Mathematics Department Stanford University
Math 61CM/DM – Basic algebraic structures

The purpose of this handout is to provide some basic definitions and a brief discussion of some key ideas and objects in algebra. One main new idea you will be studying in class is the notion of a *field*. This is a concept which generalizes the algebraic properties of the real numbers (as well as the rational numbers and the complex numbers). However, mathematicians find it useful to abstract the properties of these familiar fields into a general definition. It turns out that there are a lot of other interesting examples; we present a few of these below. One of the points of this is that a substantial portion of linear algebra can be done in the setting of general fields, rather than how it is more customarily done, over the real numbers. This will be especially pertinent to the students in 61DM. For the 61CM students, you should view this as a good way to get accustomed to a slightly different level of abstraction, and you should also use this as an opportunity to get used to the fact that the basic results and methods in linear algebra are really "algebraic", i.e., only depend on the handful of axioms in the definition of a field.

In mathematics, the most fundamental objects are *sets*. These are just collections of objects. We will be concerned with either finite or certain infinite sets. (It turns out that there is quite a lot that can be said about sets in general, but that's another story.) However, sets are kind of static objects – they just sit there. One can define progressively more sophisticated objects by prescribing certain sets of rules, or axioms, about how the elements of the sets are related to or interact with one another. We are going to describe a few different types of rules, each slightly more specific than the last, leading to different types of algebraic objects: semigroups, groups and then fields. This handout collects these definitions, discusses a few examples and basic results.

Definition 1 *A semigroup with unit $(G, *, e)$ is a set of objects G containing a distinguished element $e \in G$, along with a map $* : G \times G \to G$, with the following properties:*

1. *(Associativity) For all $x, y, z \in G$, $x * (y * z) = (x * y) * z$.*
2. *(Units) There exists an element $e \in G$ such that for all $x \in G$, $x * e = x = e * x$.*

You should think of the operation $*$ as being 'multiplication'; it is a way of combining elements of the set G to get other elements. Here is a basic example: let $G = \{1, 2, 3, \ldots\}$, and $*$ ordinary multiplication. The 'identity element' e is simply 1. It is obvious that the two rules hold. Here is another example: now let $G = \{0, 1, 2, \ldots\}$, but this time, suppose that $*$ is the symbol which corresponds to addition. Now $e = 0$ and once again the two rules hold.

This is one of the most primitive algebraic structures: we have a set and a way of combining elements in it. We only have one "extra", which is the existence of a unit e. (One can also talk about semigroups without units; there are even some interesting examples!)

Lemma 1 *In any semigroup with $(G, *, e)$, the unit e is unique.*

Proof: Suppose $e, f \in G$ are two possibly different elements which both satisfy the properties of a unit. Then $e = e * f$ since f is a unit, and $e * f = f$ since e is a unit. Combining these, we see that $e = f$. □ This means that one can talk about *the* unit, i.e. given (1) and (2), e is unique.

It is a bit more interesting if one adds one further property:

Definition 2 *A group $(G, *)$ is a semigroup with unit $(G, *, e)$ with one additional property:*

1. *(Inverses) For every $x \in G$, there exists an element $y \in G$ such that $x * y = e = y * x$.*

Similarly to the lemma above, inverses are also unique.

Lemma 2 *Suppose that $(G, *)$ is a group. If $x \in G$ there exist elements $y, z \in G$ such that $y * x = e = x * z$. Then $y = z$.*

Try to prove this yourself!

It is usually simpler to just say that G is a group, without explicitly mentioning $*$ and e.

Groups turn out to be really fundamental and extraordinarily important objects in mathematics; they are the basic way to describe *symmetry*. Groups are widely used in physics, chemistry and elsewhere.

Here are a few interesting groups:

1. $(\mathbb{R}, +)$, the set of all real numbers with addition;
2. $(\mathbb{Z}, +)$, the set of all integers with addition;
3. $(\mathbb{Q}, +)$, the set of all rational numbers with addition;
4. $(\mathbb{Q}[\sqrt{2}], +)$, the set of all numbers of the form $a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$;
5. $(\mathbb{R}^n, +)$, the set of all vectors with n components under addition;
6. $(\mathbb{R}^+, \cdot)$, the set of all positive real numbers with multiplication;
7. $(\mathbb{Z}/(n\mathbb{Z}), +)$, the set of integers *modulo* n, where n is an integer greater than 2, under addition;
8. The group of all rotations around the origin in $\mathbb{R}^2$;
9. The group of all rotations around the origin in $\mathbb{R}^3$.

For 7) here, we recall that as a set, $\mathbb{Z}/(n\mathbb{Z})$ is identified with $\{0, 1, \ldots, n-1\}$ (remainders when dividing by n), and $+$ means ordinary addition in $\mathbb{Z}$, reduced modulo n, so e.g. in $(\mathbb{Z}/(5\mathbb{Z}), +)$, $2 + 4 = 1$. It is maybe less confusing to write this set as $\{[0], \ldots, [n-1]\}$ so we don't think of its elements as ordinary integers. Then $[2] + [4] = [1]$, etc.

All but the last of these examples of groups have an important extra property:

Definition 3 *A commutative, or abelian, group G is one in which $x * y = y * x$ for all $x, y \in G$.*

Noncommutative groups (and semigroups) do play a role, even in this class. The group of rotations in $\mathbb{R}^3$ is a really important example; another example of a noncommutative semigroup is the set M_n of $n \times n$ matrices, where $*$ denotes matrix multiplication. This is noncommutative when $n \geq 2$. Another example we shall see again is the set of all permutations of a finite set S. Permutations form a group: if we permute S then permute again, then the composition of the two permutations is another permutation. The order in which we compose is important, and we would get a different answer if S has at least three elements.

Finally we come to the definition of a field:

Definition 4 *A field $(F, +, \cdot)$ is a set F with two distinct maps $+ : F \times F \to F$ and $\cdot : F \times F \to F$, which satisfy*

1. *$(F, +)$ is a commutative group, with unit 0.*
2. *$(F, \cdot)$ is a commutative semigroup with unit 1.*
3. *$1 \neq 0$ and if $x \in F$ and $x \neq 0$, then x has a multiplicative inverse (i.e., an element y such that $x \cdot y = 1 = y \cdot x$).*
4. *The distributive law holds:*
$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

One usually writes $-x$ for the additive inverse (inverse with respect to $+$), and x^{-1} or $1/x$ for the multiplicative inverse.

Examples then include $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, as well as complex numbers $(\mathbb{C}, +, \cdot)$. It turns out that $(\mathbb{Z}/(n\mathbb{Z}), +, \cdot)$ is a field if and only if n is a prime number! Furthermore,

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$$

is also a field! It is obvious that this set is closed under addition, and with just one line of computation, you can see that it is also closed under multiplication. Furthermore, it obviously contains all additive inverses. To see that it contains all multiplicative inverses, suppose that $a + b\sqrt{2} \neq 0$, and observe that computing in $\mathbb{R}$,

$$(a + b\sqrt{2})^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = (a^2 - 2b^2)^{-1}a - (a^2 - 2b^2)^{-1}b\sqrt{2}.$$

The point here is that $(a^2 - 2b^2)^{-1}a$ and $-(a^2 - 2b^2)^{-1}b$ are both rational, and $a^2 - 2b^2 \neq 0$.

Here is an example of a general result about fields:

Lemma 3 *If $(F, +, \cdot)$ is a field, then $0 \cdot x = 0$ for all $x \in F$.*

Proof: Since $0 = 0 + 0$, we have

$$0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x,$$

so

$$0 = -(0 \cdot x) + (0 \cdot x) = -(0 \cdot x) + (0 \cdot x + 0 \cdot x) = (-(0 \cdot x) + 0 \cdot x) + 0 \cdot x = 0 + 0 \cdot x = 0 \cdot x,$$

as desired. On the last line, the first equation is that $-(0 \cdot x)$ is the additive inverse of $0 \cdot x$, the second substitutes in the previous line, the third is associativity, the fourth is again that $-(0 \cdot x)$ is the additive inverse of $0 \cdot x$, while the fifth is that 0 is the additive unit. $\square$

Notice that this proof uses the distributive law crucially: this is what links addition (0 is the additive unit!) to multiplication.

For more examples, see Appendix A, Problem 1.1.