Some elements of elementary set theory

MAT2200 — Spring 2011

By Geir Ellingsud

Most of what this document contains is probably well known to most of you, but still I think it is useful to cast a glance at it the beginning of the course. It treats the elementary constructions in set theory which will be used through out the course. It will certainly be of great help in understanding the rest of what we will do. It has gotten somehow long — so take a look at it, and use it as a reference later in the course. The paragraphs are marked with red stars (like this (∗∗∗) or this (∗∗) or this (∗), or they are unmarked) according to there urgency.

For many of concepts that are introduced the Norwegian word is also given (•*like this*). It is important to introduce at least the Norwegian students to a Norwegian terminology, even though the course is given in english.

Specifying sets (∗∗∗)

A set (•*en mengde*) consists of its *elements* (•*elementer, medlemmer*), and we write $a \in A$ to express that a is a member of A. Two sets are equal if and only if they do have the same elements. If A and B are two sets, we call B a *subset* of A (•*delmengde, undermengde*) in case every element of B is an element of A. In symbols we write $B \subseteq A$. If in addition the two sets are different we write $B \subset A$ and call B is a *proper subset* of A (•*en ekte undermengde*), or we say that the inclusion is *strict* (•*streng inklusjon*).

A frequently used way of showing two sets A and B to be equal is separately to show the two inclusions $A \subseteq B$ and $B \subseteq A$. Obviously these two inclusions imply that the two sets have the same elements. Indeed, if not, one of them — say B — would have an element not contained in the other — which is A — contradicting the inclusion $A \subseteq B$.

The complement (•*komplementet*) of a subset B of A is the set consisting of the elements from A not contained in B. The complement is written B^c. There is a set without elements called the *empty set* (•*den tomme mengde*), and it is denoted by the symbol $\emptyset$. May be this seems a curious definition to make, but it is very convenient.

A set can be specified in several ways; the simplest one is listing the elements, like in $A = \{a, b, c\}$, which is a set with the three letters a, b and c as members.

We often need to define sets in a systematic way, often with a great number of elements (even infinitely many is common) and often with members depending on

some parameter. It that case it is convenient to of specify the members of the set in the following way; which we illustrate with an example: The set of even integers may be written like

$$A = \{\, 2k \mid k \in \mathbb{N} \,\} = \{2, 4, 6, \dots\}. \qquad (\star)$$

Sometimes we use a *condition* to single out the elements belonging to a set. The syntax is like $\{\, x \mid P(x) \,\}$ where $P(x)$ is a statement involving x. The set consists of the elements x for which $P(x)$ is true. As an example, the set $(\star)$ above could be written

$$A = \{\, x \in \mathbb{N} \mid x \text{ even } \}.$$

One word of warning, when listing the elements of a set, in one way or another, repeated elements are only counted once — double membership is not a concept in this context. Sometimes multiply listed elements can be tricky to spot, because the repetition might not be explicit. The following example, which also reminds you that a set very well may consist of subsets of another set, illustrates this:

$$B = \{\, \{\, a, b, c \,\} \mid a, b, c \in A \,\}.$$

This set B is *not* the set of all subsets of A with three elements. Neither the case $a = b$ nor the case $a = b = c$ is excluded, so the elements of B are the nonempty subset of A with three elements or less.

When a set is specified by listing the elements, the order does not matter. So we have

$$\{\, Katz, Maus \,\} = \{\, Maus, Katz \,\}.$$

Intersections and unions (**) — De Morgans Laws (*)

If $A_1, A_2, \dots, A_n$ are sets, their *intersection* (•*snittet*) — written $A_1 \cap A_2 \cap \cdots \cap A_n$ — is the set of elements common to *all* the sets $A_1, \dots, A_n$. In other words

$$A_1 \cap A_2 \cap \cdots \cap A_n = \{\, a \mid a \in A_i \text{ for all } \; i = 1, 2, \dots, n \,\}.$$

Their union (•*union*) — written $A_1 \cup A_2 \cup \cdots \cup A_n$ — is the set whose elements are those contained in *at least* one of the sets $A_1, A_2, \dots, A_n$. Stated with symbols:

$$A_1 \cup A_2 \cup \cdots \cup A_n = \{\, a \mid a \in A_i \text{ for at least one } \; i, 1 \le i \le n \,\}.$$

We shall often be interested in families of sets. A family may be specified by using indices from a set I — finite or infinite — and in that case it is written as $\mathscr{A} = \{\, A_i \,\}_{i \in I}$. Or it can be given just as a set of sets, like in the example $\mathscr{A} = \{\, [a, b] \mid a, b \in \mathbb{R}, a < b \,\}$.

The following notation for the intersection and the union of the sets belonging to a family will be convenient:

$$\bigcap_{i\in I} A_i = \{\, a \mid a \in A_i \text{ for all } i \in I \,\},$$
$$\bigcup_{i\in I} A_i = \{\, a \mid a \in A_i \text{ for at least one } i \in I \,\},$$

or if the family is given as a set of sets, the notation will be as follows:

$$\bigcap_{A\in\mathscr{A}} A = \{\, a \mid a \in A \text{ for all } A \in \mathscr{A} \,\},$$
$$\bigcup_{A\in\mathscr{A}} A = \{\, a \mid a \in A \text{ for at least one } A \in \mathscr{A} \,\}.$$

It is easily verified that intersection is *distributive* (•*distributiv*) over union and vice versa:

Proposition 1 *Let A_i with $i \in I$ an B be sets. Then we have*

$$B \cap \bigcup_{i\in I} A_i = \bigcup_{i\in I} B \cap A_i,$$
$$B \cup \bigcap_{i\in I} A_i = \bigcap_{i\in I} B \cup A_i.$$

Named after August De Morgan — one of the founders and the first professor of mathematics at the University College of London — the De Morgans Laws describe the complement of unions and intersections:

Proposition 2 *Let $A_1, \ldots, A_n$ be sets, then:*

$$(A_1 \cup A_2 \cup \cdots \cup A_n)^c = A_1^c \cap A_2^c \cap \cdots \cap A_n^c,$$
$$(A_1 \cap A_2 \cap \cdots \cap A_n)^c = A_1^c \cup A_2^c \cup \cdots \cup A_n^c.$$

In fact, a not being an element of $A_1 \cup A_2 \cup \cdots \cup A_n$ is equivalent to a not being a member of any of the A_i; hence a is in all the A_i^c — that is $a \in A_1^c \cap A_2^c \cap \cdots \cap A_n^c$. In a similar way, a not being member of $A_1 \cap A_2 \cap \cdots \cap A_n$ is equivalent to a not being in at least one of the A_i, hence $a \in A_1^c \cup A_2^c \cup \cdots \cup A_n^c$. □

If we are dealing with a family $\mathscr{A}$ of sets, the De Morgans Laws has the following appearance

$$(\bigcap_{A\in\mathscr{A}} A)^c = \bigcup_{A\in\mathscr{A}} A^c,$$
$$(\bigcup_{A\in\mathscr{A}} A)^c = \bigcap_{A\in\mathscr{A}} A^c.$$

Finally in this paragraph, we recall that two sets A and B are said to be *disjoint* (•*disjunkte*) if they do not have any element in common, equivalently, one may require their intersection to be empty; in symbols $A \cap B = \emptyset$. The sets from a family $\mathscr{A} = \{ A_i \}_{i\in I}$ are said to be *mutually disjoint* (•*parvis disjunkte*) if $A_i \cap A_j = \emptyset$ whenever $i \neq j$.

Maps (***)

Recall that a map or mapping or function (•*avbildning, funksjon*) ϕ between to sets A and B is a rule — specified in one way or another — which given an element a in the set A, returns an element $\phi(a)$ in B. We often write

$$\phi\colon A \to B$$

to indicate that ϕ is a mapping from A to B. We shall call the set A the *source* of ϕ and B its *target*. (•*No commonly used norwegian words for these concepts*). The sets A and B are important attributes of the mapping — sometimes, when we use the map primarily to compare them, they are even the main point of interest.

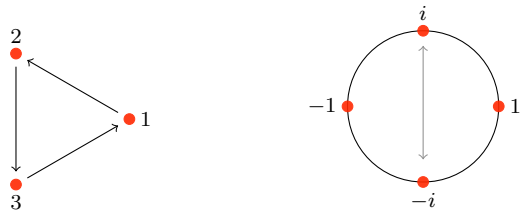
You already know a lot of maps — any function $f(x)$ of a real variable, or for that matter a complex one, gives an example. Linear maps are also well known from the courses in linear algebra. We shall give some examples of a slightly different flavor:

EXAMPLE 1 Let $A = \{ 1, 2, 3 \}$ and let $\alpha\colon A \to A$ be given as

$$\alpha(n) = \begin{cases} 2 & \text{if } n = 1 \\ 3 & \text{if } n = 2 \\ 1 & \text{if } n = 1, \end{cases}$$

There is another notation for maps like this (i.e., whose source and target are the same finite set) in which α would be written in the following way: $1 \mapsto 2 \mapsto 3 \mapsto 1$. An arrow $x \mapsto y$ means that x is mapped to y by the map under consideration. The map

α is called a permutation (•*permutasjon, ombytting*) since it — well — permutes the numbers $1, 2$ and 3. It even has a more precise name; it is said to be a *cyclic* (•*syklisk*) permutation — the drawing to the left in the following figure indicates why.



EXAMPLE 2 Yet another example of a permutation. This time we let B be the set of forth roots of unity, i.e., $B = \{\pm 1, \pm i\} \subseteq \mathbb{C}$, and we let $\beta\colon B \to B$ be given by $\beta(z) = z^3$. Then β has the following effect: $i \mapsto i^3 = -1$ and $-i \mapsto (-i)^3 = i$, so i and $-i$ are interchanged by β. Obviously β does not move neither 1 nor -1. Even if β is a pemutation, it is not a cyclic one. In the other notation β would we written $i \mapsto -i \mapsto i$, with the convention that lacking elements are not moved by the map.

Can you describe what the map $\delta\colon B \to B$ given by $\delta(z) = z^2$ does?

EXAMPLE 3 Let $\gamma\colon \mathbb{Z} \to \mathbb{Z}$ be given as $\gamma(n) = 5n$.

EXAMPLE 4 Our last example is the *determinant*. I has as source the set $\mathrm{M}_n(\mathbb{R})$ of square matrices with real entries of some size — say size n — and takes values in $\mathbb{R}$. It is defined by sending a matrix A to its determinant $\det A$. So we would like to write it as

$$\det\colon \mathrm{M}_n(\mathbb{R}) \to \mathbb{R}$$

Composition of maps (***)

Given two maps $\phi\colon A \to B$ and $\psi\colon B \to C$ there is a *composed map* (•*sammensatt avbildning*) $\psi \circ \phi\colon A \to C$ defined by the rule

$$\psi \circ \phi(x) = \psi(\phi(x)). \qquad (\spadesuit)$$

Sometimes we shall drop the $\circ$ and simply write $\psi\phi$ for the composed map. Two maps are called *composable* (•*komponerbare*) it they are — well — composable; this requires

the source of one to be the target of the other. Be aware that this is not a symmetric notion — if ψ and ϕ are composable, there is no reason why ϕ and ψ should be.

The arrow notation is practical to avoid mixing things up:

$$A \xrightarrow{\phi} B \xrightarrow{\psi} C$$

This clearly shows that the source of ψ equals the target of ϕ. Hence $\psi \circ \phi$ is meaningful, but $\phi \circ \psi$ is not — unless $C = A$ for some to us yet unknown reason.

EXAMPLE 5 The maps β and δ from the example (2) on page 5 are composable (likewise are δ and ϕ) and the composition is given by $\beta \circ \delta(z) = \beta(\delta(z)) = (z^2)^3 = z^6 = z^2$. The last equality holds for elements $z \in B$, since they are all forth roots of unity. Hence $\beta \circ \delta = \delta$!

One checks easily that forming the composition of two maps is an *associative* (•*assosiativ*) operation: i.e.,

Proposition 3 *Let θ, ψ, ϕ be three composable maps. Then we have*

$$\theta \circ (\psi \circ \phi)) = (\theta \circ \psi) \circ \phi.$$

Indeed, for $x \in A$ we have:

$$(\theta \circ (\psi \circ \phi))(x) = \theta(\psi \circ \phi(x)) = \theta(\psi(\phi(x))) = \theta \circ \psi(\phi(x)) = ((\theta \circ \psi) \circ \phi)(x)$$

where each of the equalities follows directly from the definition (♠) above applied to an appropriate pair of maps.

I follows from the law of associativity that expressions like

$$\phi_1 \circ \phi_2 \circ \phi_3 \circ \cdots \circ \phi_n \qquad (♠♠)$$

where the ϕ_i are composable maps, are meaningful. Only two maps can directly be composed, and to give meaning to an expression like (♠♠), one has to place parentheses in an intelligent way. That is, in such a way that every pair of opening and closing parentheses encloses only two maps, which of course, in their turn might be nested compositions of other maps. One example is

$$(\phi_1 \circ \phi_2) \circ (\phi_3 \circ ((\phi_4 \circ \phi_5) \circ \phi_6)).$$

Acceptable nestings can be made in a lot of different ways, however, the associativity property assures that the resulting maps all will be equal whatever nesting used. Ideally this needs a proof, buy we shall accept it as a fact — it is not very difficult to prove, although a good proof is somehow subtle to formulate.

Invertible maps (***)

For every set A there is an *identity map* (•*en identities avbildning*). It has both A as source and target, is written id_A, and it is defined by $\mathrm{id}_A(a) = a$ for all $a \in A$. Of course, for any map $\phi\colon A \to B$ we have $\phi \circ \mathrm{id}_A = \phi$ and $\mathrm{id}_B \circ \phi = \phi$.

Given a map $\phi\colon A \to B$. If there is a mapping the other way around, that is a map $\rho\colon B \to A$, with the property that

$$\rho \circ \phi = \mathrm{id}_A \quad \text{and} \quad \phi \circ \rho = \mathrm{id}_B, \tag{♣}$$

we shall say that ϕ is *invertible* (•*invertibel*), and call the map ρ the *inverse* (•*den inverse, den omvendte*) of ϕ. The inverse is usually denoted by ϕ^{-1}, and it is the *only* map satisfying (♣). Indeed, if ρ_1 and ρ_2 both satisfied (♣), we would have

$$\rho_1 \circ \phi = \mathrm{id}_A = \rho_2 \circ \phi \tag{♣♣}$$

which on composition with ρ_1 from the right, would give

$$\rho_1 \circ \phi \circ \rho_1 = \rho_2 \circ \phi \circ \rho_1.$$

But $\phi \circ \rho_1 = \mathrm{id}_B$, so finally (♣♣) would imply $\rho_1 = \rho_2$. □

Proposition 4 *The composition of two composable, invertible maps is invertible, and if ψ and ϕ are the two maps, we have the formula*

$$(\psi \circ \phi)^{-1} = \phi^{-1} \circ \psi^{-1}.$$

The easiest way to prove this, is by verifying that $\phi^{-1} \circ \psi^{-1}$ satisfies (♣), and we do that simply by composing $\phi^{-1} \circ \psi^{-1}$ with $\psi \circ \phi$:

$$(\psi \circ \phi) \circ (\phi^{-1} \circ \psi^{-1}) = \psi \circ (\phi \circ \phi^{-1}) \circ \psi^{-1} = \psi \circ (\mathrm{id}_B) \circ \psi^{-1} = \psi \circ \psi^{-1} = \mathrm{id}_A$$

It is very important also to check the other equality in (♣), that is $(\phi^{-1} \circ \psi^{-1}) \circ (\psi \circ \phi) = \mathrm{id}_B$. The argument for that being, with the obvious changes, the same as the one we just gave, and we leave it to the reader. □

EXAMPLE 6 *(of a minimalist).* In fact, as we just said, it is crucial to check both identities in (♣) to be sure we have an inverse map. To convince your self of this, take a look at the following minimalists example: Let $A = \{1, 2\}$ and $B = \{1\}$ and define $\phi\colon A \to B$ by — well — there is only one way of doing this, namely by putting

$\phi(1) = \phi(2) = 1$. Let $\psi\colon B \to A$ be given by $\psi(1) = 1$. Then $\phi \circ \psi = \mathrm{id}_B$, but $\psi \circ \phi \neq \mathrm{id}_A$ as it sends both elements of A to 1.

EXAMPLE 7 What would be the inverse of the map α in example (1) on page 4? Remember it was described as

$$\alpha : 1 \mapsto 2 \mapsto 3 \mapsto 1. \qquad (\heartsuit)$$

To get the inverse mapping, we reverse this, i.e., we send $1 \mapsto 3$, $3 \mapsto 2$ and $2 \mapsto 1$; or written together

$$1 \mapsto 3 \mapsto 2 \mapsto 1,$$

which just is ($\heartsuit$) backwards!

EXAMPLE 8 The mapping $\beta : B \to B$ (where $B = \{\pm 1, \pm i\}$) in example (2) is its own inverse! In fact, we compute

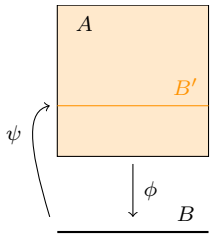
$$\beta \circ \beta(z) = \beta(\beta(z)) = (z^3)^3 = z^9 = z(z^4)^2 = z$$

since B consists of the forth roots of one.

With a little thought, we could have arrived at this conclusion without computing, remembering that the effect of β was to interchange i and $-i$. So interchanging them once more, we are restoring the order!

One more example

For those who want an example of a more visual nature, we have produced the figure above, where we have placed a copy of $B = [0, 1]$ inside the rectangle $A = \{(x, y) \mid 0 \leq x \leq 1, 1 \leq y \leq 3\}$ as $B' = \{(x, a) \mid 0 \leq x \leq 1\}$. The parameter a is any number between 1 and 2, and the maps are $\psi(x) = (a, x)$ and $\phi(x, y) = x$. One easily checks that $\phi \circ \psi = \mathrm{id}_B$, but that $\psi \circ \phi \neq \mathrm{id}_A$.



In fact, these two examples illustrate a rather general situation. Given a map $\phi\colon A \to B$, a map $\sigma\colon B \to A$ is called a *section* or a *transversal* (•*seksjon, tversnitt*) to ϕ if $\phi \circ \sigma = \mathrm{id}_B$.

Not every map has a section. Indeed, if ϕ has a section σ, necessarily $\phi(A) = B$ (because $\psi(\sigma(y)) = y$ for all $y \in B$) and this is not true for all maps. On the other hand, the condition $\psi(A) = B$ is also sufficient for ϕ to have a section. In fact, in that case all the fibers $\phi^{-1}(y)$ are nonempty, and we may define σ by letting $\sigma(y)$ be any element in $\phi^{-1}(y)$.

The freedom in choosing any element in $\phi^{-1}(y)$ as the value for $\sigma(y)$ tells us that sections almost never are unique. What would be a condition on a map for it to have only one section?

Images and inverse images (∗)

We continue to work with our map $\phi\colon A \to B$, and in addition we let $C \subseteq A$ and $D \subseteq B$ be two subsets. The *image* (•*bildet*) $\phi(C)$ of C and the *inverse image* (•*det inverse bildet*) $\phi^{-1}(D)$ of D are the sets

$$\phi(C) = \{\, \phi(a) \mid a \in C \,\} \text{ and } \phi^{-1}(D) = \{\, a \in A \mid \phi(a) \in D \,\}.$$

In the case D has only one element, say $D = \{b\}$, we usually shall write $\phi^{-1}(b)$ for $\phi^{-1}(\{\, b \,\})$ and call $\phi^{-1}(b)$ the *fiber* (•*fiberen*) of ϕ over b. The elements of $\phi^{-1}(b)$ are called the *preimages* (•*no good Norwegian word*) of b. The fiber over a point b might very well be empty. Indeed, this happens if and only if b is not in the image $\phi(A)$.

It follows more or less by definition that

$$\phi(\phi^{-1}(D)) \subseteq D \text{ and } C \subseteq \phi^{-1}(\phi(C)). \tag{⋆}$$

In either case equality does not hold in general.

A situation where an element b of B is not contained in the image $\phi(A)$, would give an example of a strict inclusion in the first case. Then $\phi^{-1}(b) = \emptyset$ and $\phi(\phi^{-1}(b)) = \emptyset \neq A$ — at least if A is nonempty. What is true generally is that $\phi(A) \cap D = \phi(\phi^{-1}(D))$.

A more concrete example comes here

EXAMPLE 9 We go back to example (3) on page 5 where we defined a map $\gamma\colon \mathbb{Z} \to \mathbb{Z}$ by $n \mapsto 5n$ — the "multiplication-by-five-map". Let $D \subseteq \mathbb{Z}$ be given as $D = \{\, n \in \mathbb{Z} \mid 3 < n < 21 \,\}$.

What is $\gamma^{-1}(D)$?

Well, we need to find all integers in D divisible by 5. That is $5, 10, 15$ and 20. Hence $\gamma(\gamma^{-1}(D)) = \{\, 5, 10, 15, 20 \,\}$ and $\gamma^{-1}(D) = \{\, 1, 2, 3, 4 \,\}$.

To produce an example of a strict inclusion in the second case, take any map $\phi\colon A \to B$ having an element a with more than one element in the fiber $\phi^{-1}(\phi(a))$ — the minimalists example (6) on page 7 will do.

Proposition 5 *Let $\phi\colon A \to B$ be a map. For any two subsets A_1 and A_2 of A we have*

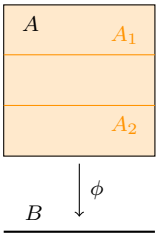
$$\begin{aligned} \phi(A_1 \cap A_2) &\subseteq \phi(A_1) \cap \phi(A_2) \\ \phi(A_1 \cup A_2) &= \phi(A_1) \cup \phi(A_2) \end{aligned} \tag{†}$$

In other words, forming images commute with intersections and unions.

Proof. It is clear that $\phi(A_1 \cap A_2) \subseteq \phi(A_i)$ for $i = 1, 2$. Since $A_1 \cap A_2 \subseteq A_i$ this follows from $(\star)$ on page 9; hence $\phi(A_1 \cap A_2) \subseteq \phi(A_1) \cap \phi(A_2)$.

We attack the other equality. Now $A_i \subseteq A_1 \cup A_2$ for both $i = 1$ and $i = 2$, hence we get $\phi(A_i) \subseteq \phi(A_1 \cup A_2)$, again by $(\star)$ on page 9.

To establish the inclusion $\phi(A_1 \cup A_2) \subseteq \phi(A_i)$, pick an element b from $\phi(A_1 \cup A_2)$. This means that $b = \phi(a)$ with a either in A_1 or in A_2. In the first case $b \in \phi(A_1)$ and in the second in $\phi(A_2)$. □



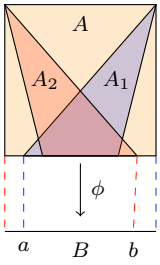
It is worth remarking, that the inclusion in equation (†) in proposition 5 very well might be strict. For example, the intersection $A_1 \cap A_2$ could be empty but $\phi(A_1) = \phi(A_2) = B$. An example of this would be the minimalists example (6) on page 7 above: $\phi\colon \{1, 2\} \to \{1\}$ given in the only possible way $\phi(1) = \phi(2) = 1$. Then the two subsets $A_1 = \{1\}$ and $A_2 = \{2\}$ of the source $\{1, 2\}$ will do.

A somehow more geometric example is illustrated in the small figure to the left. There A is the square

$$A = \{ (x, y) \mid 0 \leq x \leq 1, 1 \leq y \leq 3 \}$$

and ϕ the projection onto the x-axis. The two sets A_i are defined as $A_i = \{ (x, a_i) \mid 0 \leq x \leq 2 \}$ where a_1 and a_2 any two numbers, we only require they be different and both lay between 1 and 3.

In the second drawing, to the right, the images of the two triangles A_1 and A_2 (red and blue in the figure) intersect in the interval $[a, b]$ but the image of the intersection (violet) is certainly a smaller interval.



A final remark about images, is that the statement in proposition 5 is valid for any number of subsets, in fact it is true for any family $\mathscr{A}$ of subsets of A. We have the following proposition whose proof is similar — in fact verbatim with the obvious modifications — to the one we just gave

Proposition 6 *Assume that $\mathscr{A}$ is a family of subsets of A and that $\phi\colon A \to B$ is a map. Then*

$$\phi\Big(\bigcap_{A \in \mathscr{A}} A\Big) \subseteq \bigcap_{A \in \mathscr{A}} \phi(A) \text{ and } \phi\Big(\bigcup_{A \in \mathscr{A}} A\Big) = \bigcup_{A \in \mathscr{A}} \phi(A),$$

so the formation of images of subsets under a map, commutes with arbitrary unions and intersections.

We now move from studying images of intersections and unions, to studying inverse images. The following result tells us that the formation of inverse images behaves very well with respect to intersections and unions. We state it first for two subsets, but it is valid for any family, the general result being stated at the end of the paragraph.

Proposition 7 *Let $\phi\colon A \to B$ be a map. If B_1 and B_2 are two subsets of B we have*

$$\phi^{-1}(B_1 \cap B_2) = \phi^{-1}(B_1) \cap \phi^{-1}(B_2)$$
$$\phi^{-1}(B_1 \cup B_2) = \phi^{-1}(B_1) \cup \phi^{-1}(B_2).$$

I other words, taking inverse images commute with intersections and unions.

Proof. By $(\star)$ on page 9 we have

$$\phi(\phi^{-1}(B_1 \cap B_2)) \subseteq B_1 \cap B_2 \subseteq B_i$$

for $i = 1, 2$, and therefore

$$\phi^{-1}(B_1 \cap B_2) \subseteq \phi^{-1}(B_1) \cap \phi^{-1}(B_2).$$

On the other hand, from proposition 5 we get

$$\phi(\phi^{-1}(B_1) \cap \phi^{-1}(B_2)) \subseteq \phi(\phi^{-1}(B_1)) \cap \phi(\phi^{-1}(B_2)) \subseteq B_1 \cap B_2$$

so

$$\phi^{-1}(B_1) \cap \phi^{-1}(B_2) \subseteq \phi^{-1}(B_1 \cap B_2),$$

and we are done.

For the other equality in the proposition we refer to proposition 7 which gives us

$$\phi(\phi^{-1}(B_1) \cup \phi^{-1}(B_2)) = \phi(\phi^{-1}(B_1)) \cup \phi(\phi^{-1}(B_2))) \subseteq B_1 \cup B_2$$

by $(\star)$ on page 9, so

$$\phi^{-1}(B_1) \cup \phi^{-1}(B_2) \subseteq \phi^{-1}(B_1 \cup B_2).$$

On the other hand

$$B_i \subseteq B_1 \cup B_2$$

for $i = 1, 2$, so again by $(\star)$ on page 9

$$\phi^{-1}(B_1) \cup \phi^{-1}(B_2) \subseteq \phi^{-1}(B_1 \cup B_2)$$

and we are through. □

As promised, here comes the general statement. We shall not prove it, but the interested reader should try. The proof goes along the same lines as the proof of proposition 7 above.

Proposition 8 *Let $\mathscr{B}$ be a family of subsets of a set B and let $\phi\colon A \to B$ be a map. Then*

$$\phi^{-1}(\bigcap_{B\in\mathscr{B}} B) = \bigcap_{B\in\mathscr{B}} \phi^{-1}(B)$$
$$\phi^{-1}(\bigcup_{B\in\mathscr{B}} B) = \bigcup_{B\in\mathscr{B}} \phi^{-1}(B)$$

In other words, the formation of inverse images commutes with arbitrary unions and intersections.

Injective and surjective and all that (***)

We have now come to the two important notions of *injective* (•*injektiv*) and *surjective*(•*surjektiv*) maps. In what follows we keep the notation with the map $\phi\colon A \to B$.

- The map ϕ is injective if for any $b \in B$ there is *at most one* $a \in A$ such that $\phi(a) = b$.
- The map is surjective if for any $b \in B$ there is *at least one* $a \in A$ such that $\phi(a) = b$.

Another way of phrasing the definition of injectivity, is to say that the fibers $\phi^{-1}(b)$ are either empty or have just one element. Still another variant is the following: ϕ is injective if and only if whenever $a_1 \neq a_2$ then $\phi(a_1) \neq \phi(a_2)$, so an injective map sends different points to different points. The term *one-to-one map* (•*en-en-tydig avbildning*) is a frequently used synonym for an injective map.

EXAMPLE 10 The minimalists map $\phi\colon \{1, 2\} \to \{1\}$ is surjective, but not injective. The map $\delta\colon B = \{\pm 1, \pm i\} \to B$ with $\delta(z) = z^2$ is neither injective nor surjective, as $(\pm 1)^2 = 1$ and $(\pm i)^2 = -1$. However $\beta\colon B \to B$ given by $z \mapsto z^3$ is both injective and surjective. It just interchanges i and $-i$.

EXAMPLE 11 The "multiplication-by-five-map" $\gamma\colon \mathbb{Z} \to \mathbb{Z}$ in example (3) on page 5 and given by $\gamma(n) = 5n$ is injective but not surjective.

Surjectivity of ϕ means that $\phi(A) = B$ (check that!) or that the fibers of ϕ are all nonempty (and that!). The term *onto* (•*på*) is also in use.

A map which is both injective and surjective is called *bijective* (•*bijektiv*). This is equivalent to the map being *invertible*, which is an observation so fundamental, that it deserves to be formulates as a proposition:

Proposition 9 *A map $\phi\colon A \to B$ is invertible if and only if it is both injective and surjective.*

Proof. Assume that ϕ is invertible and let a_1 and a_2 be two members of A satisfying $\phi(a_1) = \phi(a_2)$. By applying ϕ^{-1} on both sides of this equation one deduces

$$a_1 = \mathrm{id}_A(a_1) = \phi^{-1}(\phi(a_1)) = \phi^{-1}(\phi(a_2)) = \mathrm{id}_A(a_2) = a_2,$$

and hence ϕ is injective. To see that ϕ is surjective, pick an element $b \in B$ and let $a = \phi^{-1}(b)$. Then $\phi(a) = \phi(\phi^{-1}(b)) = \mathrm{id}_B(b) = b$.

To verify the implication the other way, assume ψ to be both injective and surjective. We want to define $\phi^{-1}\colon B \to A$, so let $b \in B$ be any element. We claim that for every b there exactly one $a_b \in A$ being a solution of

$$\phi(a_b) = b. \qquad (\blacklozenge)$$

The existence of a solution follows from the fact that ϕ is surjective, and the uniqueness from the injectivity of ϕ. This solves our problem, since if we put $\phi^{-1}(b) = a_b$, we get a map $\phi^{-1}\colon B \to A$, and it is easy to verify that $\phi^{-1}(\phi(a)) = a$ and $\phi(\phi^{-1}(b)) = b$. □

Cartesian product (**)

The *cartesian product* is named after the french philosopher and mathematician René Descartes, who was one of the first to use coordinates (x, y) to describe points in the plane. He thus identified the plane with $\mathbb{R}^2$. This is short hand for the *product* $\mathbb{R} \times \mathbb{R}$, and therefore the name.

The *cartesian product* or simply the product (•*det kartesiske produktet, produktet*) of two arbitrary sets A and B is the set of all pairs (a, b) with $a \in A$ and $b \in B$, or in symbols

$$A \times B = \{\, (a, b) \mid a \in A, b \in B \,\}.$$

There are two obvious maps $p_A\colon A \times B \to A$ and $p_B\colon A \times B \to B$ given by $p_A(a, b) = a$ and $p_B(a, b) = b$ respectively. They are called the *projection* (•*projeksjonen*) onto A resp. B.

More generally if $A_1, \ldots, A_n$ are sets, we define their (cartesian) product as

$$A_1 \times A_2 \times \ldots \times A_n = \{\, (a_1, \ldots, a_n) \mid a_i \in A_i \text{ for } i = 1, 2, \ldots, n \,\}$$

There are obvious projection maps p_{A_i} given by $p_{A_i}(a_1, \ldots, a_n) = a_i$.

We sometimes write $\prod_{i=1}^{n} A_i$ for the product $A_1 \times A_2 \times \ldots \times A_n$.

Finite sets (**)

At least in the first part of the course when we shall work with finite groups, our mappings will mostly be between finite sets. In this paragraph we shall point out a few properties of such maps which later will make a few of our arguments simpler — or even possible. At several occasions in the development of the theory of finite groups, counting arguments play a crucial role. It is therefore appropriate to review a few features of the combinatorics of finite sets.

The number of elements in a finite set X is in the context of group theory most often denoted by $|X|$, although the notation $\#X$ is in use. We shall adopt the notation $|X|$. It is also called the *cardinality* (•*kardinaliteten*) of X.

Assume that A is a finite set and let $I_n = \{1, 2, \ldots, n\}$ be the set of integers between 1 and n. Let further a mapping $\phi\colon I_n \to A$ be given. We may think of ϕ as a count of the elements of A, or as a listing of them: $\phi(1)$ being the first element of A, $\phi(2)$ the second and so on.

It might happen that not every element of a is listed and so that some elements do not figure on the list — this is the case if ϕ is not surjective.

It might also happen that some element is counted several times and therefore occupies several places in the list. This happens if ϕ is not injective .

We want to give a "heil norskt" (•*sorry, no english equivalent*) and define a set A by $A = \{Solveig, Per, Aase\}$. Furthermore let a map $\phi\colon I_5 \to A$ be given by

$$\phi(1) = \phi(4) = \text{ Soveig, } \phi(2) = \text{Per and } \phi(3) = \phi(5) = \text{Aase.}$$

Then the corresponding listing of our three friends will be:

Solveig, Per, Aase, Solveig, Aase.

If however ϕ is bijective, the count is correct and every element is listed exactly once. In that case we obviously have $|A| = n$. We formalize this as a proposition:

Proposition 10 *Assume that A is a set. Then there is a bijection from I_n to A if and only if there are exactly n elements in A, i.e., if and only if $|A| = n$. More generally: Two sets have the same number of elements if and only if there is a bijection between them.*

The second statement follows, since if there are bijections from I_n to both sets, say ϕ and ψ, one obtains a bijective map between the two sets by composing one of them with the inverse of the other, e.g., $\phi \circ \psi^{-1}$.

If $\phi\colon I_n \to A$ is injective, no element is listed twice, so clearly $|A| \geq n$. The inequality is strict if and only if some element in A is not among the listed ones, which means that there are members of A not in the image of ϕ. Or rephrased, ψ is not surjective. Replacing I_n with any set B having n elements, we get:

Proposition 11 *Let $\phi\colon B \to A$ be an injective map between finite sets. Then $|B| \leq |A|$ with equality if and only if ϕ is bijective.*

In a similar manner if ψ is surjective, every element is counted at least once, and this implies that $|A| \leq n$. The inequality is strict if and only if some element is counted at least twice, i.e., if and only if ϕ is not injective. Hence

Proposition 12 *Let $\phi\colon A \to B$ be a surjective map between finite sets. Then $|B| \leq |A|$ with equality if and only if ϕ is bijective.*

These two propositions are very useful when it comes to proving that a mapping between finite sets is bijective knowing the two sets are of the *same cardinality*. It suffices to check either injectivity or surjectivity of the mapping. This is comparable to the situation in linear algebra when one is to show that a linear map between two vector spaces of the *same dimension* is an isomorphism — it suffices to prove the map to be injective or surjective.

Proposition 13 *Let A and B be two finite sets. Then $|A \times B| = |A||B|$. More generally, if $\mathscr{A}$ is a finite family of finite sets, then*

$$|\prod_{A\in\mathscr{A}} A| = \prod_{A\in\mathscr{A}} |A|$$

or expressed in words, the cardinality of a finite product of finite sets is the product of the cardinalities of the factors.

Proof. By induction, the general case follows from the case of two sets. Now the elements in $A \times B$ are pairs (a, b) where a is freely chosen from A and b freely choose from B. For each a there are $|B|$ different choices for b, and as there are $|A|$ different ways of choosing a, we altogether get $|B||A|$ different pairs. □

The following is a slight generalization of this proposition which later will turn out to be useful at a few occasions— the proof is left as an (useful) exercise to the reader (so give it a try!):

Proposition 14 *Let A and B be finite sets, and let $\phi\colon A \to B$ be a mapping. Assume that the all $b \in B$, the fibers $\phi^{-1}(b)$ have the same number of elements. Then for any $y_0 \in B$ we have*

$$|A| = |B| \cdot |\phi^{-1}(y_0)|.$$

Proposition 15 *Let A be a finite set having n elements. Then the number of different bijections from I_n to A equals $n!$.*

Proof. If we are to define a bijection $\psi\colon I_n \to A$, we may choose $\psi(1)$ freely among the members of A. This gives us n possibilities. To be sure of ψ being injective, we must avoid $\psi(1)$ when choosing $\psi(2)$, a part from that, it may be chosen freely. Hence there are $n-1$ possibilities. Similarly there are $n-2$ possibilities for choosing $\psi(3)$, and in general we may choose $\psi(i)$ freely among $n-i+1$ possibilities. Altogether, this gives

$$n(n-1)(n-2)\cdot\cdots\cdot(n-i)\cdot\cdots\cdot 2\cdot 1 = n!$$

possibilities for ψ. □

WE shall finish this paragraph with a well known result, here formulated as a statement about the number of different subsets of a finite set with a given number of elements. It may be interpreted as the number of ways to chose a given number of elements from a given set, which is obviously the same.

We remind you that the binomial coefficient $\binom{n}{k}$ is given as

$$\binom{n}{k} = \frac{n!}{(n-k)!k!} = \frac{n\cdot(n-1)\cdot\cdots\cdot(n-k+1)}{k!}.$$

Proposition 16 *Given a set A with $|A| = n$. Then the number of subsets of A with k elements is equal to $\binom{n}{k}$.*

Proof. Let $B \subseteq A$ denote a subset of cardinality k. The first element in B may be chosen i n different way. For the next one, which must be different from the first, we have $n-1$ possibilities, for the one after there are $n-2$ possibilities, etc. This gives $n\cdot(n-1)\cdot\cdots\cdot(n-k+1)$ possibilities altogether. The same element but in a different order give the same subset, so we have to divide that number by the number of ways to order k elements. But that we saw, is $k!$. □

Partitions (***)

There are two concepts that will be used extensively in this course, namely the concepts of partitions and equivalence relations. So it will be of great help to grasp these concepts properly. Teachers of mathematics know by experience that the students often find them difficult.

We start by defining a *partition* (•*partisjon, oppdeling*) of a set A. It is nothing but — well, a partition! That is a family of subsets of A — which we shall denote by $\mathscr{P}$ and whose elements we shall call the *parts* or *classes* (•*deler, klasser*) — with the two properties formulated in the following definition

Definition 1 *A* partition $\mathscr{P}$ *of a set* A*, is a family of subsets such that*

(i) *The sets in* $\mathscr{P}$ *covers* A*; that is*

$$\bigcup_{P\in\mathscr{P}} P = A.$$

(ii) *The parts of* $\mathscr{P}$ *are mutually disjoint; that is, if* $P, P' \in \mathscr{P}$ *and* $P \neq P'$*, then*

$$P \cap P' = \emptyset$$

EXAMPLE 12 We can divide the integers into the two classes consisting of the *even* and *odd* integers respectively. Let $P_0 = \{\, 2k \mid k \in \mathbb{Z} \,\}$ and $P_1 = \{\, 2k+1 \mid k \in \mathbb{Z} \,\}$. They are clearly disjoint — an integer cannot at the same time be both even and odd — and they cover $\mathbb{Z}$ since any integer is either odd or even. So $\mathscr{P} = \{\, P_0, P_1 \,\}$ is a partition of $\mathbb{Z}$.

Let us go a step further. The even integers are those divisible by two, and the odd ones those that are not. We can do similar things with *three* in stead of *two*, and divide the integers into those divisible by three and those that are not. This certainly gives a partition of $\mathbb{Z}$, but we want to divide $\mathbb{Z}$ further.

If a is an integer not divisible by 3, there are two cases. Either a behaves like $1, 4, 7, 10, \ldots$ (or like $-2, -5, -8, \ldots$ for that matter), in which case $a = 3q + 1$ for $q \in \mathbb{Z}$. The set of those numbers will be denoted by P_1. In the other case, a behaves like $2, 5, 8, 11, \ldots$ (or like $-1, -4, -7, \ldots$) and $a = 3q+2$. Those integers form a subset we shall call P_2.

In this way we have constructed a partition of $\mathbb{Z}$ into three parts, $\mathscr{P} = \{\, P_0, P_1, P_2 \,\}$, where P_0 denotes the class of integers divisible by 3. In figure 1 above, the elements of P_0 are indicated by a red circle • those in P_1 by a yellow one • and those in P_2 by an orange one •

Figure 1: *The partition of the integers $\mathbb{Z}$ in three parts after their rest when divided by 3.*

Naming the classes (**)

The names P_0 and P_1 are of course no good names for the sets of even and odd numbers, the only reason they were chosen was to illustrate the definition. Better names would be *even* and *odd*, and even better ones would be one of the at least two frequently used conventions for naming parts of a partition, which we will now describe. We start with a rather obvious lemma:

Lemma 1 *Suppose that A is a set with a partition $\mathscr{P}$. Then every element in A is contained in exactly one class P from $\mathscr{P}$.*

Proof. Let $a \in A$. That a is contained in *at most* one part follows because the parts are mutually disjoint — i.e., $P \cap P' = \emptyset$ if $P \neq P'$ — and since the members of $\mathscr{P}$ covers A — i.e., $\bigcup_{P \in \mathscr{P}} P = A$ — the element a lies in *at least* one part. □

Now, for any element $a \in A$, we let $[a] \in \mathscr{P}$ denote the unique part to which a belongs. Then obviously $[a] = [a']$ if and only if the two elements a and a' belong to the same part. Every part in $\mathscr{P}$ is of the form $[a]$, hence have

$$\mathscr{P} = \{\, [a] \mid a \in A \,\}$$

Be warned, in this description of the set $\mathscr{P}$ there are a lot repetitions! In fact a part P is repeated as many times as it has elements. We shall call a a *representative* (•*representant*) for the part where it belongs.

In our first example of even and odd integers, the class of even integers equals $[a]$ for any even integer $a = 2k$; the far most commonly used is of course $[0]$, but you may very well use $[2]$ or $[-2]$ or $[12]$ or $[98765432]$ or ....

Similarly, the other class — the one where the odd numbers belong — may be written $[2k+1]$ for any odd integer $2k+1$; the most common being $[1]$. We thus have

$$\mathscr{P} = \{\, [a] \mid a \in Z \,\} = \{\, [1], [0] \,\}$$

In the first description, there are a lot of repetitions, in fact infinitely many (e.g., the class of even numbers is repeated once for each even number), but in the second there

are non. We have chosen *exactly* one representative from each class. Such a choice of elements is called a *set of representatives* (•*et sett av representanter*) for the partition.

In our second example — where we classified the integers according to their rest after being divided by three — a set of representatives would be $\{0, 1, 2\}$. This is by far the most common one, although $\{-1, 0, 1\}$ is also quite popular. Any choice would do, like $\{-31, -272, 357\}$, but would be a utterly stupid choice unless there is a particular reason behind. The best is to keep the representatives as simple as possible.

Naming some partitions (∗)

The name $\mathscr{P}$ of these partitions we so far has studied, is as bad as P_0, P_2 and P_2 were for the parts, and it was only chosen for the same reason, to illustrate definition 17. Again there are several conventions, but $\mathbb{Z}_p$ or $\mathbb{Z}/p\mathbb{Z}$ are the most frequent ones, where $p = 2$ in our first example and $p = 3$ in the second. To sum up:

$$\mathbb{Z}_3 = \{[0], [1], [2]\} = \{[0], [1], [-1]\}$$

and

$$\mathbb{Z}_2 = \{[0], [1]\}.$$

We promised *two* standard notations for the classes of a partition. The other one is similar to the one we just described, it works in exactly the same manner, the only difference being notational. The part containing a is denoted by $\bar{a}$, so if you want, $[a] = \bar{a}$. Both ways are convenient and will used in the course.

EXAMPLE 13 Let us give a last concrete example, which is very well known from every day life. We shall let A be the set of dates, and not to complicate the matters unnecessarily [1] we shall start at 1. January 1900 and end at 31. December 2010. So

$$A = \{\ 1\text{JAN}1900,\ 2\text{JAN}1900,\ 3\text{JAN}1900, \ldots,\ 31\text{DEC}2020\}.$$

Now, every date is also a weekday, hence we may divide A into seven parts, the mondays, the tuesdays etc. In that way we get a partition of all dates, labeled by the weekdays.

With a few changes, we can connect this example with two first. First let us extend the time line to far beyond doomsday and backwards to far beyond big bang. Secondly we assume the calendar we use to day, has been in use at all times (which is far from

[1] Many different calenders have in use. The one we use today in our part of the world, the Julian calender was introduced in catholic countries in xxxx, in England and Sweden in ... and i Sovjet Union in ...

the truth). Finally we choose a *first date*, that is a date from which we count all other date. The dates before the first date have a negative sign and the ones after a positive. In this way, our dates are numbered, and the calendar (i.e., the set of dates) has become identified with $\mathbb{Z}$.

Now the first date was of course a sunday — and as the week has seven days, every sunday has a number of the form $7n+1$. Similarly, the day zero, that is the date before the first date, was a saturday. Hence every saturday has a number divisible by 7. And so on, mondays are of the form $7n+2$, tuesdays of the form $7n+3$, etc.

We end up with the partition

$$\mathbb{Z}_7 = \{\, [0], [1], [2], [3], [4], [5], [6] \,\}$$

of the integers.

Other "temporal" examples can be made with $p = 24$, $p = 365$, etc. Every time one has a cyclic phenomena, a similar reasoning may be applied.

All this to show you that the partitions $\mathbb{Z}_p$ are not too farfetched, as least some of them are common in every day life.

Mappings again (*)

A general way of generating partitions is via maps. The fibers of a map $\phi\colon A \to B$ are all subsets of the source A, and they are mutually disjoint. Indeed, if $a \in \phi^{-1}(b) \cap \phi^{-1}(b')$, then we have

$$b = \phi(a) \text{ and } b' = \phi(a)$$

so $b = b'$ and hence $\phi^{-1}(b) = \phi^{-1}(b')$. Clearly the fibers cover A, since $a \in \phi^{-1}(\phi(a))$. We have proved:

Proposition 17 *Let $\phi\colon A \to B$ be a map. Then the set of* fibers *of ϕ forms a partition of A, i.e.,*

$$\mathscr{P}_\phi = \{\, \phi^{-1}(b) \mid b \in B \,\}$$

is a partition of A.

This example is not only general, it is in fact *universal*! Meaning that any partition arises in this way — as the set of fibers of a map.

Indeed, let A be a set and $\mathscr{P}$ a partition of A. We just introduced the notation $[a]$ for the class to which the element a belongs. This is however much more than just a naming of that class, it defines a mapping $\pi_{\mathscr{P}} : A \mapsto \mathscr{P}$ by sending a to $[a]$!

Now we checked the (obvious[2]) fact that $[a] = [a']$ if and only if they belong to the same class which means that the fiber of $\pi_{\mathscr{P}}$ over a class P equals P. Indeed, chose a representative a for P, then $[a] = P$, and we have

$$\pi_{\mathscr{P}}^{-1}([a]) = \{\, a' \mid [a'] = [a] \,\} = \{\, a' \mid a' \in [a] \,\} = [a].$$

□

We sum up:

Proposition 18 *Let A be a set and $\mathscr{P}$ a partition of A. Then the mapping $A \mapsto \mathscr{P}$ defined by $a \mapsto [a]$ has as fibers the classes in $\mathscr{P}$, the fiber over $P \in \mathscr{P}$ being P.*

More counting (∗)

We shall need a few counting results involving partitions. They are rather obvious and easy to prove, but useful at occasions. The basic one is this:

Proposition 19 *Let A be a finite set, and let $\mathscr{P}$ be a partition of A. Then every part in $\mathscr{P}$ is (of course) finite, and we have*

$$|A| = \sum_{P \in \mathscr{P}} |P|$$

Proof. As any element of A is in exactly one class, this is obvious. □

Proposition 20 *Let $\phi\colon A \to B$ be a map between finite sets. Then*

$$|A| = \sum_{b \in B} |\phi^{-1}(b)|.$$

Proof. We saw that the set of fibers $\{\, \phi^{-1}(b) \mid b \in B \,\}$ forms a partition of A. The proposition follows then from proposition 21 which we just proved. □

[2]We insist that this is obvious. The equality says that a and a' are in the same class if and only if they are in the same class! This may look stupid, but obvious things like that are often important — not deep, but important — in mathematics. There is even a name for them; they are called *tautologies*.

Equivalence relations (**)

The other important concept we mentioned in the pargraph about partitions, is the concept of an equivalence relation. As we shall see, the two concepts — partitions and equivalence relations — are tightly connected.

A *relation* (•*relasjon*) on a set, or a *binary relation* (•*binær relasjon*) to be precise, is a subset $R \subseteq A \times A$; binary meaning that we are comparing *two* an *two* elements from A. We say that x is related to y, if $(x, y) \in R$, and we write $x \sim_R y$. To simplify the notation, we often suppress the reference to R if there is a marginal danger of misunderstanding, and just write $x \sim y$.

A relation is called an *equivalence relation* (•*ekvivalensrelasjon*) if the following conditions are satisfied for any elements x, y and $z \in A$

(i) *Reflexivity:* (•*Refleksivitet*) $x \sim x$.

(ii) *Symmetry:* (•*Symmetri*) $x, y \in A$ $x \sim y$ if and only if $y \sim x$.

(iii) *Transitivity:* (•*Transitivitet*) If $x \sim y$ and $y \sim z$ then $x \sim z$.

Equality is a basic example of an equivalence relation, and the three conditions are modelled on well known properties of equality.

Equivalence relation are quite special realtions, and it is important to understand that there are many, many other relations. There is one well known just at hand, namelig "less than ", i.e., the underlying set is the reals, and x is related to y if $x > y$. This relation is far from being symmetric, and it is not even reflexive (since we chose to use a strict inequality), although it is transitive.

Given an equivalence relation, we can partition our set into so called *equivalence classes*. For any $a \in A$ we define[3]

$$[a] = \{\, a' \in A \mid a' \sim a \},$$

and called it the *equivalence class* (•*ekvivalensklasse*) where a belongs. The symmetry condition (ii) above states that $a' \sim a$ if and only if $a \sim a'$, which translated into the language of equivalence classes means that $a' \in [a]$ if and only if $a \in [a']$. So we have

$$[a] = \{\, a' \in A \mid a \sim a' \}.$$

From the reflexivity condition (i) above it follows that $a \in [a]$.

The fundamental (in this context) observation, is that

[3] This notation is very close to the one we used on page 18 when we spoke about partitions. That is no coincidence, and the reason will become clear in a while.

Lemma 2 *If $a' \in [a]$, then $[a] = [a']$.*

Proof. First of all, since $a' \in [a]$ we have $a \sim a'$. If $a'' \in [a]$ is another element, the definition of $[a]$ gives $a'' \sim a$ and by transitivity we get $a'' \sim a'$. Thus $[a] \subseteq [a']$. Then $a \in [a']$, and by a symmetric argument — which means repeting the argument with the roles of a and a' interchanged — we get $[a'] \subseteq [a]$. □

We want to emphasize that the result in lemma 2 of course is special to *equivalence* relations. It is not true for most other relations, and it is certainly false for the relation $x > y$ on the reals (be sure you understand that).

Proposition 21 *The set of equivalence classes is a partition of A*

Proof. We have have to prove two things; that the equivalence classes cover A, and that they are mutually disjoint. The first follows by the remark above that reflexivity implies $a \in [a]$.

The second follows from the lemma. Indeed, we have to show that two equivalence classes are either disjoint or equal, so assume $b \in [a] \cap [a']$. Then by applying the lemma twice — first to a and b and then to a' and b — we get $[a] = [b] = [a']$. □

We have just seen that the equivalence classes of an equivalence relation forms a partition. This also works the other way around. Given a partition $\mathscr{P}$ of a set A, there is a natural way to define an equivalence relation on A with the property that the equivalence classes are exactly the classes of $\mathscr{P}$.

Lingering a little over that last sentence — it makes it clear what we have to do: We define $a \sim_{\mathscr{P}} b$ to mean that a and b are in the same class from $\mathscr{P}$. The work to be done, is to check that this indeed is an equivalence relation — that is, it satisfies the three axioms above.

Proposition 22 *With the notation above, $a \sim_{\mathscr{P}} b$ is an equivalence relation.*

Proof. We must check the three conditions above.
Because $a \in [a]$[4] our relation $a \sim_{\mathscr{P}} b$ is reflexive. The statement "a and b belong to the same class frm $\mathscr{P}$" is symmetric in a and b. This takes care of the symmetry condition.

The last challenge is the transitivity: So let $a \sim_{\mathscr{P}} b$ and $b \sim_{\mathscr{P}} c$. Then a and b belong to a common class, say P, and b and c to a common class P'. Now b belongs to both P and P', so $P \cap P' \neq \emptyset$. Since $\mathscr{P}$ is a partition, two classes from P are either disjoint or equal, hence $P = P'$. This means that a and c belong to the same class. Hence $a \sim_{\mathscr{P}} c$. □

[4]This now denotes the part of $\mathscr{P}$ where a belongs

Congruences (∗)

One of the earliest equivalence relations (not being equality), to appear in mathematics, is the relation which somehow loosely can be described as "being congruent to mod n". It can be traced back to the antique times, both in Greece, Babylon and India the old mathematicians used it in one way or other. And it is omnipresent in modern mathematics.

We certainly shall come back to it later in the course, with much more complete treatment — this is just a teaser!

The underlying set of the relation is the set $\mathbb{Z}$ of integers, and we chose a number n which is called the *modulus* (• *modulus*)— for example $n = 2$, $n = 3$ or $n = 7$ are all great choices, but any number will do equally well.

We say that to integers x and y are *congruent modulo* n (• *kongruente modulo* n), if their difference is divisible by n — i.e., if $x - y = qn$ for an integer $q \in \mathbb{Z}$. We write

$$x \equiv y \mod n. \tag{♠}$$

Here comes a few examples:

EXAMPLE 14 Two even numbers are congruent mod 2 — likewise are two odd.
A number x is even if and only if $x \equiv 0 \mod 2$.
All saturdays are congruent mod 7!! And, in fact, an integral number x is divisible by 7 if and only if $x \equiv 0 \mod 7$.
Any two numbers of the form $24q + 1$ with $q \in \mathbb{Z}$ are congruent mod 24, and they all satisfy[5]

$$24q + 1 \equiv 1 \mod 24$$

It remains to be proven that we in fact have an equivalence relation:

Proposition 23 *Let $n \in \mathbb{Z}$. The relation $x \equiv y \mod n$ is an equivalence relation.*

Proof. Obviously $x - x = 0 \cdot n$ is divisible by n. So by (♠) $x \equiv x \mod n$, and reflexivity holds.

As obvious, if $x - y$ is divisible by n so is $y - x$; indeed, if $x - y = qn$ with q an integer then $y - x = (-q)n$ and of course $-q \in \mathbb{Z}$ as q is. Hence by (♠) $x \equiv y \mod n$ implies $y \equiv x \mod n$, and symmetry holds.

Finally, suppose that

$$x \equiv y \equiv n \text{ and } y \equiv z \mod n.$$

[5]This is close to a *tautology*.

By definition (♠) that means that

$$x - y = qn \text{ and } y - z = q'n$$

where both q and q' are integers. By adding the two equalities we obtain

$$x - z = (x - y) + (y - z) = qn + q'n = (q + q')n,$$

and $q + q' \in \mathbb{Z}$. That is $x \equiv z \mod n$, and transitivity is established. □

The equivalence classes corresponding to the relation $x \equiv y \mod n$ are called the *congruences classes* $\mod n$ (•*restklasser modulo* n *eller mod* n).

The final examples

Let us take a closer look on few cases, and we start with $n = 2$. There are two classes, one with even n's odd and one for odd. So we are back to our earlier partition from page 17, which babtized $\mathbb{Z}_2$.

In a similar way, we looked at $\mathbb{Z}_3$ and $\mathbb{Z}_7$, they both fit into the same pattern. In school we learned to divide one integer by another and we learned that by dividing x by n we get a quotient q and a rest r satisfying

$$x = qn + r$$

where q and r are integers, and the rest r lies between 0 and n — 0 allowed, not n.

For example, if $n = 3$, any integral number x can be written $3q + r$ with $r = 0, 1$ or 2. So the congruence classes are $[0], [1]$ and $[2]$, which we recognize from the examples on page 17.

January 13, 2011