Introduction to Abstract Algebra

Keep in Mind...

The Concept of Abstraction

- Notice properties common to many objects.
- Prove facts (**theorems**) using just these properties.
- These theorems then hold for **all** objects with the common ("abstracted") properties. Example: every finite dimensional vector space has a basis.

Abstract algebra is **axiomatic** — we start with some assumptions and derive theorems by logical reasoning (proofs).

Some Observations about Proofs

0. **Definitions** must be thoroughly **understood**.

Every definition is an "if and only if" statement, although it is common to write just "if".

1. If the **only** thing you know about an object or concept is its definition, then that definition **must** be used to prove any statement about that object or concept. **You have no other information!**

Example

Definition An integer n is odd if $n = 2m + 1$ for some integer m.

Theorem The product of two odd numbers is odd.

PROOF. Let n_1 and n_2 be two odd numbers. We want to show that n_1n_2 is odd. By **definition** $n_1 = 2m_1 + 1$ and $n_2 = 2m_2 + 1$ for some integers m_1 and m_2. Then

$$\begin{aligned} n_1n_2 &= (2m_1 + 1)(2m_2 + 1) \\ &= 4m_1m_2 + 2m_1 + 2m_2 + 1 \\ &= 2(2m_1m_2 + m_1 + m_2) + 1 \\ &= 2m + 1, \end{aligned}$$

where $m = 2m_1m_2 + m_1 + m_2$ is an integer. Thus n_1n_2 is an odd number.

2. The statement of a theorem has a **hypothesis** (or **hypotheses**) and a **conclusion**.

Example

Above (using a more formal version of the theorem statement: "If n_1 and n_2 are odd numbers, then n_1n_2 is odd"): **hypotheses:** n_1 and n_2 are odd. **Conclusion:** n_1n_2 is odd.

Every statement in a proof must be supported either by a **hypothesis** or by a **previously known fact** (which could be an axiom or a previous result).

3. A statement is **not** a theorem if even one **counterexample** can be found. This is the standard way to show that a statement is not a theorem.

Example

Statement: Every integer ending in a 6 is divisible by 3.
But 16 is a counterexample.
This statement is **not** a theorem.

Example

Statement: Some integers ending in a 6 are divisible by 3.
This statement **is** a theorem (write a proof!).

These two examples remind us about quantifiers:

4. Be very careful with **quantifiers**: for all, for every ($\forall$); for some, there exists ($\exists$). Also watch words like **only** or **unique**. Don't **assume** any hypotheses not stated. Be **precise** about the use of terms.

Example

Statement: "Every number has a square root"??

Which set of numbers are we referring to? The statement is a theorem if we mean within the set of complex numbers, but not if we mean within the set of real numbers. As written, the statement is imprecise.

5. A theorem of the form: *If* **hypotheses** *then* **conclusion** cannot be proved by giving an example. It must hold for **all** examples (exception: if there are only a finite number of instances in which the hypotheses hold, then a proof can consist of checking **every** one of these instances).

There are some standard techniques for proofs in algebra.

6. To show that there is a **unique** element with some property:
(a) show that there is such an element (by example), and
(b) show that if there are two such elements, then they must be equal.

Example

Theorem. For every nonzero real number r, there is a unique number s such that $rs = 1$.

PROOF. (You should provide justification for each step).

Existence: Let $s = \frac{1}{r}$. Then $rs = r\left(\frac{1}{r}\right) = 1$.

Uniqueness (without using cancellation): Suppose that s and t both have the required property, that is, $rs = 1$ and $rt = 1$. Then, multiplying the first of these equalities on the right by t, we have:

$$\begin{aligned} (rs)t &= t \\ \iff r(st) &= t \\ \iff r(ts) &= t \\ \iff (rt)s &= t \\ \iff 1s &= t \\ \iff s &= t \end{aligned}$$

Sets

Fact: We must start with some undefined concepts.

Generally, **set** is undefined. Let us agree:

1. A set S is made up of elements. We write $x \in S$ to mean that x is an element of S.
2. Exactly one set has no elements. It is the empty set, denoted $\emptyset$.
3. To describe a set S, either list the elements or give a description.

Examples

$S = \{0, 1, 4, 9\}$.
$S = \{x^2 | x$ is an integer, $x^2 < 10\}$.
S is the set of squares of integers, with the squares less than 10.

4. A set is **well-defined**, that is, for any set S, an object x is either in S or not in S.

Example

The sentence "S is some cats in St. Louis" does not define a set.
The sentence does not help us decide whether a particular St. Louis cat is in or not in the collection.

Definition. A set B is a subset of a set A if every element of B is in A.

Notation: $B \subseteq A$ or $A \supseteq B$ means that B is a subset of A. $B \subset A$ means that $B \subseteq A$, but $B \neq A$ (the notation $A \subsetneq B$ is non-ambiguous).

Remark: $\emptyset \subseteq A$ and $A \subseteq A$.

Definition. Let A be any set. A is the **improper subset** of A. All other subsets of A are **proper subsets**.

Standard Sets: $\mathbb{Z}$ = all integers, i.e., $\ldots -2, -1, 0, 1, 2, \ldots$.
$\mathbb{N} = \mathbb{Z}^+$ = all positive integers (natural numbers), i.e., $1, 2, 3, \ldots$.
$\mathbb{Q}$ = all rational numbers (those expressible as $\frac{m}{n}$, for $m, n \in \mathbb{Z}$, $n \neq 0$)
$\mathbb{Q}^+$ = all positive rational numbers.
$\mathbb{Q}^*$ = all nonzero rational numbers.
$\mathbb{R}$ = all real numbers.
$\mathbb{R}^+$ = all positive real numbers.
$\mathbb{R}^*$ = all nonzero real numbers.
$\mathbb{C}$ = all complex numbers.
$\mathbb{C}^*$ = all nonzero complex numbers.

Note that these symbols represent sets.

Be careful with set notation. $\mathbb{Z}$ is the set of all integers, while $\{\mathbb{Z}\}$ is a set whose single element is the set of all integers. Similarly, $\emptyset$ is the empty set, the set with no elements, but $\{\emptyset\}$ is a set whose single element is the empty set.

Example

Let $A = \{2, 3, 4\}$ and $B = \{4, 5\}$.
Then $C = \{A, B\}$ is a set with elements $\{2, 3, 4\}$ and $\{4, 5\}$.
On the other hand, $D = A \cup B = \{2, 3, 4, 5\}$ is a set with elements $2, 3, 4$ and 5.