Lecture Notes for Abstract Algebra: Lectures 1 + 2

1 Lecture I: Notation and Introduction

1.1 Notation

This part contains some notation. We will use the term set to mean a collection of elements. We will use the symbol $\varnothing$ to denote the empty set with no elements. We often use capital letters (X, Y, A, B, etc.) to refer to sets and lowercase letters (x, y, a, b, etc.) to refer to elements. We will write $x \in X$ to mean that x is an element of a set X.

We will use the notation $A \subset B$ to mean that A is a subset of B, that is, to mean that the following implication is true: if $x \in A$, then $x \in B$. We can write this as:

$$\forall x,\, x \in A \Rightarrow x \in B.$$

In particular, for any set A it is true that $\varnothing \subset A$ and $A \subset A$.

Two sets A and B are equal if and only if both $A \subset B$ and $B \subset A$ are true. In such a case, we write $A = B$. Otherwise, we write $A \neq B$.

If we wish to emphasize that $A \subset B$ is true but that $A \neq B$, then we will write $A \subsetneq B$. In such a situation A is called a *proper* subset of B.

1.2 Relations and maps

Definition 1. For sets S, S', the Cartesian product $S \times S'$ is the set or ordered pairs

$$S \times S' = \{(x, y) \mid x \in S\, y \in S'\}.$$

A (binary) relation R between the sets S and S' is a subset of $R \subset S \times S'$. We write sometimes xRy when $(x, y) \in R$.

Definition 2. Let S be a set. **An equivalence relation** on S is a relation R on $S \times S$ satisfying the properties:

(1) R is reflexive: $(x, x) \in R$

(2) R is symmetric: $(x, y) \in R \iff (y, x) \in R$.

(3) R is transitive: $(x, y) \in R$ and $(y, z) \in R \Rightarrow (x, z) \in R$.

For $(x, y) \in R$, we use the notation xRy or $x \sim_R y$ or simply $x \sim y$.

Example 3. Let $S = \mathbb{Z}$ and $n > 0$ a natural number. The relation xRy iff n divides the difference $x - y$ is an equivalence relation. For more details on divisibility, we refer to the section on Integers.

Example 4. $(\mathbb{N}, \leq)$ is not symmetric but antisymmetric: xRy and $yRx \Rightarrow x = y$.

Example 5. Angle = equivalence in the set of couples of lines by $(0,0) \in \mathbb{R}^2$ module the relation of superposition.

Remark 6. Symmetric + transitive seems to imply reflexive: Consider the set of elements $S_x = \{y \in S \,|(x,y) \in R$. If $S_x \neq \emptyset$, and $y \in S_x$, then

$$xRy \Rightarrow yRx \Rightarrow xRx.$$

Except S_x may be empty!!

Definition 7. **A partition** of a set S is a collection of subsets $\{S_i\}_{i \in I}$ satisfying that $\cup_i S_i = S$ and

$$S_i \cap S_j \neq \emptyset \Rightarrow i = j.$$

Remark 8. An equivalence relation R determines a partition given by the equivalence classes:

$$\bar{x} = \bar{x}_R = \{y \in S \,|\, (x,y) \in R\}.$$

$\bar{x}_R \cap \bar{x}'_R \neq \emptyset \Rightarrow \exists y \in S$ such that $(x,y) \in R$ and $(x',y) \in R \Rightarrow (x,x') \in R$ and by transitivity we will have $\bar{x}_R = \bar{x}'_R$. The set of equivalence classes is the quotient set

$$S/\sim = S/R = \{\bar{x} \,|\, x \in S\}.$$

On the other hand a partition $\{S_i\}_{i \in I}$ of S defines the equivalence relation

$$x \sim x' \iff \exists i \,|\, x, x' \in S_i.$$

Definition 9. A **map or function** $f\colon X \longrightarrow Y$ is a relation R between sets X and Y satisfying:

(1) $(x,y) \in R$ and $(x,z) \in R \Rightarrow y = z$.

(2) $\forall x \in X \; \exists y \in Y \,|\, (x,y) \in R$.

A map is said to be **one-to-one or injective** if it satisfies the extra condition:

(3) $(x,y) \in R$ and $(x',y) \in R \Rightarrow x = x'$.

A map is said to be **onto or surjective** if it satisfies the extra condition:

(4) $\forall y \in Y \; \exists x \in X \,|\, (x,y) \in R$.

A map that is at the same time injective and surjective is called **bijective**.

Definition 10. If $g\colon X \longrightarrow Y$ and $f\colon Y \longrightarrow Z$ then the composition $f \circ g$ is the map $f \circ g\colon X \longrightarrow Z$ defined as $(f \circ g)(x) = f(g(x))$.

Remark 11. A map is bijective if and only it admits an inverse map $f\colon Y \longrightarrow X$ such that:

$$f \circ f^{-1} = 1_Y \quad f^{-1} \circ f = 1_X.$$

1.3 Operations on sets

Definition 12. A binary operation on a set S is a map $*\colon S \times S \longrightarrow S$.

1. The operation $*\colon S \times S \longrightarrow S$ is associative if $(a * b) * c = a * (b * c)$.
2. The operation $*\colon S \times S \longrightarrow S$ is commutative if $a * b = b * a$.

Example 13. Subtraction on the set $\mathbb{Z}$ or $\mathbb{R}$ is neither an associative nor a commutative operation. On the other hand, addition and multiplication, on $\mathbb{Z}$ or $\mathbb{R}$, are both: associative and commutative.

Example 14. The composition of maps is associative. If $h\colon X \longrightarrow Y$, $g\colon Y \longrightarrow Z$ and $f\colon X \longrightarrow T$, then

$$(f \circ g) \circ h = f \circ (g \circ h).$$

As special case, we can consider, for a set S, the set $A(S)$ of bijections $S \longrightarrow S$ and obtain:

(a) We have an identity map $1_S \in A(S)$ $(1_S(x) = x \ \forall x \in S)$, such that:

$$1_S \circ f = f \circ 1_S = f.$$

(b) For $f \in A(S)$ there exist $f^{-1} \in A(S)$ such that $f \circ f^{-1} = f^{-1} \circ f = 1_S$.

(c) For $f, g, h \in A(S)$, we have $(f \circ g) \circ h = f \circ (g \circ h)$.

Example 15. The composition of maps, on the other hand, is not necessarily commutative. Consider a finite set S of cardinality $|S| = 3$. If we denote $S = \{1, 2, 3\}$ and we compose the maps

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

the compositions will give $\sigma_1 \circ \sigma_2(3) = 1$ while $\sigma_2 \circ \sigma_1(3) = 2$. Hence $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$.

Remark 16. A subset $T \subset A(S)$ determines an equivalence relation on S determined by:

$$x \sim_T y \iff f(x) = y \quad \text{for some} \quad f \in T$$

if and only if the T satisfies conditions (a), (b) and (c).

Practice Questions:

1. Show that for subsets A, B and C, we have:
(a) $A \subset C$ and $B \subset C \Rightarrow A \cup B \subset C$.
(b) $C \subset A$ and $C \subset B \Rightarrow C \subset A \cap B$.

2. Show that a function $f\colon S \longrightarrow S$ is bijective if and only f admits an inverse function $g\colon S \longrightarrow S$ such that

$$f \circ g = g \circ f = \mathrm{id}_S.$$

3. Find examples of operations that are commutative but no associative.