Chapter 5

Relations and Partitions

Idea. We defined congruence modulo m. This is an example of a *relation* on the set $\mathbb{Z}$ of integers. Moreover, this relation satisfies the three properties of being reflexive, symmetric and transitive. We then defined congruence classes, using congruence modulo m. The classes satisfy the properties of being disjoint and the union of them containing every integer.

We now generalize the ideas of congruences and congruence classes of $\mathbb{Z}$ to *any* set X and introduce the notion of relation, equivalence relation, equivalence class and partition. We show that congruence modulo m is an equivalence relation so that all the properties of congruence classes follow.

Relations

Definition (relation)**.** A **relation** on a set X is a subset $\mathcal{R} \subseteq X \times X$, i.e. a collection of ordered pairs of elements of X.

If a **set** $\mathcal{R} \subseteq X \times X$ is given, for every $a, b \in X$ we define the **statement** $a \,\mathcal{R}\, b$, as follows:

1. If $(a, b) \in \mathcal{R}$, the statement $a \,\mathcal{R}\, b$ is true, and we say that a **is related to** b.
2. If $(a, b) \notin \mathcal{R}$, the statement $a \,\mathcal{R}\, b$ is false. We say that a is not related to b. Sometimes we write $a \not\mathcal{R}\, b$.

Remark (two ways of writing a relation)**.** We can see from the definition that a relation can either be written as a **set** of ordered pairs, or as a **predicate** $a \,\mathcal{R}\, b$ which takes two arguments, a and b, from the set X and outputs True or False. We will use both notations.

Example. (i) Four different relations on $\mathbb{Z}$ are

a) Strict order relation, $a < b$.

b) Equality relation, $a = b$.

c) Congruence mod 7, $a \equiv b \mod 7$.

d) The empty relation: a is not related to b for all $a, b \in \mathbb{Z}$.

In cases a),b),c) the relation written as a **set** of pairs is an infinite set. For example, the equality relation is the set $\{(a, a) : a \in \mathbb{Z}\}$. This is a subset of $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ sometimes called the *diagonal*.

In the case d), the empty relation is very easy to write as a set: $\mathcal{R} = \varnothing$.

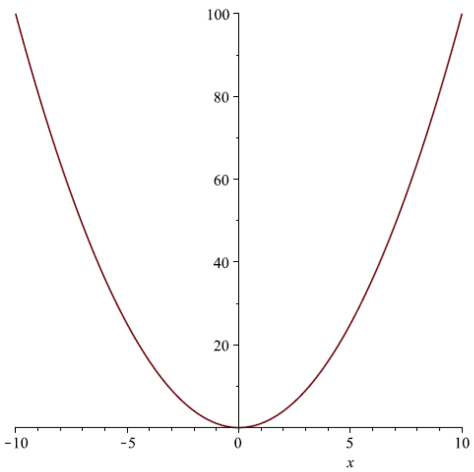
(ii) If $A = \{a, b, c, d, e, f\}$ (set of six letters), then

$$\mathcal{R} = \{(a, a), (a, b), (b, a), (b, b), (c, c), (c, e), (e, c), (e, e), (d, d), (f, f)\}$$

is a relation on A. Statements $e \mathcal{R} c$ and $d \mathcal{R} d$ are true and, for example, the statement $a \mathcal{R} d$ is false. We may thus write: $e \mathcal{R} c$, $d \mathcal{R} d$, $a \not\mathcal{R} d$.

(iii) $\mathcal{R} = \{(x, x^2) : x \in \mathbb{R}\}$ is a relation on $\mathbb{R}$.

This relation is also the graph of the function $f \colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$. This can be represented pictorially as



So the set $\mathcal{R}$ is the parabola, a subset of the Cartesian plane.

Remark. In fact, the graph of any function $f\colon X \to X$ — i.e., a function where the domain and the codomain are the same set — is a relation:

$$G_f = \{(x, f(x)) : x \in X\} \subseteq X \times X.$$

But the converse is not true, not all relations are graphs of functions.

Example. If $X = \{1, 2, 3\}$ then

a) the relation $\mathcal{R}_1 = \{(1,1), (2,2)\}$ is **not** the graph of a function since 3 is not related to anything, i.e. it has no image,

b) the relation $\mathcal{R}_2 = \{(1,1), (2,3), (1,2), (3,2)\}$ is **not** the graph of a function since 1 has two images.

Equivalence Relations

Idea. If a relation on a set X obeys three rules known as reflexivity, symmetry and transitivity, it is called an *equivalence relation*. Some of the most important relations are equivalence relations, and in this course one of them is $\equiv$ mod m, the congruence mod m relation, on the set $\mathbb{Z}$. Unless a specific symbol is already used (such as the symbol $=$ for the equality relation or the symbol $\equiv$ mod m for the congruence relation), equivalence relations are usually written as $a \sim b$, read "*a is equivalent to b*". $\sim$ is the *tilde* symbol (also called 'twiddle').

Definition (Equivalence relation)**.** Suppose that $\sim$ is a relation on a set X. Then

i) $\sim$ is **reflexive** if $\forall a \in X \ a \sim a$;

ii) $\sim$ is **symmetric** if $\forall a, b \in X \ (a \sim b \implies b \sim a)$;

iii) $\sim$ is **transitive** if $\forall a, b, c \in X \ ((a \sim b \wedge b \sim c) \implies a \sim c)$.

If $\sim$ satisfies **all** three properties then we say that $\sim$ is an **equivalence relation**.

Note that in (ii) or (iii) the elements $a, b \in X$ or $a, b, c \in X$ need **not** be different.

Example (The strict order relation on $\mathbb{Z}$ is not an equivalence relation)**.** Consider the strict order relation on the set $\mathbb{Z}$: a is related to b iff $a < b$. This relation:

Is **not reflexive** since $1 \not< 1$,

Is **not symmetric** since $1 < 2$ but $2 \not< 1$,

Is transitive, since if $a < b$ and $b < c$ then $a < c$. Is **not** an equivalence relation.

Remark (How to prove or disprove properties of a relation?)**.** If a property does not hold, give a *counterexample*, if it does hold try to give a proof. For example, one may prove that the relation $<$ is transitive, as follows: $a < b$ and $b < c$ means $0 < b - a$ and $0 < c - b$. We use the fact that the sum of two positive numbers is positive, so we add the two inequalities together to get $0 < (b - a) + (c - b) = c - a$, which implies $a < c$.

Example (The relation "**divides**" on $\mathbb{Z}$)**.** Consider the relation $\mid$ on $\mathbb{Z}$, where a is related to b iff $a \mid b$ (a divides b).

The relation $\mid$ **is reflexive**, since $\forall a \in \mathbb{Z}$, $a \mid a$.

Is **not symmetric** since $5 \mid 20$ but $20 \nmid 5$.

Is transitive, because for all $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$ (exercise, see homework).

Example (Some examples of relations on a finite set)**.** We consider simple examples of relations on the set $\mathbb{N}_3 = \{1, 2, 3\}$. In each example, we determine whether the relation is reflexive, symmetric, transitive and is an equivalence relation.

(i) $\mathcal{R}_1 = \{(1,2)\,, (2,1)\,, (3,3)\}$.

Is **not** reflexive since $(1,1) \notin \mathcal{R}_1$;

Is symmetric. (Check that if $(a,b) \in \mathcal{R}_1$ then $(b,a) \in \mathcal{R}_1$. There are three checks to be made.)

Is **not** transitive since $(1,2)\,, (2,1) \in \mathcal{R}_1$ but $(1,1) \notin \mathcal{R}_1$ (so $a = 1$, $b = 2$ and $c = 1$ in the definition of transitive, highlighting the point above that a, b, c need **not** be different).

Is not an equivalence relation (e.g., because it is not reflexive).

(ii) $\mathcal{R}_2 = \{(1,1)\,, (2,2)\,, (3,3)\}$.

Is reflexive, symmetric and transitive, hence is an equivalence relation. It is easy to see that $a\,\mathcal{R}_2\,b$ means $a = b$.

Example (Very important — congruence mod m is an equivalence relation)**.** $\equiv$ mod m is an equivalence relation on the set $\mathbb{Z}$.

This is proved in Proposition 3.1 where we establish that congruence mod m is reflexive, symmetric and transitive.

Partitions

Idea. Informally, a partition is a splitting of a set X into non-empty subsets. We will show that every equivalence relation on X creates (*induces*) a partition of X. It is also true that every possible partition is induced by an equivalence relation.

Definition. Let X be a set. A **partition** Π of X is a collection of non-empty disjoint subsets of X that cover X. That is,

$$\Pi \subseteq \mathcal{P}(X),$$

and

i) the sets in Π are *non-empty*, so
$$\forall A \in \Pi \quad A \neq \varnothing,$$

ii) the sets in Π are *disjoint*, so
$$\forall A_1, A_2 \in \Pi \quad A_1 \neq A_2 \implies A_1 \cap A_2 = \varnothing,$$

iii) the sets *cover* X, i.e. $X = \bigcup_{A \in \Pi} A$ (the union of all parts of Π is X), or equivalently,
$$\forall x \in X \quad \exists A \in \Pi : \ x \in A.$$

We call the sets in Π the **parts** of the partition.

Example (Examples and non-examples of partitions)**.** (a) Some possible partitions of $\mathbb{Z}$:

(i) $\Pi = \{\{\text{odd integers}\}, \{\text{even integers}\}\} = \{[0]_2, [1]_2\} = \mathbb{Z}_2$. Yes, $\mathbb{Z}_2$ is a partition of $\mathbb{Z}$ into two parts.

(ii) $\Pi = \{\{n \in \mathbb{Z} : n < 0\}, \{0\}, \{n \in \mathbb{Z} : n > 0\}\}$.

(b) But $\{\{n \in \mathbb{Z} : n < 0\}, \{n \in \mathbb{Z} : n > 0\}\}$ is **not** a partition of $\mathbb{Z}$ since 0 is in no part.

Similarly $\{\{n \in \mathbb{Z} : n \leq 0\}, \{n \in \mathbb{Z} : n \geq 0\}\}$ is **not** a partition of $\mathbb{Z}$ since the parts are not disjoint.

(c) If $X = \{a, b, c, d, e, f\}$ then

$$\Pi = \{\{a, b\}, \{c, e\}, \{d\}, \{f\}\}$$

is a partition of X.

(d) $\Pi = \{[n, n+1) : n \in \mathbb{Z}\}$ is a partition of $\mathbb{R}$. Recall that $[n, n+1)$ is the half-open interval $\{x \in \mathbb{R} : n \leq x < n+1\} \subseteq \mathbb{R}$.

Just as we went from congruences (equivalence relations on $\mathbb{Z}$) to congruence classes (a partition of $\mathbb{Z}$) we can go from any equivalence relation on a set X to a partition of X.

Definition (equivalence classes)**.** Suppose that $\sim$ is an equivalence relation on a set X. For each $a \in X$ define the **equivalence class of** a to be the set of elements of X related to a. Denote this class by $[a]$ so

$$[a] = \{x \in X : x \sim a\} .$$

We write

$$X/\!\sim\; = \{[a] : a \in X\} .$$

Example ($\equiv$ mod m and $\mathbb{Z}_m$)**.** When $X = \mathbb{Z}$ and $a \sim b$ was defined as $a \equiv b \mod m$ we wrote

- $[a]_m$ in place of $[a]$;
- $\mathbb{Z}_m$ in place of $\mathbb{Z}/\left(\equiv \bmod m\right)$.

Remark (Arithmetic operations on $\mathbb{Z}_m$)**.** What we managed to do for $\mathbb{Z}_m$ was to define addition and multiplication on $\mathbb{Z}_m$. That would be the aim with other examples of X and $\sim$ in but this is **not** achieved in this course. See Algebraic Structures.

Theorem 5.1 (Equivalence classes coincide or are disjoint, and form a partition)**.** Suppose that $\sim$ is an equivalence relation on a set X. Then for $a, b \in X$,

i) If $a \sim b$ then $[a] = [b]$,

ii) If $a \nsim b$ then $[a] \cap [b] = \varnothing$.

Hence $X/\!\sim$ is a partition of X.

Proof. i) Assume that $a \sim b$. Take any $x \in [a]$. By definition of $[a]$, $x \sim a$; also $a \sim b$ so by transitivity, $x \sim b$, so $x \in [b]$. We have proved that $[a] \subseteq [b]$. Now, $a \sim b$ implies by symmetry that $b \sim a$ as well, hence the same argument will show $[b] \subseteq [a]$. We conclude that $[a] = [b]$.

ii) We prove the contrapositive: $[a] \cap [b] \neq \varnothing \implies a \sim b$, which is logically equivalent to ii). Assume that $[a] \cap [b] \neq \varnothing$, meaning that $\exists c$: $c \in [a]$ and $c \in [b]$. Then $c \sim a$, so by symmetry $a \sim c$. Also, $c \sim b$. Then by transitivity $a \sim b$, as required.

It remains to show that $X/\!\sim$ is a partition of X. By i) and ii), elements of $X/\!\sim$ (the equivalence classes) are disjoint. We now observe that each equivalence class, $[a]$, is non-empty, because by reflexivity, $[a]$ contains a. Also, equivalence classes cover all elements of X; indeed, $\forall a \in X$ $a \in [a]$. We have thus **verified the definition** of a partition for $X/\!\sim$. $\square$

Example. Let $X = \mathbb{Z}$ and $\sim$ be given by $x \sim y$ if, and only if, $(x-y)(x+y)$ is divisible by 7. Show that $\sim$ is an equivalence relation. Describe the equivalence classes.

Solution. To show that $\sim$ is an equivalence relation, write $(x-y)(x+y)$ as x^2-y^2. Thus, $x \sim y$ iff $7 \mid (x^2-y^2)$.

$\sim$ *is reflexive*: let $x \in \mathbb{Z}$. As $7 \mid 0$, $7 \mid (x^2-x^2)$ and so $x \sim x$. Reflexivity is proved.

$\sim$ *is symmetric*: let $x, y \in \mathbb{Z}$ and assume $x \sim y$. Then $7 \mid (x^2-y^2)$ so $x^2-y^2 = 7k$ for some integer k. Then $y^2-x^2 = 7(-k)$ so 7 divides y^2-x^2 and so $y \sim x$. Symmetry is proved.

$\sim$ *is transitive*: let $x, y, z \in \mathbb{Z}$ and assume $(x \sim y) \wedge (y \sim z)$. Then $x^2-y^2 = 7k$ and $y^2-z^2 = 7\ell$ for some integers k, ℓ. Adding these together, $x^2-z^2 = 7k+7\ell = 7(k+\ell)$. So $7 \mid (x^2-z^2)$ and so $x \sim z$. Transitivity is proved.

Let us construct the equivalence class $[0]$ of 0. We have $x \in [0]$ iff $x \sim 0$ iff $7 \mid (x^2-0)$, i.e., x^2 is divisible by 7. Look at the table where the possible remainders of x^2 mod 7 are given:

$x \mod 7$	0	1	2	3	4	5	6
$x^2 \mod 7$	0	1	4	2	2	4	1

From the table, x^2 is divisible by 7 iff $7 \mid x$. Hence $[0]$ is the set of all integers divisible by 7.

We have not exhausted the set $\mathbb{Z}$ yet, so let us take an integer not in $[0]$; say, 1. To describe $[1]$, note that $x \in [1]$ iff $7 \mid (x^2-1)$ iff $x^2 \equiv 1 \mod 7$. From the table, this happens when $x \equiv 1 \mod 7$ or $x \equiv 6 \mod 7$. Thus $[1] = [1]_7 \cup [6]_7$.

The students should finish this example to show that all equivalence classes under $\sim$ are given in terms of congruence classes mod 7 as follows:

$$[1] = [1]_7 \cup [6]_7\,, \quad [2] = [2]_7 \cup [5]_7\,, \quad [3] = [3]_7 \cup [4]_7\,, \quad \text{and} \quad [0] = [0]_7\,.$$

From Partitions to Relations

This section may be omitted from lectures

Idea. We have seen that every equivalence relation on X induces a partition of X.

One may ask if all partitions of X arise in this way. We will now show that the answer is yes.

Definition. Given a partition Π of X define a relation $\sim_\Pi$ by

$$\forall a, b \in X, \quad a \sim_\Pi b, \text{ if, and only if, } \exists A \in \Pi : \ a, b \in A,$$

i.e. a and b lie in the same part of Π.

We say that $\sim_\Pi$ is the relation associated to Π.

Example. Let $A = \{a, b, c, d, e, f\}$ and $\Pi = \{\{a, c\}, \{b, d\}, \{e\}, \{f\}\}$ be a partition of A. Then

$$\begin{aligned} \mathcal{R}_\Pi &= \{(a, a), (a, c), (c, a), (c, c), (b, b), (b, d) \\ &\qquad\qquad (b, d), (d, b), (d, d), (e, e), (f, f)\}. \end{aligned}$$

Theorem 5.2. Let Π be a partition of X and $\sim_\Pi$ the associated relation. Then $\sim_\Pi$ is an equivalence relation.

Proof. Let Π be a partition of X. We need to prove that $\sim_\Pi$ is reflexive, symmetric and transitive.

Reflexive

Let $a \in X$. We need to prove that $a \sim_\Pi a$. By definition of a partition, there exists $A \in \Pi$ such that $a \in A$. It is then trivial to say that $a, a \in A$ which is the definition of $a \sim_\Pi a$.

Symmetric

Let $a, b \in X$. We assume that $a \sim_\Pi b$ and prove that $b \sim_\Pi a$.

By definition of $\sim_\Pi$ there exists $A \in \Pi$ such that $a, b \in A$. It is then trivial to say that $b, a \in A$ which is the definition of $b \sim_\Pi a$.

Transitive

Let $a, b, c \in X$. We assume $a \sim_\Pi b$ and $b \sim_\Pi c$, and prove that $a \sim_\Pi c$.

By assumption, there exist $A_1, A_2 \in \Pi$ such that $a, b \in A_1$ and $b, c \in A_2$. Here $b \in A_1$ and $b \in A_2$ means that $A_1 \cap A_2 \neq \varnothing$. But by the definition of a partition if parts are not disjoint they are identical, so $A_1 = A_2$ which we relabel as simply A. Thus $a, b, c \in A$. Here $a, c \in A$ is the definition of $a \sim_\Pi c$ as required. $\square$

Remark. One can start with a partition Π on X, consider the associated relation $\sim_\Pi$ and then induce a partition $X/{\sim_\Pi}$. It can be shown that $X/{\sim_\Pi} = \Pi$, i.e. you return to the beginning.

Alternatively you can start with a relation $\sim$ on X, induce a partition $\Pi = X/{\sim}$ and continue to induce a relation $\sim_\Pi$. Again you return to the beginning and obtain $\sim_\Pi = X/{\sim}$.