MAT 3004 – Abstract Algebra I

Tutorial 1

Introduction What is **abstract algebra**?

Abstract algebra is the study of abstract algebraic structures. Well, the question now reduces to: what are **algebraic structures**?

Essentially, an algebraic structure consists of an nonempty set A with a collection of **operations** on A with finite **arity** (number of arguments of a function or operation)[1], and a finite set of identities[2], which are called **axioms**.

Example 1. A group $(G, \cdot)$ consists of a nonempty set G, three operations:

(O1) $\mu : G \times G \to G$, $(a, b) \mapsto ab$ (multiplication);
(O2) $e : \{\emptyset\} \to G$, $\emptyset \mapsto e$ (identity);
(O3) $i : G \to G$, $a \mapsto a^{-1}$ (inverse);

and three axioms:

(A1) $(ab)c = a(bc)$ (associativity);
(A2) $ae = ea = a$, $\forall\, a \in G$ (identity);
(A3) $aa^{-1} = a^{-1}a = e$, $\forall\, a \in G$ (inverse);

Hierarchy of structures A motivation of the study of abstract algebra is the tradeoff between generality and the richness of the theory: the more general a structure is, the less you can say about the structure; vice versa. The algebraic structures that we will encounter throughout this course will all be structured sets, hence all set theory results apply to groups, rings, fields; however, we cannot make group-theoretic claims to sets in their generality.

In terms of generality, algebraic structures form a hierarchy[3]. From a particular structure, we can delete some of the operations and axioms to create a more general structure; we can also add operations and axioms to create a more specified structure.

Magma, semigroups, monoids Starting with the formulation of a group in Example 1, we can define some more general structures:

- A **monoid** is the structure when we delete (O3) and (A3) from the group operations & axioms (no more inverses);
- A **semigroup** is the structure when we delete (O2) and (A2) from the *monoid* operations & axioms (no more identity);

[1] In daily usage, we seldom say an operation $*$ has arity k, instead we say $*$ is a k-ary operation. The convention is to use a Latin prefix with -ary ending.

[2] Note that in this context, identity basically means equality; not to be confused with the *identity element* of a group!

[3] The following example is somewhat misleading: the hierarchy is not always linear.

- A **magma** is the structure when we delete (A1) from the *semigroup* axiom (there was associativity, and it's gone!);

Exercise E1.1 (Integers):
In this exercise, we will re-learn preschool arithmetic, from an abstract algebra perspective! Under the binary operation $+$, the usual addition:

a) What algebraic structure does $\mathbb{Z}$, the set of integers, have?
b) What algebraic structure does $\mathbb{N}$, the set of natural numbers, have?
c) What algebraic structure does $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$, the set of positive integers, have?

Now let the binary operation be $\cdot$, the usual multiplication.

d) What are the respective structures of $\mathbb{Z}$, $\mathbb{N}_+$, and $\{\pm 1\}$?

Define the binary operation ^ by $a\hat{\ }b = a^b$.

e) Show that $\mathbb{Z}$ is a magma under the binary operation ^.
f) Does $\mathbb{Z} \setminus \{0\}$ together with $/$, the usual division, form any of the algebraic structures introduced above? Why or why not?

Closure The reason why the nonzero integers do not form any algebraic structure under division is quite obvious - the quotient of two integers may not even be an integer! However, believe it or not, many beginners are too overwhelmed by the operations and axioms of an algebraic structure, such that they often forget to verify closure.

Exercise E1.2 (Multiplication modulo a prime):
The purpose of the following exercise is to show: The set $[n-1] = \{1, 2, \cdots, n-1\}$ is a group under multiplication modulo n if and only if n is prime. We carry out the details step by step.

a) Show that if n is prime, then $([n-1], \times)$ is an abelian monoid with identity 1.
b) Show by Euclidean algorithm (Bézout's Theorem) that there is indeed an inverse for every element in $([n-1], \times)$, making it a group.
c) Show the contrapositive of the forward direction: if n is a composite, then the set $[n-1]$ does not form a group since it is **not closed**.

Groups, as actions The previous exercise shows that groups and related structures are like numbers, and binary operations are like arithmetic operations. However, we are now seeing from a different perspective. Instead of seeing the group elements as **objects**, we can see them as **actions**. In general, a group can be seen as the collection of actions on many things, say, sets (symmetric group, Cayley's theorem), groups (group action), vector spaces (representation theory). We now particularly focus on one case, where the group elements are symmetries of a geometric object. These groups are called symmetry groups[4]. Let's see a few examples.

Example 2. Here are a few familiar groups, regarded as symmetries on geometric objects.

a) $(\mathbb{Z}, +)$ is the symmetry group of an infinite comb. A group element k is the translation by k units.
b) $(\mathbb{Z}_n, +)$ is the symmetry group of a regular n-gon with arrows. A group element $[k]$ is the rotation by $k \cdot \frac{2\pi}{n}$ radians.

[4] Not to be confused with *symmetric* groups, which consists of all automorphisms of some set.

c) Can you give an example of a geometric object such that V, the Klein 4-group, is its symmetry group? (A rectangle, or an ellipse)
d) What is the symmetry group of a regular n-gon? What are the group elements other than rotations? (Dihedral groups; the reflections)

In this example, what does the binary operation do? Clearly, it does not make sense to calculate the sum or product of two actions. What we did is actually composition[5] - we first apply one action, then apply another. See if this interpretation makes sense in the previous examples!

Since compositionality can be captured by a binary operation, we might want to inspect the usual actions that we compose, and check whether these actions form a group.

Example 3.

a) Let S be a finite set with n elements. Then the bijections from S to itself forms a group under function composition. (Essentially, what is this group?)
b) Let V be a finite-dimensional vector space over $\mathbb{R}$. Then the invertible linear transformations from V to itself forms a group under composition. (Essentially, what is this group?)

Don't take commutativity for granted! In a group G where $ab = ba$ for all $a, b \in G$, we say that G is **abelian**, or that the binary operation is **commutative**. If we use the intuition that we gained from numbers, it is really easy to hold the false belief that all groups are abelian. Here we provide an example to illustrate that symmetries are not commutative:

Consider an equilateral triangle $\triangle$ and label the vertices. Obviously, a reflection wrt the vertical axis and a clockwise rotation by $2\pi/3$ are symmetries of the triangle. Try to apply reflection first, then rotation; also try to apply rotation first, then reflection. Will the labels of the resulting triangle be the same?

Exercise E1.3 (Abelian):
The following exercise is supposed to provide a better understanding of the abelian property.

a) (Left-right cancellation) Let G be a group such that for any $x, y, z \in G$ with $xy = zx$, $y = z$ iff G is abelian.
b) (Middle cancellation) Let G be a group such that for every $a, b, c, d, x \in G$ with $axb = cxd$, $ab = cd$ iff G is abelian. Can you think of an example of G and choices of a, b, c, d, x where $axb = cxd$ but $ab \neq cd$?
c) (Order 2) If G is a group with the property that the square of every element is the identity, then G is abelian.

Hint. To prove G is abelian, all we need to do is to prove $ab = ba$ for all $a, b \in G$.
For a), let $x = a^{-1}$, $y = ab$, $z = ba$.
For b), let $c = b$, $d = a$, $x = a^{-1}$.
For c), multiply a on the left and b on the right of $(ab)^2 = e$.

To construct an counterexample such that $axb = cxd$ but $ab \neq cd$, we must start with an non-abelian group: we try the symmetry group of an equilateral triangle, as we have shown that it is non-abelian. Also, we want to make sure that at least one of b or d does not commute with x, otherwise $abx = axb = cxd = cdx$, and applying right cancellation yields $ab = cd$. The rest of the construction is left as exercise.

[5] By convention, our compositions are right-associative: we apply the right-most action first.