# Algebra

Tyler Chang
April 22, 2018

## Groups, Rings, and Fields

A *group* $G$ is a nonempty set paired with a single binary operation: $* : G \times G \to G$ that satisfies:

- Associativity: For $a, b, c \in G$, $a * (b * c) = (a * b) * c$
- Identity: There exists $e \in G$ such that $a * e = a$ for all $a \in G$.
- Inverse: For all $a \in G$, there exists an $a^{-1} \in G$ such that $a * a^{-1} = e$.

If $*$ is also commutative, then $G$ is an *abelian* group.

A *ring* $R$ is a nonempty set paired with two binary operations: $+$ and $\times$ (both mapping from $R \times R$ to $R$) that satisfy:

- Additive Associativity: For $a, b, c \in R$, $a + (b + c) = (a + b) + c$
- Zero: There exists $0_R \in R$ such that $a + 0_R = a$ for all $a \in R$.
- Inverse: For all $a \in R$, there exists an $-a \in R$ such that $a + -a = 0_R$.
- Commutativity: For all $a, b \in R$, $a + b = b + a$
- Multiplicative Associativity: For $a, b, c \in R$, $a \times (b \times c) = (a \times b) \times c$
- Distributive: For $a, b, c \in R$, $a \times (b + c) = a \times b + a \times c$.

If multiplication is also commutative, then $R$ is a *commutative ring.* The natural numbers $\mathbb{N}$ with the standard multiplication and addition operations are a common example of a commutative ring. A set $S$ is a subring of $R$ if it is a subset of $R$ and remains a ring with respect to the two operations it inherits from $R$. $\mathbb{N}$ is a subring of the rationals $\mathbb{Q}$ with respect to the standard definition of multiplication and addition.

A *field* $F$ is a commutative ring that also has a multiplicative identity (denoted $1_F$) and each element other than $0_F$ has a multiplicative inverse ($a \times a^{-1} = 1$). The rationals $\mathbb{Q}$ and the reals $\mathbb{R}$ are both fields with the standard multiplication and addition operations. More abstractly, the set of all polynomials of arbitrary degree $\mathbb{P}$ is also a field with addition and multiplication defined in the usual way.

A subset of any of the above that is closed under all operations is called a subring/group/field. If that subset absorbs multiplication (for example, consider the even integers) then it is called an *ideal.*

If two groups, rings, or fields share the same algebraic structure with the only difference being the names of their elements, then they are essentially the same and algebraically indistinguishable. For example, consider the fields $S_1 = \{1, 2, 3\}$ and $S_2 = \{a, b, c\}$ with the addition/multiplication structures below:

$S_1$:

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

and

| × | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

;

$S_2$:

| + | a | b | c |
|---|---|---|---|
| a | a | b | c |
| b | b | c | a |
| c | c | a | b |

and

| × | a | b | c |
|---|---|---|---|
| a | a | a | a |
| b | a | b | c |
| c | a | c | b |

We capture this notion of sameness by saying $S_1$ and $S_2$ are *isomorphic*. Clearly, if a bijection $f : S_1 \to S_2$ exists that preserves the algebraic structure (i.e., $f(s + t) = f(s) + f(t)$ and $f(s \times t) = f(s) \times f(t)$ for all $s, t \in S_1$), then $S_1$ and $S_2$ are isomorphic and we call $f$ an *isomporphism*. A more general function that preserves group/ring/field structure but is **not** bijective, is called a *homomorphism*.

## Vector Spaces

A vector space $V$ over a field $F$ is a set of vectors $v \in V$ with an addition operation defined $+ : V \times V \to V$ and a scalar multiplication operation $\circ : F \times V \to V$. (Note, that multiplication is typically denoted $\alpha v$ where $\alpha \in F$, $v \in V$.) To qualify as a vector space, $V$ must satisfy:

- Associativity: For all $u, v, w \in V$, $u + (v + w) = (u + v) + w$
- Commutativity: For all $u, v \in V$, $u + v = v + u$
- Zero: There exists $0 \in V$ such that $u + 0 = u$
- Inverse: For all $v \in V$, there exists an inverse $-v \in V$ such that $v + -v = 0$
- Compatibility: For $\alpha, \beta \in F$ and $v \in V$, $\alpha(\beta v) = (\alpha\beta)v$.
- Distributivity: For $\alpha, \beta \in F$, and $u, v \in V$, $\alpha(u+v) = \alpha u+\alpha v$ and $(\alpha+\beta)v = \alpha v+\beta v$.

There are generalizations of the above called *modules* that can be defined over rings instead of just fields. However, in this document only proper vector spaces are considered.

Every element of a vector space $V$ can be expressed as a linear combination of some linearly independent subset of its elements, called *basis elements*. That is, there exist basis elements $e_1$, $e_2$, $\ldots$, $e_n$ such that for all $v \in V$, $v = \sum_{i=1}^{n} \alpha_i e_i$ where $\alpha_i \in F$. If $n < \infty$, then $V$ is an $n$-dimensional vector space. If $n = \infty$, then $V$ is an infinite-dimensional vector space. Once we have agreed on a basis, it makes sense to drop the basis elements themselves, and implicitly express each vector $v$ in terms of the coefficients of each of its basis elements. That is,

$$v = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$$

where each coefficient $\alpha_i$ can be interpreted as the magnitude of $v$ in the direction of $e_i$.

For any vector space $V$, its *dual space* $V^*$ is the set of all linear maps from $V \to F$. That is, for all $v^* \in V^*$, $v^* : V \to F$. To qualify as a linear map, $v^*$ must satisfy $v^*(v+u) = v^*(v)+v^*(u)$ and $v^*(\alpha v) = \alpha(v^* v)$. If follows that $V^*$ must satisfy all the vector axioms itself, and so $V^*$ is itself a vector space. It often makes sense to define a basis for $V^*$ in terms of the basis of $V$, so we choose the basis elements of $V^*$ specifically such that for each basis element $e^i \in V^*$ and basis element $e_j \in V$, $e^i e_j = 0_F$ if $i \neq j$ and $e^i e_j = 1_F$ if $i = j$. Note that by definition, the dual-dual: $(V^*)^* \supseteq V$. Generally, it is convenient if $(V^*)^* = V$. Then we say that $V$ is *reflexive*. For example, if $V = \mathbb{R}^n$, then $V^* = \mathbb{R}^{1\times n}$. Since furthermore $(V^*)^* = \mathbb{R}^n = V$, $\mathbb{R}^n$ is reflexive.

Now we define linear maps from arbitrary cartesian products of vector spaces $V \times U$ to $F$, where $U$ and $V$ are both vector spaces over $F$. In general, if we take the dual space of $V$, $V^*$ with basis $a^1, \ldots, a^n$ and the dual space of $U$, $U^*$ with basis $b^1, \ldots, b^m$, we define the set of all linear maps from $V \times U$ to $F$ to be the *tensor product* of $V^*$ and $U^*$ (denoted $V^* \otimes U^*$). Note, tensor products are themselves vector spaces, and the standard basis for a tensor product space is given by the set $\{a^i b^j\}$. That is, for $M \in V^* \otimes U^*$, $M = \sum_{i=1}^{n} \sum_{j=1}^{m} A^{ij} a^i b^i$, where each $A^{ij}$ can be interpreted as the total action $M$ takes on the basis element $a_i$ of $V$ together with the basis element $b_j$ of $U$. In general, the linear maps in the tensor product of $n$ dual spaces are called *$n$-tensors*. For example, the space of all 2-tensors on $\mathbb{R}^n \times \mathbb{R}^{1\times n}$ is given by $\mathbb{R}^{1\times n} \otimes \mathbb{R}^n$, i.e., the space of $n \times n$ matrices.

## Norm Spaces and Inner Product Spaces

Given a vector space $V$ on a field $F$ where $F = \mathbb{R}$ or $\mathbb{C}$, a *norm* is a function $\|.\| : V \to F$ that measures the magnitude of each $v \in V$. In order to qualify as a norm, $\|.\|$ must satisfy the norm axioms:

- Positivity and Zero Vector: $\|v\| \geq 0_F$ for all $v \in V$, and $\|v\| = 0_F$ if and only if $v = 0_F$ (or if the elements of $V$ are functions, we relax this to $v = 0_F$ almost everywhere).
- Homogeneity: For all $\alpha \in F$ and $v \in V$, $\|\alpha v\| = |\alpha|\|v\|$.
- Triangle Inequality: For all $u, v \in V$, $\|u + v\| \leq \|u\| + \|v\|$.

A vector space $V$ together with a norm $\|.\|$ is called a *norm space*. Every norm space also admits a metric space $(V, d)$ where $d(u, v) = \|u - v\|$. If a norm space is *complete* under the metric topology, then it is called a *Banach space*.

An *inner product space* is a vector space together with a symmetric positive-definite 2-tensor $\langle\ .\ ,\ .\ \rangle : V \times V \to F$. Every inner product space admits a norm space with the norm $\|x\| = \sqrt{\langle x, x\rangle}$ that satisfies the Cauchy-Schwarz inequality: $\langle v, u\rangle \leq \|v\|\|u\|$ with equality when $u = v$. Using the inner product, we define the projection of $u$ onto $v$ (or equivalently, the projection of $v$ onto $u$) in a norm space by $proj_V(u, v) = \langle u, v\rangle$. If an inner product space is complete under the metric topology, then it is called a *Hilbert space*.

We say that two vectors $v$ and $u$ in an inner product space $(V, \langle ., .\rangle)$ are *orthogonal* if $\langle v, u\rangle = 0_F$, and we say $v$ is *normalized* if $\|v\| = 1_F$. In general, a favourable property of a basis $E = \{e_i\}_{i=1}^{n}$ for $V$ is that $E$ be an *orthonormal basis*. That is, $\langle e_i, e_j\rangle = 0_F$ if $i \neq j$ and $\langle e_i, e_j\rangle = 1_F$ if $i = j$ for all $1 \leq i, j \leq n$.

## Fundamental Theorem of Algebra

The Fundamental Theorem of Algebra (FTA) states that every degree $n$ polynomial with complex or real coefficients of the form: $P_n(x) = a_n x^n + \ldots + a_1 x + a_0$ has exactly $n$ roots in the complex plane (with multiplicity).