Mathematics Department Stanford University
Math 51H – Basic algebra

We start with the definition of a group, since it involves only one operation.

Definition 1 *A group $(G, *)$ is a set G together with a map $* : G \times G \to G$ with the properties*

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

Note that the most conventional notation for a map, such as $*$, is $*(x, y)$; we write however, as usual in this case, $x * y$.

A basic property is that one can talk about *the* unit, i.e. given (1) and (2), e is unique:

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

Proof: Suppose $e, f \in G$ are units. Then $e = e * f$ since f is a unit, and $e * f = f$ since e is a unit. Combining these, $e = f$. $\square$

Note that this proof used only (1) and (2), so it is useful to define a more general notion than that of a group.

Definition 2 *A semigroup $(G, *)$ is a set G together with a map $* : G \times G \to G$ with the properties*

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

Thus, a semigroup would be a group if each element had an inverse. Notice also that the proof of the above lemma shows that even in a semigroup, the unit is unique.

We also have that inverses are unique in a group. More generally:

Lemma 2 *Suppose that $(G, *)$ is a semigroup with unit e, $x \in G$, and suppose that there exist $y, z \in G$ such that $y * x = e = x * z$. The $y = z$.*

Notice that if G is a group, the existence of such a y, z is guaranteed, even with $y = z$, by (3). Thus, this lemma says in particular that in a group, inverses are unique.

However, it says more: in a semigroup, any left inverse (if exists) equals any right inverse (if exists). In particular, *if* both left and right inverses exist, they are both unique: e.g. if y, y' are left inverses, they are both equal to any left inverse z, and thus to each other.

Proof: We have $y = y * e = y * (x * z)$ where we used that e is the unit and $x * z = e$. Similarly, $z = e * z = (y * x) * z$. But by the associativity, $y * (x * z) = (y * x) * z$, so combining these three equations shows that $z = y$, as desired. $\square$

There are many interesting groups, such as $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}^n, +)$, $(\mathbb{R}^+, \cdot)$, where $\mathbb{R}^+$ consists of the positive reals, as well as semigroups, such as $(\mathbb{R}, \cdot)$ (all non-zero elements have inverses), $(\mathbb{Z}, \cdot)$ (only ± 1 have inverses). Another group with a different flavor is $(\mathbb{Z}/(n\mathbb{Z}), +)$, the integers modulo $n \geq 2$ integer: as a set, this can be identified with $\{0, 1, \ldots, n-1\}$ (the remainders when dividing by n), and addition gives the usual sum in $\mathbb{Z}$, reduced modulo n, so e.g. in $(\mathbb{Z}/(5\mathbb{Z}), +)$, $2 + 4 = 1$. It is less confusing though to write $\{[0], \ldots, [n-1]\}$ for the set, and $[2] + [4] = [1]$ then.

In general, when the operation is understood, one might just write the set for a group or semigroup, i.e. say G is a group.

Many (semi)groups are commutative; in fact, all of the above examples are:

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

Noncommutative semigroups will play a role in this class, including the set M_n of $n \times n$ matrices with matrix multiplication as the operation, which is non-commutative if $n \geq 2$, and permutations of a finite set S which is non-commutative if the set has at least 3 elements (this will be discussed when we talk about determinants).

We then can make the following definition:

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

1. *$(F, +)$ is a commutative group, with unit 0.*
2. *$(F, \cdot)$ is a commutative semigroup with unit 1 such that $1 \neq 0$ and such that $x \neq 0$ implies that x has a multiplicative inverse (i.e. y such that $x \cdot y = 1 = y \cdot x$).*
3. *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 $+$), x^{-1} for the multiplicative inverse.

Examples then include $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, and indeed complex numbers $(\mathbb{C}, +, \cdot)$.

A more interesting field is the subset of $\mathbb{R}$ given by numbers of the form
$$\{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}.$$
The most interesting part in showing that this is a field is that multiplicative inverses exist; that these exist (within this set!) when $a + b\sqrt{2} \neq 0$ follows from the following computation in $\mathbb{R}$:
$$(a + b\sqrt{2})^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = (a^2 - 2b^2)^{-1}a - (a^2 - 2b^2)^{-1}b\sqrt{2}.$$
Notice that $(a^2 - 2b^2)^{-1}a, -(a^2 - 2b^2)^{-1}b$ are indeed rational, and $a^2 - 2b^2 \neq 0$ as follows from Homework 1, problem 4.

Finally, $(\mathbb{Z}/(n\mathbb{Z}), +, \cdot)$ is not a field in general; e.g. if $n = 6$, $[2] \cdot [3] = [0]$. However, if n is a prime p, then it is — it is the finite field of $p = n$ elements.

As an example of a general result in a field:

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. Note that (ii) is the statement that if $x, y \neq 0$ then $x \cdot y \neq 0$, which in particular shows easily that $(\mathbb{Z}/(n\mathbb{Z}), +, \cdot)$ is not a field if $n \geq 2$ is not a prime. (There is a bit more work in showing that if $n = p$ is a prime, this is a field.)