Math 113
Abstract Algebra

Kelvin Lee

UC Berkeley

Contents

1 Sets and Relations **3**
1.1 Sets . . . 3
1.2 Set Operations . . . 3
1.3 Relations . . . 4
1.4 Modular Arithmetic . . . 5

2 Groups **6**
2.1 Properties of $+$ on $\mathbb{R}$ and $\times$ on $\mathbb{R}\backslash\{0\}$ . . . 6

Chapter 1

Sets and Relations

1.1 Sets

Definition 1.1.1 (Subset)**.** A set A is a **subset** of a set B if $x \in A \implies x \in B$. We write $A \subseteq B$ or $A \subset B$.

Definition 1.1.2 (Proper subset)**.** A **proper subset** is $A \subseteq B$ but $A \neq B$, i.e., $A \subset B$.

Remark. $A = B$ is equivalent to saying that $A \subseteq B$ and $B \subseteq A$.

1.2 Set Operations

Definition 1.2.1 (Union)**.** $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$

Definition 1.2.2 (Intersection)**.** $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

Definition 1.2.3 (Difference)**.** $A \backslash B = A - B = \{a \in A \mid a \notin B\}$.

Definition 1.2.4 (Cartesian product)**.** $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

Remark. $A \times B \neq B \times A$.

Definition 1.2.5 (Complement)**.** The **complement** of $A \subseteq U$ is $A^c = \{a \in U \mid a \notin A\}$ where U is the universe.

Remark. $A \cup A^c = U$; $A \cap A^c = \emptyset$; $(A^c)^c = A$.

Theorem 1.2.6 (De Morgan's Laws).

$$(A \cup B)^c = A^c \cap B^c,$$

$$(A \cap B)^c = A^c \cup B^c.$$

1.3 Relations

Definition 1.3.1 (Relations)**.** A **relation** between sets A and B is a subset $\mathcal{R} \subseteq A \times B$. If $(a, b) \in \mathcal{R}$, then a is related to b, or $a\mathcal{R}b$, or $a \sim b$.

Example 1.3.2. $\mathcal{R} \subseteq \mathbb{R} \times \mathbb{R}$. $\mathcal{R} = \{(x, x) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$, i.e., $a\mathcal{R}b \iff f(a) = b$, where $f : \mathbb{R} \to \mathbb{R}$ and $f(x) = x$.

Example 1.3.3. $\mathcal{R} \subseteq \mathbb{R}^2$, $a\mathcal{R}b \iff b = a^3$, i.e., $\mathcal{R} = \{(x, x^3) \mid x \in \mathbb{R}\}$.

1.3.1 Functions

Definition 1.3.4 (Function)**.** A **function** $f : A \to B$ is a relation $\mathcal{R} \subseteq A \times B$ such that $\forall a \in A, \exists! b \in B$ such that $(a, b) \in \mathcal{R}$.

Definition 1.3.5 (Binary Operation)**.** A **binary operation** on a set A is a function $A \times A \to A$.

Definition 1.3.6 (Disjoint)**.** $A, B \subseteq U$ are **disjoint** if $A \cap B = \emptyset$.

Definition 1.3.7 (Partition)**.** A **partition** of U is a collection of disjoint subsets of U whose union is U.

Example 1.3.8. $U = \mathbb{Z}$ can be partitioned into $\{x \in \mathbb{Z} \mid x < 0\}, \{x \in \mathbb{Z} \mid x > 0\}$.

Example 1.3.9. $U = \mathbb{R}$ can be partitioned by the sets $\{x\}$ for each $x \in \mathbb{R}$.

Definition 1.3.10 (Equivalence Relation)**.** A relation $\mathcal{R} \subseteq A \times A$ is an **equivalence relation** if it is

(i) **reflexive**: $a\mathcal{R}a \quad \forall a \in A$.

(ii) **symmetric**: $a\mathcal{R}b \iff b\mathcal{R}a$.

(iii) **transitive**: $a\mathcal{R}b$ and $b\mathcal{R}c \implies a\mathcal{R}c$.

Remark. Equivalence relation "are the same" as partition, i.e., they contain the same information. (Why)?

- If $\mathcal{R}$ is an equivalence relation on A, then create partition of A: say a and b are in the same subset of the partition $\iff a\mathcal{R}b$. This is a partition of A.
- Given a partition of A, make a relation $\mathcal{R}$ on A by saying $a\mathcal{R}b \iff a$ and b are in the same subset of the partition. Check $\mathcal{R}$ is an equivalence relation.

Example 1.3.11. If $\mathbb{Z}$ are partitioned into $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ for some $n2$, the corresponding equivalence relation is *congruence modulo* n. For $a\mathcal{R}b$, write $a \equiv b \pmod{n}$.

1.4 Modular Arithmetic

Notation.

$$\bar{i} = \{x \in \mathbb{Z} \mid i \text{ is the remainder when } x \text{ is divided by } n\} = \{an + i \mid a \in \mathbb{Z}\}.$$

Define $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Goal is to define $+$ and $\times$ on $\mathbb{Z}_n$.

To do so, first, given $x \in \mathbb{Z}$, let $\overline{x} = \{an + x \mid a \in \mathbb{Z}\}$. Then $\overline{x} = \overline{y}$ when $x - y = kn$ for some $k \in \mathbb{Z}$, i.e., $x - y \in \overline{0}$. Now for $+/\times$: define $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ that has the mapping $(\overline{a}, \overline{b}) \to \overline{a+b}$ and define $\times : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ that has the mapping $(\overline{a}, \overline{b}) \to \overline{ab}$.

Question. Define $\overline{a} + \overline{b} = \overline{a+b}$. But if $\overline{a} = \overline{x}$ and $\overline{b} = \overline{y}$, then is $\overline{a+b} = \overline{x+y}$?

Question. Write out tables of binary operations for $n = 3$.

Chapter 2

Groups

2.1 Properties of $+$ on $\mathbb{R}$ and $\times$ on $\mathbb{R}\backslash\{0\}$

(i) **Closure**: adding/ multiplying two elements gives another element (built in to definition of a binary operation).

(ii) **Commutativity**:

$$\begin{cases} a+b &= b+a \\ ab &= ba \end{cases} \quad \forall a, b.$$

(iii) **Associativity**

$$\begin{cases} a+(b+c) &= (a+b)+c \\ a(bc) &= (ab)c \end{cases} \quad \forall a, b, c.$$

(iv) **Identity**

$$\begin{cases} a+0 &= 0+a = a \\ a \cdot 1 &= 1 \cdot a = a \end{cases} \quad \forall a.$$

(v) **Inverses**

$$\begin{cases} a+(-a) &= 0 \\ a \cdot \frac{1}{a} &= 1 \end{cases} \quad \forall a.$$

Definition 2.1.1. We say a binary operation $p : A \times A \to A$ is:

- **commutative** if $p(a, b) = p(b, a) \quad \forall a, b \in A$.
- **associative** if $p(a, p(b, c)) = p(p(a, b), c) \quad \forall a, b, c \in A$.
- **has an identity** if $\exists e \in A$ such that $p(a, e) = p(e, a) = a \quad \forall a \in A$.
- **has inverses** if $\exists$ identity $e \in A$ and $\forall a \in A, \exists b \in A$ such that $p(a, b) = p(b, a) = e$. We denote the inverse as a^{-1}.

Example 2.1.2. $A = \mathbb{Z}_n, p =$ addition mod n, i.e., $p(i, j) = \bar{i} + \bar{j}$.

1. **Associativity:**

$$\begin{aligned}\bar{i} + (\bar{j} + \bar{k}) = \bar{i} + \overline{j+k} &= \overline{i + (j+k)} \\ &= \overline{(i+j)+k} \\ &= \overline{i+j} + \bar{k} \\ &= (\bar{i} + \bar{j}) + \bar{k}.\end{aligned}$$

2. **Identity:** $\bar{0}$.

3. **Inverses:** $\bar{i}$ has inverse $\overline{-i} = \overline{n-i}$. (e.g. $n = 2$: inverse of $\bar{1} = \overline{-1} = \overline{2-1} = \bar{1}$.

4. **Commutativity:**
$$\bar{i} + \bar{j} = \overline{i+j} = \overline{j+i} = \bar{j} + \bar{i}.$$

Example 2.1.3. $A = \mathrm{Mat}_n(\mathbb{R})$ = set of $n \times n$ matrices with entries in $\mathbb{R}$. $p : A \times A \to A$ is matrix multiplication. **Associativity:** matrix multiplication is associative. **Identity:** I_n the identity matrix. **Inverses:** No, consider the inverse for the zero matrix. **Commutativity:** $AB \neq BA$ for matrices.

Example 2.1.4. $A = GL_n(\mathbb{R})$ General linear group (invertible matrices). **Associativity:** yes. **Identity:** yes. **Inverses:** yes. **Commutativity:** no.

Example 2.1.5. A = set of functions $f : \mathbb{R} \to \mathbb{R}, p(f, g) = f \circ g$. **Associativity:** yes. **Identity**: $f(x) = x$. **Inverses**:? **Commutativity:** no, e.g.?

2.1.1 Properties

- If p is a binary operation on A with identity e, and $ab = ac = e$ and $ba = ca = e$. (ab means $p(a, b)$, ac means $p(a, c)$), then $b = c$. This is the **cancellation law**.

  Remark. (Why?) $ab = e \implies cab = ce \implies eb = c \implies b = c$. Hence, inverses are *unique*. That is, if $e, f \in A$ are such that

  $$\begin{cases} ea = ae & = a \\ fa = af & = a \end{cases} \quad \forall a \in A,$$

  then $e = f$.
  (Why?) $e = ef = f$ (f, e is identity).

- $(ab)^{-1} = b^{-1}a^{-1}$.

Definition 2.1.6 (Groups)**.** A **group** is a set G with a binary operation $p : G \times G \to G$ that is *associative*, *has an identity* e, and *has inverses*. Write this as (G, p) or just G if the binary operation is understood from context.

Definition 2.1.7 (Abelian)**.** A group (G, p) is **Abelian** or **communitative** if p is commutative.

Notation: write $p(a, b)$ as ab or $a + b$ sometimes depending on the context.

Remark. Some authors have four properties: with the extra one being **closure**. For us, closure is built in to the definition of p.

Example 2.1.8. Examples of Abelian group:$(\mathbb{R},+)$,$(\mathbb{R}\backslash\{0\},\times)$, $(\mathbb{Z}_n,+)$.
Examples of non-Abelian group: $(GL_n(\mathbb{R}),\times)$.
Examples of non-group: $(\text{Mat}_n(\mathbb{R}),\times)$, $(\{f:\mathbb{R}\to RR\},\text{commposition})$, $(\mathbb{N},+)$.

Definition 2.1.9 (Order)**.** The **order** of a group is the cardinality of G as a set.

Notation: $|G|=$ order of G. $|\mathbb{R}|=\infty, |\mathbb{Z}_n|=n$.

Theorem 2.1.10 (Cancellation Law)**.** *In a group G, if $ab=ac$, then $b=c$, i.e., we can cancel a.*

Proof. a has inverse $a^{-1}\in G$. Hence,

$$ab=ac \implies a^{-1}ab=a^{-1}ac \implies eb=ec \implies b=c.$$

□

Example 2.1.11.

- $GL_n(\mathbb{R}), GL_n(\mathbb{C}), GL_n(\mathbb{Q})$ under matrix multiplication. (*General linear groups*)
- $SL_n(\mathbb{R}), SL_n(\mathbb{C}), SL_n(\mathbb{Q})$ under matrix multiplication. (*Special linear groups*, i.e. $SL_n(\mathbb{R})=\{A\in GL_n(\mathbb{R})\mid \det A=1\}$.) Matrix multiplication can be reimagined as a binary operation $SL_n(\mathbb{R})\times SL_n(\mathbb{R})\to SL_n(\mathbb{R})$.
- Given a set $[n]=\{1,2,\dots,n\}$, let $S_n=$ set of bijections $[n]\to[n]$. For example, $f:[3]\to[3]$ $(f(1)=1, f(2)=3, f(2)=3)$ is an element of S_3. Define binary operation p on S_3 by function composition $fg=f\circ g$, e.g. $(fg)(1)=(f\circ g)(1)=f(g(1))$. This forms a group (S_n,p), called the **symmetric group**, e.g. for f above: $f\circ f$ is $(1\to1, 2\to2, 3\to3)$, which is the identity function.

  Remark. It is a group. **Associativity:** function composition is associative. **Identity:** $f(i)=i \quad \forall i$. **Inverse:** every bijection has an inverse bijection (if $f(i)=j$, then define $f^{-1}(j)=i$) and so $f\circ f^{-1}=f^{-1}\circ f=e$. Hence, S_n is a group.
  These bijection can be thought of as permutations of the list $\{1,2,\dots,n\}$, e.g. f above permutes 123 to 132. It also permutes 132 to 123. f takes the second slot to third slot and the third slot to second slot. f permutes: $123 \overset{f}{\rightsquigarrow} 132 \overset{f}{\rightsquigarrow} 123$. There are $n!$ different permutations of $123\cdots n$ and so $|S_n|=n!$.