. If S and T are two sets, and every element of S is also an element of T, then we say that S is a *subset* of T, and we write

$$S \subseteq T$$

1.1.1 How to describe a set

There are (at least) two ways to describe a set. In both cases, we uses braces $\{\ldots\}$ to show that we are dealing with a set. The first way is to *list* the elements of the set. For example, if the set S has three elements, namely the numbers 1, 3, and 7, we may write

$$S = \{1, 3, 7\}$$

to describe the set S. It does not matter in which order we list the elements. Thus $\{2, 3\}$ is the same set as $\{3, 2\}$. Also, repeated elements make no difference, so $\{b, a\}$ is the same set as $\{a, b, a\}$.

If the set is infinite, we use dots to indicate that the sequence continues. For example, the set of natural numbers can be described as

$$\{0, 1, 2, 3, \ldots\}.$$

The set of natural numbers will be denoted by $\mathbb{N}$.

The second way to describe a set S is to specify a particular property that characterizes the elements of the set. For integers, such a property might for example be “to be even” or “to be greater than 5” or “to be a prime number”. However, it is not enough to specify a property. To illustrate this, consider “the set of all numbers greater than 2 and smaller than 10”. Which numbers are in this set? Is 5 in the set? You would probably say yes. Is

π in the set? Well, that depends on what you mean by "numbers". The point here is that you must first specify a basic set of allowed objects, and then give a property that defines your set from these allowed objects. To describe the set of all natural numbers between 2 and 10 we write

$$\{x \in \mathbb{N} \mid x > 2 \text{ and } x < 10\}$$

We read this as "the set of all x in $\mathbb{N}$ such that x is greater than 2 and smaller than 10. Of course, π is not a member of this set. In general, to describe the set of all objects in S that satisfies property P, we write

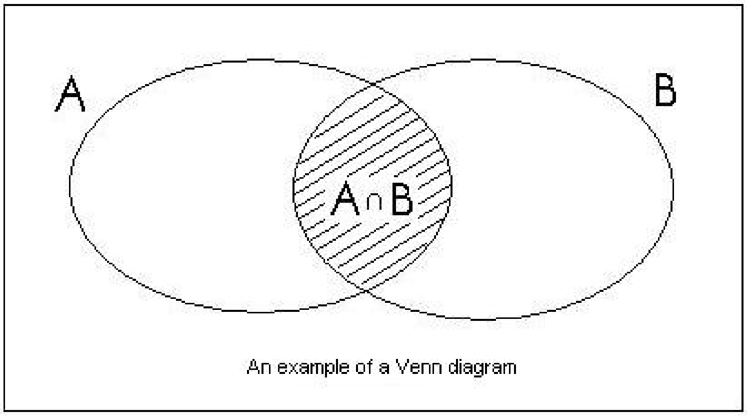
$$\{x \in S \mid x \text{ satisfies the property P}\}$$

This way of describing a set is generally more useful than the first, and will be used in most cases in this course.
There is actually a third way to describe a set: to simply describe it in words. For example "the set of all natural numbers that are a multiple of five", of "the set of all people in the world who have the letter h in their surname".

1.1.2 Constructions on sets

Given two sets A and B, we can define the following sets:

- $A \cup B$, the *union* of A and B: the set of all elements that are in A *or* in B, or in both.
- $A \cap B$, the *intersection* of A and B: the set of all elements that are both in A and B.
- $A \setminus B$, the set of all elements that are in A but not in B.



All of these can be illustrated by Venn diagrams, as explained in the lecture. We say that two sets A and B are *equal*, and write $A = B$, if they contain exactly the same elements. We say that they are *disjoint*, if they have no elements in common. There is exactly one set which has no elements at all. It is called the *empty set*, and is denoted by the symbol $\emptyset$. It is a subset of every set.

1.1.3 Cartesian product

If A and B are two sets, we want to consider pairs (a, b), where the first element a belongs to A and the second element b belongs to B. The set of all such pairs is called the *Cartesian product* of A and B, and is denoted by $A \times B$. Let us take some examples:

- Let $A = \{1, 2\}$ and let $B = \{x, y\}$. Then $A \times B = \{(1, x), (2, x), (1, y), (2, y)\}$.
- Let $A = B = \mathbb{R}$, the real line. Then $A \times B$ is the plane.
- Let $A = \{5\}$ and let $B = \{u, v, z\}$. Then $A \times B = \{(5, u), (5, v), (5, z)\}$.

Now let $A = \{x, y\}$. What are the elements of $A \times A$? Well, $A \times A$ is the set $\{(x, x), (x, y), (y, x), (y, y)\}$. The point here is that (x, y) is not the same element as (y, x). We express this by saying that the elements of the Cartesian product are *ordered pairs*. For two ordered pairs to be equal, their first entries must be equal and their second entries must be equal.

1.1.4 Exercises

For exercises E1 to E18, let

$$\begin{aligned} A &= \{x \in \mathbb{N} \mid 1 \leq x \leq 6\} \\ B &= \{2, 4, 6\} \\ C &= \{6, 7\} \end{aligned}$$

Decide whether the following statements are true or false:
E1 B and C are disjoint.
E2 $2 \in A$.
E3 $2 \notin B$.
E4 $A \cap C = B \cap C$.
E5 $A \subseteq B$.
E6 $C \subseteq B$.
E7 $B \subseteq A$.
Describe the following sets:
E8 $A \setminus B$.
E9 $B \cap C$
E10 $A \cup B$

E11 $B \times C$
E12 $B \cup (A \cap C)$
E13 $C \cap (A \cup B)$
E14 $B \setminus A$
E15 $B \cup \emptyset$
E16 $A \cap \emptyset$
E17 How many elements are there in $A \times C$?
E18 How many elements are there in $A \times (B \cap C)$?
In exercises E19 to E25, let A, B and C be any sets.
E19 Is A a subset of A?
E20 Is $\emptyset$ a subset of A?
E21 Is A a subset of $A \times A$?
E22 Is $\emptyset$ a subset of $A \times A$?
E23 Prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
(There are two ways of doing this. One way is to draw the Venn diagram of both sides and check that they are equal. The other way is to show that any element of the left hand side must be in the right hand side, and the other way around.)
E24 Prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
E25 Prove that $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$
Determine the number of elements in the following sets:
E26 $\{x \in \mathbb{N} \mid x = x^2\}$.
E27 $\{a \in \mathbb{N} \mid a < 19 \text{ and } a = 2^k \text{ for some } k \in \mathbb{Z}\}$.
E28 $\{x \in \mathbb{N} \mid x \text{ is even and } x \leq 23\}$.
Answer the following questions:
E29 If set A has 2 elements, how many elements does $A \times A$ have?
E30 If the finite set A has n elements, how many elements does $A \times A$ have?
E31 If the set A has 1 elements, how many subsets does A have?
E32 If the set A has 2 elements, how many subsets does A have?

1.2 Relations

If we are given a set S, we shall be interested in relations between the elements of the set. Let us consider the set of integers, to see some examples. The following are relations on the set of integers:

- "a is less than or equal to b"
- "a divides b" (this will be defined later)
- "a is equal to b"
- "a has the same sign[1] as b"

[1] Here we consider negative numbers to have a minus sign, positive numbers to have a plus sign, and the number 0 to have a neutral sign

When we are given a relation we can consider the set of all ordered pairs that satisfy the relation. Take for example the first relation in the above list. This defines a set R, in which for example $(4, 14)$ and $(5, 5)$ are members, while $(5, 4)$ and $(14, 4)$ are not. Similarly, consider the set S of all pairs satisfying the last relation in the list. In this case $(-2, -3)$ and $(5, 99)$, and $(0, 0)$ are all in the set S, while $(1, -1)$ and $(0, 1)$ are not in S. We can go on like this, and observe that every relation on a set A determines a certain subset of $A \times A$. In fact, this point of view is used as the abstract definition of a relation:

Definition 1. A *relation* on a set A is a subset of $A \times A$.

If R is any relation on a set, we write $a\ R\ b$ if the pair (a, b) belongs to the relation. The following definitions will allow us to gain a better understanding of relations.

Definition 2. A relation is *symmetric* if $a\ R\ b$ implies $b\ R\ a$.
A relation is *reflexive* if $a\ R\ a$ for every a.
A relation is *transitive* if $a\ R\ b$ and $b\ R\ c$ implies $a\ R\ c$.

Examples: the relation $\leq$ is reflexive and transitive, but not symmetric. The relation $=$ is symmetric, reflexive, and transitive.

1.2.1 Equivalence relations

We define a *partition* of a set S to be a collection of nonempty pairwise disjoint subsets of S set whose union is S. Each subset in a partition is called a *cell*. If we are given a partition of a set S, we can consider the following relation: "a and b are in the same cell". Thus every partition determines a relation. If a is an element, we write $cl(a)$ for the cell that contains a.

Definition 3. An *equivalence relation* is a relation determined by a partition, by the rule "a and b are in the same cell".

For example, consider the partition of the integers into the three sets of negative numbers, positive numbers, and the set $\{0\}$. The relation determined by this partition is the last relation in the above list of examples.

Theorem 1. A relation is an equivalence relation if and only if it is symmetric, reflexive and transitive.

Proof. Given in lectures. □

1.2.2 Exercises

For exercises E33 to E40, let R be the relation $>$ on the natural numbers. Are the following statements true or false?
E33 $(5,4) \in R$
E34 R is symmetric.
E35 $(9,9) \notin R$.
E36 R is transitive.
E37 $8 \; R \; 1$.
E38 R is reflexive.
E39 $(2,-1) \in R$.
E40 R is an equivalence relation.
For exercises E41 to E48, define a relation R on $\mathbb{N}$ by

$$a \; R \; b \quad \text{if} \quad (a-b) \text{ is an even integer}$$

Are the following statements true or false?
E41 $(5,9) \in R$
E42 R is reflexive.
E43 $(10,1) \notin R$.
E44 R is symmetric.
E45 $7 \; R \; 4$.
E46 R is transitive.
E47 $(2,2) \in R$.
E48 R is an equivalence relation.
For exercises E49 to E55, let $A = \{1,2,3,\ldots,9,10\}$. Are the following lists of sets partitions of A?
E49 $\{1,2\}, \; \{3,5,7,9\}, \; \{4,6,8\}$.
E50 $\{a \in A \mid a \text{ is even}\}, \; \{a \in A \mid a \text{ is odd}\}$.
E51 $\{1,2\}, \; \{3,5,7\}, \; \{2,4,6,7,8,9,10\}$.
E52 $\{8,4,2\}, \; \{9,1,10\}, \; \{5\}, \; \{7,3,6\}$.
E53 $\{1,3,5,7\}, \; \{0,2,4,6,8\}, \; \{11,10,9\}$.
E54 What is the maximal possible number of cells in a partition of A?
E55 What is the minimal possible number of cells in a partition of A?

1.3 Functions

Let A and B be sets. A function f from A to B can be thought of as some kind of rule, or machine, that assigns one element of B to each element of A. For example, if $A = B = \mathbb{N}$, there is a function which to each element $n \in \mathbb{N}$ assigns the square $n^2 \in \mathbb{N}$. A function is sometimes called a *map* or *mapping*. If an element $b \in B$ is assigned to $a \in A$ we say that a is *sent to* b, or that *a maps to b*, and we write $f(a) = b$.
Now let f be a function from A to B. We can then consider the set of all pairs $(a,b) \in A \times B$ such that $f(a) = b$. This is a subset of $A \times B$, called the

graph of f. The graph of a function has the following property: for every $a \in A$ there is a unique element $b \in B$ such that (a, b) is in the graph. This leads to the abstract definition of a function:

Definition 4. A *function* from a set A to a set B is a subset f of $A \times B$ such that for every $a \in A$ there is a unique $b \in B$ such that $(a, b) \in f$. Usually we write $f(a) = b$ instead of $(a, b) \in f$.

If f is a function from A to B we write $f : A \to B$. We call A the *domain* of f and B the *codomain* of f. The set

$$im(f) = \{b \in B \mid b = f(a) \text{ for some } a \in A\}$$

is called the *image* of f. If an element a is mapped to an element b we write $a \mapsto b$. The most common way of specifying a function is illustrated by the following example, in which we take $A = B = \mathbb{N}$.

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N} \\ x &\mapsto x^2 \end{aligned}$$

This function, which sends each natural number to its square, can also be described by the formula

$$f(x) = x^2$$

which is perhaps more familiar.

Definition 5. Let $f : A \to B$ be a function. We say that f is *injective* (or *one-to-one*) if $f(x) = f(y)$ implies $x = y$. We say that f is *surjective* (or *onto*) if for every $b \in B$, there is some $a \in A$ such that $f(a) = b$. We say that f is *bijective* if it is both surjective and injective.

In other words, f is surjective if $im(f)$ equals B, and f is injective if two different elements of A always are mapped to two different elements of B (hence "two-to-two" would actually be a better word than "one-to-one"). If $f : A \to B$ and $g : B \to C$ are functions, we can define a function h from A to C by the rule $h(a) = g(f(a))$. This function called the *composite* and is denoted by $g \circ f$.

1.3.1 Exercises

For exercises E56 to E70, define

$$\begin{aligned} g : \mathbb{N} &\to \mathbb{N} \\ x &\mapsto x^2 - x + 1 \end{aligned}$$

and let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(x) = x + 2$.
E56 Is f injective?

E57 Is f surjective?
E58 Is f bijective?
E59 What is the domain of f?
E60 What is the codomain of f?
E61 What is the image of f?
E62 Is g injective?
E63 Is g surjective?
E64 Is g bijective?
E65 What is the codomain of g?
E66 Write down some elements of $im(g)$.
E67 Compute $g \circ f(7)$.
E68 Compute $f \circ g(7)$.
E69 Is $f \circ g$ injective?
E70 Is $g \circ f$ injective?

1.4 Problems

P1 If A has five elements and B has three elements, how many different functions are there from A to B?
P2 Try to find a relation on some set which is reflexive and symmetric, but not transitive.
P3 If the set A has n elements, how many subsets does A have?
P4 Is it true that the composite of two injective functions is injective?
P5 Is it true that the composite of two surjective functions is surjective?
P6 Define a function $f : \mathbb{N} \to \mathbb{N}$ by $f(a) =$ "sum of the digits of a". This means that for example $f(2) = 2$, $f(35) = 8$ and $f(18247) = 22$. Let $g = f \circ f$. Answer the following questions:
(i) Compute $f(669)$.
(ii) Is f injective?
(iii) Is f surjective?
(iv) Is f bijective?
(v) Compute $g(15005)$.
(vi) Compute $g(259781)$.
(vii) What is the codomain of g?
(viii) What is the domain of g?
(ix) Is g injective?
(x) Is g surjective?