Mathematics Notes

Algebra (tags: abstract algebra, complex numbers)

Abstract Algebra (tags: abstract algebra)

Groups (tags: abstract algebra)

Definition. *A binary operation is a function,*

$$f : G \times G \longmapsto G$$

which - by the definition of a function - maps a unique tuple from $G \times G$ to a unique value in the codomain G.

Definition. *Let G be a set and $*$ a binary operation on G and denote this $(G, *)$. Then $(G, *)$ is a* ***group*** *if:*

closure $\forall x, y \in G, x * y \in G$;

associativity $\forall x, y, z \in G, (x * y) * z = x * (y * z)$;

identity $\exists e \in G$ *s.t.* $\forall x \in G, e * x = x * e = x$;

inverse $\forall x \in G, \exists x^{-1} \in G$ *s.t.* $x * x^{-1} = x^{-1} * x = e$.

These are known as the ***group axioms****.*

Definition. *The group is an **Abelian group** if it has the additional property:*

commutativity $\forall x, y \in G, x * y = y * x \in G.$

Notation. from here on we will use juxtaposition notation for the group operation (so $xy = x * y$) and (usually) 1 for the identity element instead of e. This is known as *multiplicative notation.*

Corollaries of the group axioms

The group operation is defined to map a unique tuple in $G \times G$ to a unique value in G so that if we have $x, y \in G$ then $f((x, y)) = f(x, y) = xy \in G$ and for $a, b, c \in G$,

$$a = b \iff (c, a) = (c, b) \implies f((c, a)) = f((c, b)) \iff ca = cb$$

$$\therefore a = b \implies ca = cb$$

Then, using all the group axioms - associativity, inverse and identity,

$$ca = cb \implies c^{-1}(ca) = c^{-1}(cb) \iff (c^{-1}c)a = (c^{-1}c)b \iff 1a = 1b \iff a = b$$

Therefore we have the principle of cancellation,

$$ca = cb \implies a = b$$

Note that, since we have used the axioms of inverse and identity and the definitions of these require these elements to exhibit these properties from both the left and the right, the principle of cancellation can also be shown from both the left and the right. So, also,

$$ac = bc \implies a = b$$

There are (at least) two approaches to finding the other consequences of the group axioms.

First approach. We begin by noticing that the law of cancellation implies that,

unique identity and inverses $\forall a, x, b \in G, ax = b$ has a unique solution because,

$$ax = ax' \iff x = x'$$

That unique solution is $a^{-1}b$. If $b = a$ we have $ax = a$ and x, by identity axiom, is an identity element. Since, the solution to this equation - x - is unique, it follows that there is a unique value that is the identity element. Then, if we let b be this unique identity element we have $ax = 1$ and the unique solution, x, is the inverse of a, i.e. a^{-1}. Therefore, the inverses of group elements are also unique.

Second approach. This approach begins by showing the uniqueness of the identity element solely using the defintion of the identity. Here, for clarity, we revert to using e to denote the identity element.

unique identity Assume there are two identity elements, e, e'. Then, by the definition of the identity $ee' = e'e = e = e'$ so that there is a single value that has the property of the identity element.

Then, using the definition of the inverse we have,

unique inverses Assume there are two distinct inverses of an element a: a^{-1} and a'. Then,

$$\begin{aligned} & aa^{-1} = 1 = aa' && \text{defn. of inverse, uniqueness of identity} \\ \iff & a^{-1} = a' && \text{law of cancellation} \end{aligned}$$

Some Examples of Groups

- $(\mathbb{R} \setminus \{0\}, \times)$ is a group whereas $(\mathbb{R}, \times)$ is not a group because 0 has no multiplicative inverse.

- $(\mathbb{R}, +)$ is a group.
- The set of $n \times n$ invertible matrices is called the General Linear group and denoted GL_n

Permutations and Symmetric Groups

Definition. *A **permutation** is a bijection from a set to itself. Since permutations are bijective, they are invertible and since they are functions, function composition defines an associative law of composition over them. As a result, they form a group.*

Definition. *The **symmetric group** defined over a set is the group whose elements are the permutations of the objects of the set and whose law of composition is the composition of functions. The name probably comes from the study of symmetries of geometric objects that were eventually realised to be equivalent to permutations of the vertices.*

Notation. The symmetric group over the integers from 1 to n is denoted S_n.

S_2 The symmetric group S_2 consists of the two elements i and τ which are, respectively, the identity map and the transposition which interchanges 1 and 2. The group composition law is described by the fact that the identity map is the identity of the composition and by the relation $\tau\tau = \tau^2 = i$. Which results in the multiplication table:

$$\begin{aligned} i \cdot i &= i \\ i \cdot \tau &= \tau \\ \tau \cdot i &= \tau \\ \tau \cdot \tau &= i \end{aligned}$$

Note that the law of composition is commutative.

S_3 The symmetric group S_3 contains 3! elements. It is the smallest group whose law of composition is not commutative. It can be described using any two permutations of $\{1, 2, 3\}$. For example, if we take,

$$x = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \; y = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Then the permutations are,

$$\{1, x, x^2, y, xy, x^2y\} = \{\, x^i y^j \;\mid\; 0 \leq i \leq 2, \; 0 \leq j \leq 1 \,\}$$

These are the elements of the group. The composition law over these elements is the function composition of these permutation functions and its multiplication table is characterized by the rules:

$$x^3 = 1, \; y^2 = 1, \; yx = x^2 y$$

These are derived directly from the permutations themselves. Note that this composition law is not associative as $yx \neq xy$.
Any product of the elements x, y and of their inverses can be brought into the form $x^i y^j$ with i, j taking the ranges given above by repeated application of the above rules. To do so, we move all occurrences of y to the right side using the last relation and bring the exponents into the indicated ranges using the first two relations:

$$\begin{aligned} x^{-1}y^3x^2y &= x^2yx^2y = x^2(yx)xy = x^2(x^2y)xy = x^4(yx)y \\ &= x^4(x^2y)y = x^6y^2 = (x^3)^2y^2 = 1 \cdot 1 = 1 \end{aligned}$$

Rules like these that determine a complete multiplication table are called *defining relations* for the group.

Subgroups (tags: abstract algebra)

Definition. *A subset H of a group G is called a* ***subgroup*** *if it has the following properties:*

- ***Closure:*** *If $a \in H$ and $b \in H$ then $ab \in H$.*
- ***Identity:*** $1 \in H$.
- ***Inverses:*** *If $a \in H$ then $a^{-1} \in H$.*

These conditions show that the subset H is a group with respect to the induced law of composition created by applying the law of composition of G on the members of H. Note that the associative property is not mentioned because the associativity of the composition of members of G automatically carries over to H.

Notation. If H and G are groups then we may write $H \leq G$ to indicate that H is a subgroup of G.

Note that an alternative, more compact, formulation of the definition of a subgroup is as follows.

Let G be a group and $\emptyset \neq H \subseteq G$. Then H is a subgroup if

$$\boldsymbol{x, y \in H \implies x^{-1}y \in H}.$$

This is because,

$$[(x, y \in H \implies xy \in H) \wedge (x \in H \implies x^{-1} \in H)] \iff (x, y \in H \implies x^{-1}y \in H).$$

The implication,

$$[(x, y \in H \implies xy \in H) \wedge (x \in H \implies x^{-1} \in H)] \implies (x, y \in H \implies x^{-1}y \in H)$$

is obvious. In the other direction,

$$(x, y \in H \implies x^{-1}y \in H) \implies [(x, y \in H \implies xy \in H) \wedge (x \in H \implies x^{-1} \in H)]$$

is because, if we set $x = y$,

$$x^{-1}x = e \in H \implies x^{-1}e = x^{-1} \in H$$

and then, for $x \neq y$,

$$x^{-1}, y \in H \implies xy \in H.$$

Every group, at a minimum, has two trivial subgroups: the maximal subgroup - the group itself; and the minimal subgroup - the set containing just the identity. A subgroup that is neither of these is known as a *proper subgroup*.

Important examples are the subgroups of the additive group of integers $\mathbb{Z}^+$. Denote the subset of $\mathbb{Z}^+$ consisting of all multiples of a given integer b by $b\mathbb{Z}$ such that,

$$b\mathbb{Z} = \{\, n \in \mathbb{Z} \mid n = bk,\ k \in \mathbb{Z} \,\}$$

Proposition 1. *For any integer b, the subset $b\mathbb{Z}$ is a subgroup of $\mathbb{Z}^+$ and every subgroup of $\mathbb{Z}^+$ is of the form $b\mathbb{Z}$ for some integer b.*

Proof. $b\mathbb{Z}$ is a subgroup of $\mathbb{Z}^+$ because,

- $b(0) = 0 \in b\mathbb{Z}$;
- If $a_1, a_2 \in b\mathbb{Z}$ then $a_1 = bk_1, a_2 = bk_2$ for $k_1, k_2 \in \mathbb{Z}$ and so $a_1 + a_2 = bk_1 + bk_2 = b(k_1 + k_2) \in b\mathbb{Z}$

- For any $a = bk \in b\mathbb{Z}$, $-a = b(-k) \in b\mathbb{Z}$

Now we need to prove that any subgroup of $\mathbb{Z}^+$ is $b\mathbb{Z}$ for some b. Let H be an arbitrary subgroup of $\mathbb{Z}^+$. Then by subgroup properties,

- $0 \in H$;
- If $a_1, a_2 \in H$ then $a_1 + a_2 \in H$
- For any $a \in H$, $-a \in H$

We proceed to show that there is always some integer b such that $H = b\mathbb{Z}$. Firstly, if H is the minimal subgroup $\{0\}$ then H trivially conforms to $b\mathbb{Z}$ with $b = 0$.
Otherwise, $\exists a \in H$ s.t. $a \neq 0$ then also $\exists - a \in H$ s.t. $-a \neq 0$. One of these must be a positive non-zero integer so there is at least one such member of H. We take b to be the smallest positive non-zero integer in H. Then,

$b\mathbb{Z} \in H$

- $b \in H$ (by selection) so by subgroup properties $b{+}b \in H$ and $(b{+}b){+}b \in H$ and $b + \cdots + b \in H$
- By subgroup properties $b \in H \implies -b \in H$

So, $\{\, bk \in \mathbb{Z} \mid k \in \mathbb{Z} \,\}$ is in H.

$H \in b\mathbb{Z}$ Take any $n \in H$. Using division with remainder and dividing by b we get,

$$n = bq + r \;\; q \in \mathbb{Z},\, 0 \leq r < b$$

But, since $b\mathbb{Z} \in H$ this means that $bq \in H$ and so $-bq \in H$. Therefore $n - bq = r \in H$. But $0 \leq r < b$ and, by assumption, b is the smallest positive *non-zero* integer in H and so, $r = 0$. So, every $n \in H$ divides by b. □

Greatest Common Divisor

If we extend this to groups which are generated by two integers a, b, then we have a subgroup of $\mathbb{Z}^+$,

$$a\mathbb{Z} + b\mathbb{Z} = \{\, n \in \mathbb{Z} \mid n = ar + bs \;\; r, s \in \mathbb{Z} \,\}$$

This is known as the subgroup *generated* by a, b because it is the smallest subgroup which contains a and b. Proposition 1 tells us that it has the form $d\mathbb{Z}$ for some integer d.

Corollary 1. *If d is the positive integer which generates the subgroup $a\mathbb{Z}+b\mathbb{Z}$ then d is the greatest common divisor of a and b and so,*

- *d can be written in the form $d = ar + bs$ for some integers r and s.*
- *d divides a and b.*
- *If an integer e divides a and b, it also divides d.*

Proof. The first property follows directly from the definition of the subgroup. The second property is a result of the fact that a, b are in the subgroup $a\mathbb{Z} + b\mathbb{Z}$ so that $d\mathbb{Z} = a$ and $d\mathbb{Z} = b$. The third property is evident because $d = ar + bs = ek_1r + ek_2s = e(k_1r + k_2s)$. □

Cyclic Subgroups

Definition. *If we take a single member of a group (along with its inverse and the identity), the subgroup generated by that element takes the form (using multiplicative notation),*

$$H = \{x^{-(n-1)}, \cdots, x^{-2}, x^{-1}, 1, x, x^2, \cdots, x^{n-1}\}$$

where, either, $x^n = 1$ so that there are n distinct values in the group, or else n is infinite and the values never repeat. This is known as a ***cyclic group*** *and also as the* ***subgroup generated by x*** *and is denoted by $\langle x \rangle$.*

The cyclic subgroup, $\langle x \rangle$, generated by x is the smallest subgroup of G containing x in the sense that, if $H \leq G$ and $x \in H$ then $\langle x \rangle \subseteq H$.

Proposition 2. *The set S of integers n such that $x^n = 1$ is a subgroup of $\mathbb{Z}^+$*

Proof. If $x^m = 1$ and $x^n = 1$, then $x^{m+n} = x^m x^n = 1$ also so we have closure of addition. Since $x^0 = 1$, 0 is in the subgroup so we have an identity. Finally, for some n in the subgroup, $x^n = 1 \iff x^{-n} = x^n x^{-n} = x^0 = 1$ so n being in the subgroup implies that $-n$ is also in the subgroup and we have inverses. □

Corollary 2. *It follows from S being a subgroup of $\mathbb{Z}^+$ and from Proposition 1 that S has the form $m\mathbb{Z}$ where m is the smallest positive integer such that $x^m = 1$. Therefore, in H, the m elements $1, x, x^2, \cdots, x^{m-1}$ are all different and any element in H will simplify to one of them: for $n \in S$, $n = mq + r$ such that $x^n = (x^m)^q x^r = 1^q x^r = x^r$.*

Definition. *The **order** of a group G is the number of distinct elements it contains. It is typically denoted $|G|$.*
*An element of a group is said to have **order** m (possibly infinity) if the cyclic subgroup it generates has order m. This means that m is the smallest positive integer with the property $x^m = 1$ or, if the order is infinite, that, $x^m \neq 1$ for all $m \neq 0$.*

Theorem 1. *A group of finite order cannot have any element of infinite order.*

Proof. If G is a group and $x \in G$ has infinite order then,

$$\begin{aligned} & x^m = x^n \\ \iff \quad & x^{m-n} = 1 = x^{n-m} \\ \iff \quad & x^{|m-n|} = 1 \\ \therefore \quad & |m-n| = 0. && \text{because order of x is infinite} \end{aligned}$$

So, there are no two distinct powers of x that produce the same object so that $\langle x \rangle \leq G$, the cyclic group generated by x, is infinite. Since $\langle x \rangle \subseteq G$ this requires that G also be infinite. □

Theorem 2. *If a group element x has finite order m then:*

1. *Let* $n \in \mathbb{Z}$. *If* $n = km + r$ *where* $k, r \in \mathbb{Z}$ *and* $0 \leq r \leq m - 1$, *then* $x^n = x^r$.
2. *For* $n \in \mathbb{N}$, $x^n = 1 \iff m|n$.
3. $1, x, x^2, \ldots, x^{m-1}$ *is a complete, repetition-free, list of elements of* $\langle a \rangle$.
4. *The subgroup* $\langle a \rangle$ *generated by* x *has cardinality* m.

Examples of Cyclic Subgroups

(1) **Cyclic group with order 3**

$$G = \{1, x, x^2\}$$

where $x^3 = 1$ is a cyclic group of order 3 generated by the element x. Note that, since this is a group, it must also contain the inverses, x^{-1}, x^{-2} but $x^3 = 1$ so $x^{-1} = x^2$ and $x^{-2} = x$.

(2) **Symmetries of an equilateral triangle**

Consider an equilateral triangle with vertices labeled A, B, C:

$$\begin{array}{cc} & A \\ B & C. \end{array}$$

Every permutation of the vertices is a transformation that produces an object that occupies the same space as the original, i.e. a *symmetry*. If we take one of them, say, the clockwise rotation one place that results in,

$$\begin{array}{cc} & B \\ C & A \end{array}$$

and we name this r, then clearly – since there are 3 vertices – performing this same rotation 3 times leaves us back where we started. So, using function composition as the law of composition and multiplicative notation, $r^3 = i$ where i is the identity transformation. Also the inverse of r is r^2. So, we have a group consisting of $\{i, r, r^2\}$ and function composition. Notice the resemblance of this group to the previous group $\{1, x, x^2\}$; this group is *isomorphic* to the cyclic group of order 3.

(3) Group $(\mathbb{Z}_5^*, \otimes)$

Consider the element 2 modulo 5. Using multiplicative notation we have,

$$2^2 = 4, 2^3 = 8 = 3, 2^4 = 16 = 1, 2^5 = 32 = 2.$$

So $2^1 = 2^5 \iff 1 = 2^4$ meaning that the element 2 has order 4 in the group and we see, as expected that the group it generates, $\langle 2 \rangle$ has 4 members. In this case, the members are all the members of the group – that's to say, *the element 2 generates the whole group.* If we consider the element 4 we have,

$$4^2 = 16 = 1, 4^3 = 64 = 4.$$

So this element oscillates between 1 and 4 and so, the cyclic subgroup that it generates $\langle 4 \rangle$ has order 2.
Since the group $(\mathbb{Z}_5^*, \otimes) = \langle 2 \rangle$ it can also be described as a cyclic group. This will be the case for any such group modulo a prime number – i.e. $(\mathbb{Z}_p^*, \otimes)$ where p is prime.

(4) Cyclic group with infinite order

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

under matrix multiplication (which is commutative in this case), generates a cyclic group of infinite order because

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

(5) **The Klein Four Group,** V is the simplest group that is not cyclic (it cannot be generated by a single element). It appears in many forms but, as an example, it can be realized as the group consisting of the four matrices,

$$\begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix}$$

Any two non-identity elements generate V.

Isomorphisms **(tags: abstract algebra)**

Definition. *An* ***isomorphism*** *is a bijection between two groups that preserves the structure of the groups by being compatible with the law of composition of both groups. More formally, two groups are* ***isomorphic*** *if there exists a bijection* $\phi : G \longmapsto G'$ *such that,*

$$\phi(ab) = \phi(a)\phi(b) \textit{ for all } a, b \in G$$

where ab *represents composition according to the law of composition of* G *and* $\phi(a)\phi(b)$ *represents composition according to the law of composition of* G'.

> *An* ***isomorphism*** *is a* ***bijection*** *between two* ***groups****. That's to say, it is already assumed in the definition of an isomorphism that the codomain* G' *is a group.*

Proposition 3. *As a consequence of this sole property that, across the bijection, the respective laws of composition are preserved, all other properties of the groups are also preserved.*

Proof. Let e be the identity in G and $e' = \phi(e) \in G'$, and $1'$ be the identity element in G' then,

- Since G' is a group, it has the inverses property that every element has an inverse so,

$$\begin{aligned} & e' = \phi(e) = \phi(ee) = \phi(e)\phi(e) = e'e' && \text{using preservation of law of composition} \\ \iff \quad & (e')^{-1}e' = ((e')^{-1}e')e' && \text{using the inverses property of } G' \\ \iff \quad & 1' = e' \end{aligned}$$

  which implies that e' is the identity in G' so that ϕ maps the identity in G to the identity in G'.

- We can use the fact just shown that $\phi(e) = e' = 1'$ to show,

$$\begin{aligned} & 1' = e' = \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) && \text{using preservation of law of composition} \\ \iff \quad & \phi(a)^{-1}1' = \phi(a)^{-1}\phi(a)\phi(a^{-1}) && \text{using the inverses property of } G' \\ \iff \quad & \phi(a)^{-1} = \phi(a^{-1}) \end{aligned}$$

  which shows that ϕ maps $a^{-1} \in G$ to $\phi(a)^{-1} \in G'$.

□

For example, if $e \in G$ is the identity of G mapped to an element $e' = \phi(e) \in G'$, then for any $a \in G$ mapped to $a' = \phi(a) \in G'$,

$$a' = \phi(a) = \phi(ea) = \phi(e)\phi(a) = e'a'$$

And $a' = e'a' = a'e'$ means that e' is the identity in G'. Furthermore, the order of elements in G and G' will also be the same as,

$$a^n = e \iff e' = \phi(e) = \phi(a^n) = \phi(a)^n = (a')^n$$

Since two isomorphic groups have the same properties, it is often convenient to identify them with each other when speaking informally. For example, the symmetric group S_n of permutations of $\{1, \cdots, n\}$ is isomorphic to the group of permutations matrices, a subgroup of $GL_n(\mathbb{R})$ and we often blur the distinction between these two groups.

Notation. Sometimes when two groups are isomorphic this is indicated using the notation,

$$G \approx G'$$

Examples

- Let $C = \{\cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots\}$ be an infinite cyclic group. Then the map,
$$\phi : \mathbb{Z}^+ \longmapsto C \text{ s.t. } \phi(n) = a^n$$
is an isomorphism where the preservation of the respective laws of composition can be seen as,
$$\phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n)$$
and also $n + (-n) = 0$ and,
$$\phi(-n) = a^{-n} = (a^n)^{-1}.$$

- Let G be the set of real matrices of the form,
$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$$
This is a subgroup of $GL_2(\mathbb{R})$ and so, its law of composition is the same as that of $GL_2(\mathbb{R})$, i.e. matrix multiplication.
$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix}$$
So, G is isomorphic to $\mathbb{R}^+$, the additive group of reals.

Definition. *The groups isomorphic to a given group G form what is called the* ***isomorphism class*** *of G. Groups are often classified into isomorphism classes, for example, there is one isomorphism class of groups of order 3 and there are two classes of groups of order 4 and five classes of 12.*

Proposition 4. *There is only one isomorphism class for each order of cyclic group.*

Proof. Any two cyclic groups of the same order are isomorphic because, if
$$G = \{1, x, x^2, \cdots, x^{n-1}\},\ G' = \{1, y, y^2, \cdots, y^{n-1}\}$$
are two cyclic groups of order n then the map $\phi(x^i) = y^i$ is an isomorphism. □

Automorphisms

Definition. *The domain and codomain of an isomorphism can be the same set of objects so that $\phi : G \longmapsto G$. This is known as an* ***automorphism****.*

Example Let $G = \{1, x, x^2\}$ be a cyclic group of order 3 so that $x^3 = 1$. The transposition which interchanges x and x^2 is an automorphism of G,

$$\begin{array}{ccc} 1 & \longmapsto & 1 \\ x & \longmapsto & x^2 \\ x^2 & \longmapsto & x \end{array}$$

	1	x	x^2
1	1	x	x^2
x	x	x^2	1
x^2	x^2	1	x

$\longmapsto$

	1	x^2	x
1	1	x^2	x
x^2	x^2	x	1
x	x	1	x^2

This is because the group is cyclic and x and x^2 have the same order ($x^3 = 1$ and also $(x^2)^3 = x^6 = (x^3)^2 = 1^2 = 1$). So the law of composition is preserved.

Conjugation The most important example of automorphism is conjugation.

Definition. ***Conjugation*** *by $b \in G$ is the map from G to itself defined by,*

$$\phi(a) = bab^{-1}$$

with the result that,

$$ba = \phi(a)b$$

so that we can think of conjugation of a by b as the way that we need to change a if we want to move the multiplication by b to the other side.

This is an automorphism because it

- is compatible with law of composition,

  $$\phi(xy) = bxyb^{-1} = bxb^{-1}byb^{-1} = \phi(x)\phi(y)$$

- has an inverse so it is bijective,

  $$(\phi^{-1} \circ \phi)(a) = \phi^{-1}(\phi(a)) = b^{-1}(bab^{-1})b = (b^{-1}b)a(b^{-1}b) = a$$

  Note that this is different from the inverse element of a corresponding under the mapping ϕ,

  $$\phi(a)\phi(a^{-1}) = bab^{-1}ba^{-1}b^{-1} = ba(1)a^{-1}b^{-1} = b(1)b^{-1} = 1$$

Another thing to note is that - in an abelian group where the composition law is commutative - conjugation becomes the identity map,

$$ba = ab \iff bab^{-1} = a \iff \phi(a) = a$$

Homomorphisms **(tags: abstract algebra)**

Definition. *A* ***homomorphism*** *is a mapping (not necessarily bijective) between two groups, $\phi : G \longmapsto G'$, such that,*

$$\phi(ab) = \phi(a)\phi(b) \textit{ for all } a, b \in G$$

where ab represents composition according to the law of composition of G and $\phi(a)\phi(b)$ represents composition according to the law of composition of G'.

So, the difference between a *homomorphism* and a *isomorphism* is that the latter is bijective whereas the former is not. As a result, a *homomorphism* may be one-way only.

> *A* ***homomorphism*** *is a* ***mapping*** *between two* ***groups****. That's to say, it is already assumed in the definition of a homomorphism that the codomain G' is a group.*

Examples of homomorphisms

(6) Let $C = \{a^{n-1}, \cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots, a^{n-1}\}$ be a finite cyclic group. Then the map,

$$\phi : \mathbb{Z}^+ \longmapsto C \ \text{ s.t. } \ \phi(n) = a^n$$

is a homomorphism. Note that if C were an infinite cyclic group then this would be an isomorphism.

(7) the sign of a permutation $sign : S_n \longmapsto \pm 1$

(8) the determinant function $det : GL_n(\mathbb{R}) \longmapsto \mathbb{R}^\times$

(9) an arguably trivial example is called the *inclusion* map $i : H \longmapsto G$ of a subgroup H into a group G, defined by $i(x) = x$. It functions as the identity for elements in the subgroup H but, since it is not surjective, there is no inverse mapping.

Image of a homomorphism

Since a homomorphism is not bijective it has an image different to the codomain group,

$$im\ \phi = \{\, x \in G' \mid \exists a \in G \text{ s.t. } \phi(a) = x \,\}$$

The image of a homomorphism is a subgroup of the codomain group G' because the homomorphism preserves the group structure as described in Proposition 3.

Notation. The image of the mapping ϕ with domain G is sometimes denoted $\phi(G)$.

Kernel of a homomorphism

Definition. *The* ***kernel*** *of a homomorphism is the set of elements in the domain that are mapped to the identity,*

$$ker\ \phi = \{\, a \in G \mid \phi(a) = 1' \,\}$$

Proposition 5. *The kernel of a homomorphism is a subgroup of the domain group G.*

Proof. If $a, b \in ker\ \phi$ then,

- closure: $\phi(ab) = \phi(a)\phi(b) = 1' \cdot 1' = 1'$ which shows that

$$a, b \in ker\ \phi \implies ab \in ker\ \phi.$$

- identity: By Proposition 3, $1' = e' = \phi(e)$ and so $e \in ker\ \phi$.
- inverses: Since $a \in ker\ \phi$, then

$$\begin{aligned} & 1' = e' = \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) = 1'\phi(a^{-1}) \\ \iff \quad & 1' = \phi(a^{-1}) \end{aligned}$$

so that $a \in ker\ \phi \iff a^{-1} \in ker\ \phi$.

□

Examples of Kernels of Homomorphisms

(10) The determinant function 8, $det : GL_n(\mathbb{R}) \longmapsto \mathbb{R}^{\times}$ - has a kernel,

$$\{\, \text{real } n \times n \text{ matrices } A \mid det\, A = 1 \,\},$$

which is a subgroup of $GL_n(\mathbb{R})$ known as the *special linear group* $SL_nn(\mathbb{R})$.

(11) The sign of a permutation 7 has a kernel that is the set of *even* permutations,

$$A_n = \{\text{even permutations}\},$$

which is a subgroup of the symmetric group S_n and is known as the *alternating group*, A_n.

(12) The map from the additive group of integers to a finite cyclic group 6,

$$\phi : \mathbb{Z}^+ \longmapsto C \ \text{ s.t. } \ \phi(n) = a^n$$

has the kernel,

$$ker\ \phi = \{\, n \in \mathbb{Z}^+ \mid a^n = 1 \,\}$$

which has been proven to be a subgroup in Proposition 2.

Normal Subgroups

Definition. *A subgroup N of a group G is called a* ***normal subgroup*** *if it has the property that,*

$$\forall\, a \in N, b \in G,\ bab^{-1} \in N$$

which is to say, that the conjugate by any element of G of any element in N is also in N.

Examples of Normal Subgroups

(13) The kernel of a homomorphism is a normal subgroup because,

$$\begin{aligned} a \in ker\ \phi \iff & \phi(a) = 1 \\ \implies \quad & \phi(baa^{-1}) = \phi(a) \cdot 1 \cdot \phi(a^{-1}) \\ \iff \quad & \phi(baa^{-1}) = \phi(a)\phi(a)^{-1} \qquad \text{using Proposition 3} \\ \iff \quad & \phi(baa^{-1}) = 1. \end{aligned}$$

So,

a. $SL_n(\mathbb{R})$ 10 is a normal subgroup of $GL_n(\mathbb{R})$;

b. A_n 11 is a normal subgroup of the symmetric group S_n.

(14) Any subgroup of an abelian group is normal because when the composition law is commutative, as was mentioned in the section on conjugation,

$$ba = ab \iff bab^{-1} = abb^{-1} = a$$

so that conjugation becomes the identity map and so, trivially, all conjugates of elements in a subgroup are also in the subgroup.

Subgroups of non-abelian groups, however, need not be normal. For example,

(15) Group T of invertible upper triangular matrices is not a normal subgroup of $GL_2(\mathbb{R})$. To show this note,

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, BAB^{-1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

where $A \in T, B \in GL_2(\mathbb{R})$ but $BAB^{-1} \notin T$.

The center of a group

Definition. *The **center** of a group G is the set of elements that commute with every element of G,*

$$Z = \{\, z \in G \mid zx = xz,\ \forall x \in G \,\}.$$

Notation. The **center** of a group G may be denoted by Z or by $Z(G)$.

The center of a group, Z, is a subgroup of G. This can be easily seen as,

$$\forall a, b \in Z, x \in G\ .\ (ab)x = axb = x(ab)$$

and,

$$\forall a \in Z, x \in G\ .\ ax = xa \iff a^{-1}ax = x = a^{-1}xa \iff xa^{-1} = a^{-1}x.$$

For example,

(16) The center of the general linear group $GL_n(\mathbb{R})$ is the group of *scalar matrices* of the form cI for $c \in \mathbb{R}$, i.e. matrices of the form,

$$\begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}$$

in $GL_2(\mathbb{R})$. Note that, for *diagonal* matrices whose elements on the main diagonal are all non-zero but not-necessarily equal as in *scalar* matrices, multiplication is commutative with other diagonal matrices but not generally so with other matrices in the general linear group.

Equivalence Relations and Partitions (tags: abstract algebra)

Notation. In the following treatment of equivalence relations we will use the notation $a \sim b$ to denote the equivalence of a and b; $\overline{a}$ to indicate the equivalence class of a; and $\overline{S}$ to indicate the partition of S comprised of equivalence classes such as the class $\overline{a} = \overline{b}$ which includes both a and b.

Any map of sets $\phi : S \longmapsto T$ defines an equivalence relation on the domain S such that $a \sim b$ iff $\phi(a) = \phi(b)$. We will refer to this as the *equivalence relation determined by the map.* The corresponding partition is made up of the sets of elements in the domain S that are mapped to the same element in the codomain T.

Definition. *Let $\phi : S \longmapsto T$ be a map, then the **inverse image** of an element $t \in T$ is defined as,*

$$\phi^{-1}(t) = \{\, s \in S \mid \phi(s) = t \,\}$$

and can also be applied to a set $U \in T$ as,

$$\phi^{-1}(U) = \{\, s \in S \mid \phi(s) \in U \,\}$$

*Note that in this notation, ϕ^{-1} **does not indicate an inverse function** as the inverse of the function may not exist but the inverse image is nevertheless defined.*
*The inverse images - the sets $\phi^{-1}(t)$ for all $t \in T$ - may also be called the **fibres** of the map ϕ.*

Clearly, the non-empty fibres of the map ϕ form a partition of S. We can express this partition of S as a bijection, that we shall call $\overline{\phi}$, between the fibres of ϕ in S and the element of the image of S to which their members are mapped,

$$\overline{\phi} : \overline{S} \longmapsto im\ \phi$$

so that,

$$\overline{\phi}(\overline{s}) = \phi(s).$$

Congruence

Since a homomorphism maps the identity to the identity and inverses to inverses (Proposition 3), we can deduce that the inverse image of the identity in G' is going to contain at least the identity of G and that the inverse image of an element $(a')^{-1} \in G'$ will contain at least the element $a^{-1} \in G$. So, in terms of equivalence classes we can say that, for a homomorphism ϕ,

$$1 = e \in \phi^{-1}(1') \implies \overline{\phi}(\overline{1}) = 1'$$

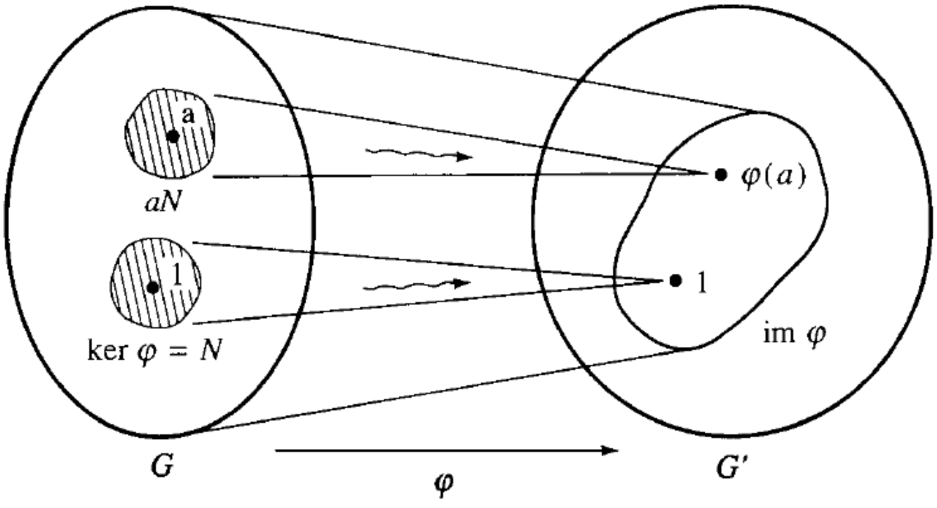


Figure 1: A schematic diagram of a group homomorphism

$$a^{-1} \in \phi^{-1}((a')^{-1}) \implies \overline{\phi}(\overline{a^{-1}}) = (a')^{-1}$$

Definition. *The equivalence relation determined by a homomorphism is known as* ***congruence*** *and is commonly denoted using* $\equiv$ *instead of* $\sim$*. For a homomorphism* ϕ*,*

$$a \equiv b \iff \phi(a) = \phi(b).$$

Since ϕ *is a homomorphism we also have,*

$$a \equiv b \iff \phi(ac) = \phi(bc),\ \phi(a^{-1}) = \phi(b^{-1}).$$

More generally, a ***congruence relation*** *is an equivalence relation on an algebraic structure (such as a group, ring, or vector space) that is compatible with the structure in the sense that algebraic operations done with equivalent elements will yield equivalent elements.*

Congruence Examples

(17) The modulus function of complex numbers forms a homomorphism from the multiplicative group of complex numbers to the multiplicative

group of reals,

$$\phi : \mathbb{C}^\times \longmapsto \mathbb{R}^\times \text{ s.t. } \phi(a) = |a|$$

and the induced equivalence relation is $a \equiv b \iff |a| = |b|$. The fibres of this map are the concentric circles about 0. They are in bijective correspondence with elements of *im* ϕ, the set of positive reals.

Proposition 6. *If $\phi : G \longmapsto G'$ is a group homomorphism with kernel N then, for $a, b \in G$,*

$$\phi(a) = \phi(b) \iff \exists n \in N, \ s.t. \ b = an$$

or, equivalently, $a^{-1}b \in N$.

Proof.

$$\begin{aligned}
& b = an & \\
\implies \quad & \phi(b) = \phi(an) & \\
\implies \quad & \phi(b) = \phi(a)\phi(n) & \text{by homomorphism property} \\
\implies \quad & \phi(b) = \phi(a)1' & \text{n is in the kernel} \\
\implies \quad & \phi(b) = \phi(a) &
\end{aligned}$$

$$\begin{aligned}
& \phi(b) = \phi(a) & \\
\implies \quad & \phi(a)^{-1}\phi(b) = 1' & \text{codomain is a group so has inverses} \\
\implies \quad & \phi(a^{-1})\phi(b) = 1' & \text{by Proposition 3} \\
\implies \quad & \phi(a^{-1}b) = 1' & \text{by homomorphism property} \\
\implies \quad & a^{-1}b = n \in N & \\
\implies \quad & b = an &
\end{aligned}$$

□

Corollary 3. *A group homomorphism is injective if and only if its kernel is the trivial subgroup $\{1\}$. So, a homomorphism is an isomorhpism if its kernel contains only the identity and its image is the whole of the codomain (i.e. it's surjective).*

Cosets (tags: abstract algebra)

The set of elements of the form an - described in Proposition 6 - is denoted by aN and is called a *coset* of N in G.

Definition. *A coset can be defined for any subgroup H of a group G. A* ***left coset*** *is a subset of the form,*

$$aH = \{\, ah \mid h \in H \,\}.$$

Cosets are not, in general, subgroups. This can be easily seen as the left coset aH does not contain the identity as, although H contains the identity, aH contains $a1 = a$.

Note that the arbitrary subgroup H could also be thought of as a coset $1H = H$ and also that the left cosets aH are equivalence classes for the congruence relation,

$$a \equiv b \iff b = ah,\ h \in H.$$

This is a congruence because, for some arbitrary $c \in G$,

$$1 \equiv c \iff \exists h \in H \text{ s.t. } c = 1h = h.$$

That's to say, the elements that are congruent to the identity are precisely the members of the subgroup H so that it plays a similar role to the kernel N in Proposition 6. Furthermore, since the congruence relation is an equivalence relation it forms a partition of the domain G.

Proposition 7. *The left cosets of a subgroup partition the group.*

Proof. The left cosets are equivalence classes and, as a result, they partition the group. □

Examples of cosets

(18) The coset of an element with the kernel N,

$$aN = \{\, g \in G \mid g = an,\ n \in N \,\}$$

is the set of all elements that are *congruent* to a. The *congruence classes* are precisely the cosets aN for each $a \in G$. They are also the *fibres* of the homomorphic map.

(19) Continuing the example of the symmetric group S_3 represented as

$$G = \{1, x, x^2, y, xy, x^2y\}$$

with group multiplication rules,

$$x^3 = 1, y^2 = 1, yx = x^2y.$$

The element xy has order 2 so it generates a cyclic subgroup $H = \{1, xy\}$ of order 2. The left cosets of H in G are the three sets,

$$\{1, xy\} = 1H = xyH,\ \{x, x^2y\} = xH = x^2yH,\ \{x^2, y\} = x^2H = yH.$$

Note that they do partition the group G. Also, notice that the cosets aH for $a \in H$ produce the subgroup H itself as should be expected as the group properties of the subgroup dictate that all products of its elements are already present in the subgroup. For this reason, the cosets aH that are distinct from H are those such that $a \notin H$.

The index of a subgroup

Definition. *The **index** of a subgroup is the number of left cosets it forms in the parent group.*

Notation. The **index** of a subgroup H in G is denoted by $[G : H]$.

In the example (19) the index of H is 3. Note that if G were to contain infinitely many elements then the index of a subgroup may also be infinite.

Proposition 8. *Each coset aH has the same number of elements as H.*

Proof. As usual, equal cardinality is demonstrated by showing the existence of a bijection. It is clear that there is a bijective map between the subgroup H and any coset aH because the map $H \longmapsto aH$ is,

- injective because $ah = ah' \implies h = h'$ because by group properties a has an inverse in G;
- surjective because every $c \in aH$ has the form ah and is therefore mapped to by some $h \in H$.

□

Lagrange's Theorem

Since the left cosets of H in G form a partition of G and their order is the same as that of H we see that the order of G is the order of H multiplied by its index in G. This results in a formula known as the *Counting Formula* as follows,

$$|G| = |H| \cdot [G : H].$$

If G is of infinite order and H is finite, then the index of H in G will be infinite.

Theorem 3. ***Lagrange's Theorem:*** *Let G be a finite group, and let H be a subgroup of G. The order of H divides the order of G.*

Corollary 4. *Let G be a finite group, and let a be an element of G. Then the order of a divides the order of G. That's to say, the order of the cyclic group generated by a, $|\langle a \rangle|$, divides $|G|$.*

Corollary 5. *If G is a group of order n, then $g^n = e$ for every element g of G.*

Proof. This is clearly a consequence of the previous corollary. If we let the order of g be m, then by the previous corollary,

$$m \mid n \iff n = km \text{ for } k \in \mathbb{N} \iff g^n = g^{km} = (g^m)^k = e^k = e. \qquad \square$$

Corollary 6. *Suppose that a group G has p elements and that p is a prime integer. Let $a \in G$ be any element, not the identity. Then G is the cyclic group $\{1, a, \ldots, a^{p-1}\}$ generated by a.*

Proof. Since $a \neq 1$ by selection, it has order greater than 1. Since its order must divide the order of G, which is prime, its order is equal to the order of G, p. So, the order of the nonidentity element a is the same as the order of G and so it generates the whole group. □

Corollary 7. *All groups with some prime order, p, are in the same isomorphism class.*

Proof. Any group with prime order p is the cyclic group of order p and by Proposition 4 there is only a single isomorphism class for each cyclic group of a given order. □

Example applications of Lagrange Theorem

(20) **Fermat's Little Theorem**: *If p is a prime number then*

$$a^p \equiv a \bmod p \textit{ for all } a \in \mathbb{Z}.$$

> *We need to be a little careful here. We might assume – given that we are multiplying the integer a in modulo p that the group we want to use is $(\mathbb{Z}_p, \otimes)$. However, this is not a group! The reason is that $\mathbb{Z}_p$ contains 0 which has no inverse under the proposed law of composition, multiplication.*
>
> *If, however, we take $\mathbb{Z}_p^*$ where the $*$ means $\mathbb{Z}/\{0\}$ then we have a set of $p-1$ distinct elements. Over this set we can form the multiplicative group $G = (\mathbb{Z}_p^*, \otimes)$ because the primality of p means that every element has a multiplicative inverse.*
>
> *Note that this is **not** a group of prime order. The primality of p is essential to make sure that every element has a multiplicative inverse but, since we also have to eliminate 0 for the same reason, the order is $p-1$ which is not necessarily prime.*

Proof. Take the set $\mathbb{Z}_p^*$ under multiplication and some arbitrary $a \in \mathbb{Z}$.

(i) Primality of p means that it is possible to find $1 = na + mp$ for $m, n \in \mathbb{Z}$ (see 1). This implies that there exists a multiplicative inverse of every non-zero element in modulo p. Specifically, n is the inverse of a because $na = (-m)p + 1 \iff na \bmod p \equiv 1$.

(ii) Existence of the multiplicative inverses implies that we have a group $G = (\mathbb{Z}_p^*, \otimes)$.

(iii) G being a group implies that, for any element $a \in G$, by 5 we have $a^{p-1} = 1$.

(iv) In G, $a^{p-1} = 1 \iff a^p = a$ which translates to $a^p \equiv a \bmod p$.

□

Lagrange's Theorem and Homomorphisms

The Counting Formula can also be applied when a homomorphism is given. Let $\phi : G \longmapsto G'$ be a homomorphism. As we saw in coset example 18, the left cosets of $ker\ \phi$ are the fibres of the map ϕ. They are in bijective correspondence with the elements of the image. Therefore,

$$[G : ker\ \phi] = |im\ \phi| \,.$$

Which implies that,

Corollary 8. *If $\phi : G \longmapsto G'$ is a homomorphism of finite groups then,*

$$|G| = |ker\ \phi| \cdot |im\ \phi| \,.$$

As a result, $|ker\ \phi|$ divides $|G|$, and $|im\ \phi|$ divides both $|G|$ and $|G'|$.

Right Cosets

Right cosets also exist and are defined as,

$$Ha = \{\, g \in G \ |\ g = ha,\ h \in H \,\}$$

and these are equivalence classes for the *right congruence* relation,

$$a \equiv b \iff b = ha,\ h \in H.$$

Right cosets are not necessarily the same as left cosets. For instance, continuing the example in 19, the right cosets of the subgroup $\{1, xy\}$ of S_3 are,

$$\{1, xy\} = H1 = Hxy,\ \{x, y\} = Hx = H,\ \{x^2, x^2y\} = Hx^2 = Hx^2y.$$

Note that this generates a different partition of G then was generated by the left cosets.

Proposition 9. *A subset H of a group G is normal if and only if every left coset is also a right coset. If H is normal then,*

$$\forall a \in G,\ aH = Ha.$$

Proof. Suppose that H is normal. For any $h \in H$ and any $a \in G$,

$$ah = (aha^{-1})a.$$

Since H is normal, the conjugate by h of a is also in H, that's to say, $aha^{-1} \in H$ which implies that $(aha^{-1})a \in Ha$. Therefore, any arbitrary member of aH is also a member of Ha. Clearly, the same proof also works in the other direction so that any member of Ha is also a member of aH and the two cosets are equal. So, we have shown that (H is normal) $\implies$ (left and right cosets of H are equal).

Now we need to show that (left and right cosets of H are equal) $\implies$ (H is normal). Firstly, clearly the above logic doesn't apply if H is not normal; there will be at least one element whose conjugate is not in H so $aH \neq Ha$. However, it could still be the case that each left coset is also a right coset if, for every a in G, there is some b in G such that $aH = Hb$. However, this is not possible because aH and Ha both contain a which means that in a given partition of G they must be the same partition. So $aH \neq Ha$ implies that the partitions are different; Ha creates different equivalence classes. Therefore (left and right cosets of H are equal) $\implies$ (H is normal). □

Fields (tags: abstract algebra)

Complex Numbers (tags: abstract algebra, complex numbers)

Proposition 10. *For every $\alpha \in \mathbb{C}$, there exists a unique $\beta \in \mathbb{C}$ such that $\alpha + \beta = 0$.*

Proof. By contradiction: Say there are two such elements, β, γ such that,

$$\begin{aligned} \alpha + \beta = 0 &= \alpha + \gamma \\ (\alpha + \beta) + \beta &= (\alpha + \beta) + \gamma \\ 0 + \beta = \beta &= 0 + \gamma = \gamma \end{aligned} \qquad \square$$

Proposition 11. *For every $\alpha \in \mathbb{C}$ with $\alpha \neq 0$, there exists a unique $\beta \in \mathbb{C}$ such that $\alpha\beta = 1$.*

Proof. By contradiction: Say there are two such elements, β, γ then,

$$\begin{aligned} \alpha\beta &= 1 = \alpha\gamma \\ \beta &= \frac{1}{\alpha} = \gamma \end{aligned} \qquad \square$$

Complex Numbers Problems (tags: abstract algebra, complex numbers)

Find all the roots of $x^3 = 1$ for $x \in \mathbb{C}$ (tags: complex numbers)

Since $x^3 - 1 = (x-1)(x^2+x+1)$, we have (via zero-factor theorem) possible roots from,

$$x - 1 = 0 \iff x = 1$$

$$x^2 + x + 1 = 0 \implies x = \frac{-1 \pm \sqrt{-3}}{2} = \frac{-1 \pm \sqrt{3}\,i}{2}$$

More generally,

$$(a + bi) + (a - bi) = 2a$$

and since also,

$$\left[\frac{-1 + \sqrt{3}\,i}{2}\right]^2 = \frac{-1 - \sqrt{3}\,i}{2}$$

as well as the reverse,

$$\left[\frac{-1 - \sqrt{3}\,i}{2}\right]^2 = \frac{-1 + \sqrt{3}\,i}{2}$$

this means that if $x = \frac{-1 \pm \sqrt{3}\,i}{2}$ then $x^2 + x$ is of the form $(a+bi)+(a-bi) = 2a$ and so we have that $x^2 + x = -1 \iff x^2 + x + 1 = 0$.

In addition,

$$(a + bi)(a - bi) = a^2 + b^2$$

which means that if $x = \frac{-1 \pm \sqrt{3}\,i}{2}$ then $x^3 = x^2 x$ is of the form $(a+bi)(a-bi) = a^2 + b^2$ so we have that $x^3 = \frac{-1}{2}^2 + \frac{\sqrt{3}}{2}^2 = \frac{1}{4} + \frac{3}{4} = 1$.

So we see that - allowing for complex x - the cubic polynomial $x^3 - 1$ has 3 roots as we should expect from the Fundamental Theorem of Algebra *(is this the correct interpretation of this?)*.

Number Theory (tags: number theory)

Natural Numbers (tags: number theory)

Peano Axioms (tags: number theory)

Axiom 1. *Closure under addition:*
For all $a, b \in \mathbb{N}$ we have $a + b \in \mathbb{N}$.

Axiom 2. *Closure under multiplication:*
For all $a, b \in \mathbb{N}$ we have $a \times b \in \mathbb{N}$.

Axiom 3. *Commutative Law for addition:*
For all $a, b \in \mathbb{N}$ we have $a + b = b + a$.

Axiom 4. *Associative Law for addition:*
For all $a, b, c \in \mathbb{N}$ we have $(a + b) + c = a + (b + c)$.

Axiom 5. *Commutative Law for multiplication:*
For all $a, b \in \mathbb{N}$ we have $a \times b = b \times a$.

Axiom 6. *Associative Law for multiplication:*
For all $a, b, c \in \mathbb{N}$ we have $(a \times b) \times c = a \times (b \times c)$.

Axiom 7. *Multiplicative Identity:*
There is a special element of $\mathbb{N}$, denoted by 1, which has the property that for all $n \in \mathbb{N}$, $n \times 1 = n$.

Axiom 8. *Additive cancellation:*
For all $a, b, c \in \mathbb{N}$ if $a + c = b + c$ then $a = b$.

Axiom 9. *Multiplicative cancellation:*
For all $a, b, c \in \mathbb{N}$ if $a \times c = b \times c$ then $a = b$.

Axiom 10. *Distributive Law:*
For all $a, b, c \in \mathbb{N}$, $a \times (b + c) = (a \times b) + (b \times c)$.

Axiom 11. *Definition of "less than":*
For all $a, b \in \mathbb{N}$, $a < b$ if and only if there is some $c \in \mathbb{N}$ s.t. $a + c = b$.

Axiom 12. *Trichotomous property:*
For all $a, b \in \mathbb{N}$ exactly one of the following is true: $a = b$, $a < b$, $b < a$.

Notation: We also write ab for $a \times b$.

Properties following from these axioms (tags: number theory)

Proposition 12. *If $a, b \in \mathbb{N}$ satisfy $a \times b = a$, then $b = 1$.*

Proof.

$$\begin{aligned} & a \times b = a = a \times 1 && \text{by Multiplicative Identity axiom} \\ \iff \quad & b \times a = 1 \times a && \text{by Commutative Law for multiplication} \\ \iff \quad & b = 1 && \text{by Multiplicative cancellation} \end{aligned}$$

□

Proposition 13. *If $a, b, c \in \mathbb{N}$ and $a < b$ then $a \times c < b \times c$.*

Proof.

$$\begin{aligned} & a < b \implies a + d = b \text{ for some } d \in \mathbb{N} && \text{by Definition of "less than"} \\ \therefore \quad & b \times c = (a + d) \times c = (a \times c) + (d \times c) && \text{by Distributive Law} \\ \therefore \quad & a \times c < (a \times c) + (d \times c) = b \times c && \text{by defn. "less than" and closure} \end{aligned}$$

□

Proposition 14. 1 *is the least element of* $\mathbb{N}$.

Proof. Assume m is the least element of $\mathbb{N}$. Then, also $m < 1$. So, by Proposition 13,

$$m < 1 \implies m \times m < 1 \times m = m$$

But, closure of multiplication and $m \times m < m$ together contradict the assumption that m is the least element of $\mathbb{N}$.
Therefore m cannot be less than 1. Since we know that $1 \in \mathbb{N}$ and that the minimum element of $\mathbb{N}$, m, cannot be less than 1, it follows that 1 must be the minimum element of $\mathbb{N}$ and $m = 1$. □

Integers (tags: number theory)

Odd and Even Numbers (tags: number theory)

Definition. *An **even** number, $n \in \mathbb{Z}$, is one that satisfies,*

$$\exists\, m \in \mathbb{Z} \;\cdot\; n = 2m$$

Definition. *An **odd** number, $n \in \mathbb{Z}$, is one that satisfies,*

$$\exists\, m \in \mathbb{Z} \;\cdot\; n = 2m + 1$$

Consequences

Sum of even numbers, $m + n$:

$$\begin{aligned} m + n &= 2k + 2l \quad \text{where } k, l \in \mathbb{Z} && \text{by defn. of even no.s } m, n \\ &= 2(k + l) \\ &= 2q \quad \text{where } q \in \mathbb{Z} \end{aligned}$$

So $m + n$ is also even. However, if $m + n$ is even:

$$\begin{aligned} m + n &= 2k \quad \text{where } k \in \mathbb{Z} && \text{by defn. of even } m + n \\ k &= \frac{m}{2} + \frac{n}{2} \end{aligned}$$

So m and n are not necessarily even. A counterexample is

$$3 + 5 = 8 \iff \frac{3}{2} + \frac{5}{2} = 4$$

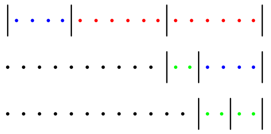
To summarize:

- m, n even $\implies$ $m + n$ even
- $m + n$ even $\implies$ m, n even Wrong!

Divisibility and Primes (tags: number theory)

Greatest Common Divisor (also called Highest Common Factor)

The greatest common divisor of 16 and 6 can be visualized as follows:



$16 = 6 \times 2 + 4$

$6 = 4 \times 1 + 2$

$4 = 2 \times 2 + 0$

This implies the algorithm:

```
gcd($a, b$) :
    if  $b == 0$  then
        return  $a$
    else
        return  gcd($b, b \bmod a$)
    end if
```

Proposition 15. *For non-zero integers a and b, if $a = bq + r$ where $q, r \in \mathbb{Z}$, then $gcd(a, b) = gcd(b, r) = gcd(b, a \bmod b)$.*

Proof. $(a \bmod b) = r = a - bq$. For any m s.t. $m \mid a$ and $m \mid b$ we must also have $m \mid (a - bq)$ so the set of divisors of a and b is a subset of the set of divisors of b and $r = (a \bmod b)$. Conversely, for any m s.t. $m \mid b$ and $m \mid r = (a \bmod b)$ we have that $m \mid (bq + r) = a$ so the set of divisors of b and $r = (a \bmod b)$ is a subset of the set of divisors of a and b. So the sets are equal proving that they must have the same maximum element - the greatest common divisor. □

Proposition 16. *If $d = gcd(a, b)$ then there is no integer linear combination of a and b that equals any positive value less than d.*

Proof. Assume $d = gcd(a, b)$ and that $\exists\, e < d \in \mathbb{N}, m, n \in \mathbb{Z}$ s.t. $e = am + bn$. Then,

$$e = am + bn = dz_1m + dz_2n = d(z_1m + z_2n) \quad \text{for } z_1, z_2 \in \mathbb{Z}$$

$$\iff \qquad z_1m + z_2n = \frac{e}{d} \notin \mathbb{Z}$$

But this is impossible as, by the definition of the integers, $z_1m + z_2n \in \mathbb{Z}$. □

The Fundamental Theorem of Arithmetic **(tags: number theory)**

Definition of prime number: An integer that is only divided cleanly by itself and one. More formally, an integer, p, is prime if it is greater than 1 and,

$$\exists!\, m, n \in \mathbb{Z} \,\cdot\, \frac{p}{m} = n \wedge (m \neq p \wedge m \neq 1)$$

Primality $\implies$ Unique Prime Factorization:

> "Any number either is prime or is measured by some prime number."
> *Euclid, Elements Book VII, Proposition 32*

So, if an integer n is not prime then,

$$\begin{aligned} \exists\, a, b \in \mathbb{Z} \,\cdot\, \frac{n}{a} &= b \\ \iff n &= ab \end{aligned}$$

Then, for a (the same applies to b),

$$\begin{aligned} \exists\, c, d \in \mathbb{Z}\,,\, c, d \notin \{1, a\} \,\cdot\, \frac{n}{a} &= b \\ \iff n &= cd \end{aligned}$$

We can continue to descend like this until we must eventually encounter one or more primes. Furthermore, if a number, n, has a prime factorization, p_1p_2 then,

$$n = p_1p_2 = p_3p_4 \iff \frac{p_1}{p_3} = \frac{p_4}{p_2} = n$$

But $\frac{p_1}{p_3} = n$ contradicts the definition of primeness of p_1. Therefore prime factorizations are unique.

Proof of existence

Proof. It must be shown that every integer greater than 1 is either prime or a product of primes. First, 2 is prime. Then, by strong induction, assume this is true for all numbers greater than 1 and less than n. If n is prime, there is nothing more to prove. Otherwise, there are integers a, b where $n = ab$, and $1 < a \leq b < n$. By the induction hypothesis, $a = p_1p_2...p_j$ and $b = q_1q_2...q_k$ are products of primes. But then $n = ab = p_1p_2...p_jq_1q_2...q_k$ is a product of primes. □

Proof of uniqueness

Proof. Suppose, to the contrary, that there is an integer that has two distinct prime factorizations. Let n be the least such integer and write $n = p_1p_2...p_j = q_1q_2...q_k$, where each p_i and q_i is prime. (Note that j and k are both at least 2.) We see that p_1 divides $q_1q_2...q_k$, so p_1 divides some q_i by Euclid's lemma. Without loss of generality, say that p_1 divides q_1. Since p_1 and q_1 are both prime, it follows that $p_1 = q_1$. Returning to our factorizations of n, we may cancel these two terms to conclude that $p_2...p_j = q_2...q_k$. We now have two distinct prime factorizations of some integer strictly smaller than n, which contradicts the minimality of n. □

Some Proofs on the Integers (tags: number theory)

Proposition 17. *For any integer m, $\sqrt{m}$ is rational iff m is a square, i.e. $m = a^2$ for some integer a.*

To begin with we show the easier direction of implication: $(m = a^2) \implies (\sqrt{m}$ is rational).

Proof. Assume $m, a, b \in \mathbb{Z}$.

$$\begin{aligned} & m = a^2 \\ \iff & \sqrt{m} = |a| \\ & = a/b \text{ for } b = 1 \text{ or } -1. \end{aligned}$$

□

Now the other (harder) direction, ($\sqrt{m}$ is rational) $\implies (m = a^2)$.

Proof. Assume $m, a, b \in \mathbb{Z}$. ($\sqrt{m}$ is rational) can be formalized as:

$$\exists\, m, a, b \in \mathbb{Z} \cdot (\sqrt{m} = \frac{a}{b}) \;\wedge\; (a \text{ and } b \text{ are coprime})$$

$$\sqrt{m} = \frac{a}{b}$$

$$\implies m = \frac{a^2}{b^2}$$

$$\iff mb^2 = a^2$$

But a and b are coprime so they don't share any prime factors. This means that a^2 and b^2 also don't share any prime factors. So, if $|b| > 1$, the prime factorization of mb^2 is necessarily different from that of a^2 meaning that $mb^2 \neq a^2$ contradicting the hypothesis of coprimality. On the other hand, if $|b| = 1$, then b has no prime factors (its prime factorization is empty) and so mb^2 has the same prime factorization as m which may be equal to that of a^2 in the case that $m = a^2$. □

Proposition 18. *For all nonnegative integers $a > b$ the difference of squares $a^2 - b^2$ does not give a remainder of 2 when divided by 4.*

Beginner's attempt - try proof by contradiction:

$$\begin{aligned} a^2 - b^2 &= 4n + 2 \\ 2k &= 4n + 2 && \text{by } a^2 - b^2 \text{ even} \\ k &= 2n + 1 \implies k \text{ is some odd number.} \end{aligned}$$

So, proof by contradiction is our first instinct but doesn't seem to get us anywhere. Instead, proceed by cases:

Case a, b are even:

$$\begin{aligned} &\exists\, k, l \in \mathbb{Z} \,\cdot\, a = 2k, b = 2l \\ &\implies a^2 - b^2 = 4k^2 - 4l^2 \\ &\qquad\qquad = 4\left(k^2 - l^2\right) \\ &\qquad\qquad = 4m \;\text{ where }\; m \in \mathbb{Z} \end{aligned}$$

So 4 divides $a^2 - b^2$ with 0 remainder.

Case a, b are odd:

$$\begin{aligned} &\exists\, k, l \in \mathbb{Z} \,\cdot\, a = 2k + 1, b = 2l + 1 \\ &\implies a^2 - b^2 = \left(4k^2 + 4k + 1\right) - \left(4l^2 + 4l + 1\right) \\ &\qquad\qquad = 4\left(k^2 + k - l^2 - l\right) \\ &\qquad\qquad = 4m \;\text{ where }\; m \in \mathbb{Z} \end{aligned}$$

So, again, 4 divides $a^2 - b^2$ with 0 remainder.

Case a even, b odd:

$$\begin{aligned}
&\exists\, k, l \in \mathbb{Z} \;\cdot\; a = 2k, b = 2l + 1 \\
&\implies a^2 - b^2 = 4k^2 - \left(4l^2 + 4l + 1\right) \\
&\qquad\qquad\quad = 4\left(k^2 - l^2 - l\right) - 1 \\
&\qquad\qquad\quad = 4m + 3 \;\text{ where }\; m = k^2 - l^2 - l - 1 \in \mathbb{Z}
\end{aligned}$$

So, here, 4 divides $a^2 - b^2$ with 3 remainder. So the proposition is proven as we have proven all the possible cases.
There is also another approach given in the Cambridge University Discrete Mathematics lecture notes, TODO

Absolute Value (tags: number theory, absolute value)

$$|x| \geq x, |y| \geq y \implies |x| + |y| \geq x + y$$

$$|x+y| = \begin{cases} |x| + |y| & x, y \geq 0 \\ |-|x| + |y|| & x < 0, y \geq 0 \\ ||x| - |y|| & x \geq 0, y < 0 \\ |-(|x| + |y|)| & x, y < 0 \end{cases} \iff \begin{cases} ||x| + |y|| & x, y \geq 0 \text{ or } x, y < 0) \\ ||x| - |y|| & x < 0, y \geq 0 \text{ or } x \geq 0, y < 0 \end{cases}$$

Clearly, $||x| + |y|| \geq ||x| - |y||$ so that,

$$|x + y| \leq ||x| + |y|| = |x| + |y|$$

and this is known as the "triangle inequality".

Proposition 19. $|x - y| \leq |x - z| + |y - z|$

Proof.

$$|x - y| = |(x - z) + (z - y)| \leq |x - z| + |z - y| = |x - z| + |y - z|$$

□

Proposition 20. $|x-y| \geq ||x|-|y||$

Proof. Need to show $-|x-y| \leq |x| - |y| \leq |x-y|$. So, prove as two separate inequalities:

$$\begin{aligned} & |y| = |x+(y-x)| \leq |x| + |y-x| \\ \iff \quad & -|y-x| = -|x-y| \leq |x| - |y| \end{aligned}$$

$$\begin{aligned} & |x| = |(x-y)+y| \leq |x-y| + |y| \\ \iff \quad & |x| - |y| \leq |x-y| \end{aligned}$$

□

Complex Number (tags: number theory, complex numbers)

Definition. *The **modulus** of a complex number, $z = a + bi$, is the quantity defined as,*

$$|z| = \sqrt{a^2 + b^2}.$$

TODO: modulus is also called "absolute value" and can be calculated as product with conjugate The modulus obeys the following properties:

- $|z_1 z_2| = |z_1|\,|z_2|$

Vector Spaces (tags: vector spaces, polynomials, periodic functions)

Vector Space properties (tags: vector spaces, polynomials)

Definition of a Vector Space (tags: vector spaces)

A field F is a subfield of $\mathbb{C}$ if the following properties hold:

- If $a, b \in F$, then $a + b \in F$.
- If $a \in F$, then $-a \in F$.
- If $a, b \in F$, then $ab \in F$.
- If $a \in F$ and $a \neq 0$, then $a^{-1} \in F$.
- $1 \in F$.

Note that using the first, second and last of these axioms we can deduce that $1 - 1 = 0$ is an element of F.

Let F denote a field which is a subfield of $\mathbb{C}$ and V denote a vector space over F.

Definition. ***Addition, Scalar Multiplication***

- *An **addition** on a set V is a function that assigns an element $u+v \in V$ to each pair of elements $u, v \in V$.*
- *A **scalar multiplication** on a set V is a function that assigns an element $\lambda v \in V$ to each $\lambda \in F$ and each $v \in V$.*

Note that both functions are closed over V.

Definition. ***A vector space** is a set V along with an addition on V and a scalar multiplication on V such that the following properties hold:*

commutativity $\vec{\boldsymbol{u}}+\vec{\boldsymbol{v}}=\vec{\boldsymbol{v}}+\vec{\boldsymbol{u}}$ *for all* $\vec{\boldsymbol{u}},\vec{\boldsymbol{v}}\in V$*;*

associativity $(\vec{\boldsymbol{u}}+\vec{\boldsymbol{v}})+\vec{\boldsymbol{w}}=\vec{\boldsymbol{u}}+(\vec{\boldsymbol{v}}+\vec{\boldsymbol{w}})$ *and* $(ab)\vec{\boldsymbol{v}}=a(b\vec{\boldsymbol{v}})$ *for all* $\vec{\boldsymbol{u}},\vec{\boldsymbol{v}},\vec{\boldsymbol{w}}\in V$ *and all* $a,b\in F$*;*

additive identity *there exists an element* $\vec{\mathbf{0}}\in V$ *such that* $\vec{\boldsymbol{v}}+\vec{\mathbf{0}}=\vec{\boldsymbol{v}}$ *for all* $\vec{\boldsymbol{v}}\in V$*;*

additive inverse *for every* $\vec{\boldsymbol{v}}\in V$ *there exists* $\vec{\boldsymbol{w}}\in V$ *such that* $\vec{\boldsymbol{v}}+\vec{\boldsymbol{w}}=\vec{\mathbf{0}}$*;*

multiplicative identity $1\vec{\boldsymbol{v}}=\vec{\boldsymbol{v}}$ *for all* $\vec{\boldsymbol{v}}\in V$*;*

distributive properties $a(\vec{\boldsymbol{u}}+\vec{\boldsymbol{v}})=a\vec{\boldsymbol{u}}+a\vec{\boldsymbol{v}}$ *and* $(a+b)\vec{\boldsymbol{u}}=a\vec{\boldsymbol{u}}+b\vec{\boldsymbol{u}}$ *for all* $a,b\in F$ *and* $\vec{\boldsymbol{u}},\vec{\boldsymbol{v}}\in V$*;*

Derived properties of a Vector Space (tags: vector spaces)

Proposition 21. *A vector space contains a unique additive identity element.*

Proof. If $\vec{\mathbf{0}'}$ is also an additive identity then by the additive identity property,

$$\vec{\mathbf{0}}+\vec{\mathbf{0}'}=\vec{\mathbf{0}}$$

but since $\vec{\mathbf{0}}$ is also an additive identity,

$$\vec{\mathbf{0}'}+\vec{\mathbf{0}}=\vec{\mathbf{0}'}$$

Then, by the commutativity of vector addition,

$$\vec{\mathbf{0}}=\vec{\mathbf{0}}+\vec{\mathbf{0}'}=\vec{\mathbf{0}'}+\vec{\mathbf{0}}=\vec{\mathbf{0}'}$$ □

Proposition 22. *A vector space contains a unique additive inverse for each element.*

Proof. If $\vec{\boldsymbol{v}}$ and $\vec{\boldsymbol{w}}$ are both additive inverses of $\vec{\boldsymbol{u}}$ then, by the additive inverse property we have,

$$\vec{\boldsymbol{u}} + \vec{\boldsymbol{v}} = \vec{\boldsymbol{0}} \text{ and also } \vec{\boldsymbol{u}} + \vec{\boldsymbol{w}} = \vec{\boldsymbol{0}}$$

using the uniqueness of the additive identity,

$$\vec{\boldsymbol{u}} + \vec{\boldsymbol{v}} = \vec{\boldsymbol{0}} = \vec{\boldsymbol{u}} + \vec{\boldsymbol{w}}$$

Then, if we add one of the additive inverses of $\vec{\boldsymbol{u}}$ to both sides,

$$\vec{\boldsymbol{u}} + \vec{\boldsymbol{v}} + \vec{\boldsymbol{v}} = \vec{\boldsymbol{u}} + \vec{\boldsymbol{w}} + \vec{\boldsymbol{v}}$$

and use the associativity of vector addition,

$$\begin{aligned} (\vec{\boldsymbol{u}} + \vec{\boldsymbol{v}}) + \vec{\boldsymbol{v}} &= (\vec{\boldsymbol{u}} + \vec{\boldsymbol{v}}) + \vec{\boldsymbol{w}} \\ \vec{\boldsymbol{0}} + \vec{\boldsymbol{v}} &= \vec{\boldsymbol{0}} + \vec{\boldsymbol{w}} \\ \vec{\boldsymbol{v}} &= \vec{\boldsymbol{w}} \end{aligned}$$

□

Because additive inverses are unique we can use the notation $-\vec{\boldsymbol{v}}$ to denote the additive inverse of $\vec{\boldsymbol{v}}$. Then we define $\vec{\boldsymbol{w}} - \vec{\boldsymbol{v}}$ to mean $\vec{\boldsymbol{w}} + -\vec{\boldsymbol{v}}$.

Definition. *Vector Subtraction*

$$\vec{\boldsymbol{u}} - \vec{\boldsymbol{v}} := \vec{\boldsymbol{u}} + -\vec{\boldsymbol{v}}$$

Proposition 23. $0\vec{\boldsymbol{v}} = \vec{\boldsymbol{0}}$ *for every* $\vec{\boldsymbol{v}} \in V$.

Note that this proposition is asserting something about scalar multiplication and the additive identity of V. The only part of the definition of a vector space that connects scalar multiplication and vector addition is the distributive property. Therefore the distributive property must be used in this proof.

Proof. Firstly take,

$$\vec{\boldsymbol{v}} + 0\vec{\boldsymbol{v}} = 0\vec{\boldsymbol{v}} + 1\vec{\boldsymbol{v}}$$

and then use the properties of the underlying field to say

$$(0+1)\vec{\boldsymbol{v}} = 1\vec{\boldsymbol{v}} = \vec{\boldsymbol{v}}$$

Now we have shown that,

$$\vec{\boldsymbol{v}} + 0\vec{\boldsymbol{v}} = \vec{\boldsymbol{v}}$$

which, by the definition and uniqueness of the additive identity, shows that $0\vec{\boldsymbol{v}} = \vec{\mathbf{0}}$. But if we want to continue algebraically we can now add the additive inverse to both sides,

$$\begin{aligned}(\vec{\boldsymbol{v}} + -\vec{\boldsymbol{v}}) + 0\vec{\boldsymbol{v}} &= (\vec{\boldsymbol{v}} + -\vec{\boldsymbol{v}}) \\ \vec{\mathbf{0}} + 0\vec{\boldsymbol{v}} = 0\vec{\boldsymbol{v}} &= \vec{\mathbf{0}}\end{aligned}$$

□

Another, simpler proof exists.

Proof. Using the underlying field properties and the distributivity of scalar vector multiplication,

$$0\vec{\boldsymbol{v}} = (0+0)\vec{\boldsymbol{v}} = 0\vec{\boldsymbol{v}} + 0\vec{\boldsymbol{v}}$$

and then adding the additive inverse to both sides,

$$\begin{aligned}(0\vec{\boldsymbol{v}} + -(0\vec{\boldsymbol{v}})) &= (0\vec{\boldsymbol{v}} + -(0\vec{\boldsymbol{v}})) + 0\vec{\boldsymbol{v}} \\ \vec{\mathbf{0}} &= \vec{\mathbf{0}} + 0\vec{\boldsymbol{v}} = 0\vec{\boldsymbol{v}}\end{aligned}$$

□

Proposition 24. $a\vec{\mathbf{0}} = \vec{\mathbf{0}}$ *for every* $a \in F$*.*

Proof. Using the distributivity of scalar multiplication of vectors and the additive identity,

$$a\vec{\mathbf{0}} = a(\vec{\mathbf{0}} + \vec{\mathbf{0}}) = a\vec{\mathbf{0}} + a\vec{\mathbf{0}}$$

Then, adding the additive inverse to both sides,

$$\begin{aligned}(a\vec{\mathbf{0}} + -(a\vec{\mathbf{0}})) &= a\vec{\mathbf{0}} + (a\vec{\mathbf{0}} + -(a\vec{\mathbf{0}})) \\ \vec{\mathbf{0}} &= a\vec{\mathbf{0}} + \vec{\mathbf{0}} = a\vec{\mathbf{0}}\end{aligned}$$

□

Proposition 25. $(-1)\vec{\boldsymbol{v}} = -\vec{\boldsymbol{v}}$ *for every* $\vec{\boldsymbol{v}} \in V$*.*

Proof. Using the distributivity of scalar multiplication of vectors and the underlying field properties we have,

$$(-1)\vec{\boldsymbol{v}} + \vec{\boldsymbol{v}} = (-1)\vec{\boldsymbol{v}} + 1\vec{\boldsymbol{v}} = (-1+1)\vec{\boldsymbol{v}} = 0\vec{\boldsymbol{v}} = \vec{\mathbf{0}}$$

Now we could add the additive inverse to both sides to show that,

$$\begin{aligned}(-1)\vec{\boldsymbol{v}} + (\vec{\boldsymbol{v}} + -\vec{\boldsymbol{v}}) &= \vec{\mathbf{0}} + -\vec{\boldsymbol{v}} \\ (-1)\vec{\boldsymbol{v}} + \vec{\mathbf{0}} &= \vec{\mathbf{0}} + -\vec{\boldsymbol{v}} \\ (-1)\vec{\boldsymbol{v}} &= \vec{\boldsymbol{v}}\end{aligned}$$

□

But we already have,

$$(-1)\vec{\boldsymbol{v}} + \vec{\boldsymbol{v}} = \vec{\mathbf{0}}$$

and this, by the definition of the additive inverse, proves that $(-1)\vec{\boldsymbol{v}}$ is an additive inverse of $\vec{\boldsymbol{v}}$. Since we have previously proven the uniqueness of the additive inverse in Proposition 22 we can conclude, in fact, that $(-1)\vec{\boldsymbol{v}} = -\vec{\boldsymbol{v}}$ the unique additive inverse of v.

The notation F^S (tags: vector spaces)

If S is a set then F^S denotes the set of functions $S \mapsto F$.

Addition is defined as, for $f, g, (f+g) \in F^S$,

$$(f+g)(x) = f(x) + g(x)$$

for all $x \in S$.

Scalar multiplication is defined as, for $\lambda \in F, \lambda f \in F^S$,

$$(\lambda f)(x) = \lambda f(x)$$

for all $x \in S$.

Example: If S is the interval $[0,1]$ and $F = \mathbb{R}$ then $\mathbb{R}^{[0,1]}$ is the set of real-valued functions on the interval $[0,1]$. $\mathbb{R}^{[0,1]}$ is a vector space with additive identity $0 : [0,1] \mapsto \mathbb{R}$ defined as $0(x) = 0$ and the additive inverse of some function $f \in \mathbb{R}^{[0,1]}$ is the function defined as $(-f)(x) = -f(x)$.
Any *non-empty* set S in conjunction with a subset of $\mathbb{C}$ would similarly produce a vector space. In fact, the vector space F^n can be thought of as the space of functions from the set $\{1, 2, 3, \ldots, n\}$ to F. For example, vectors in 3-dimensional space can be viewed as:

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv f : \{1,2,3\} \mapsto \mathbb{R} \text{ with } f(t) = \begin{cases} x & t = 1 \\ y & t = 2 \\ z & t = 3 \end{cases}$$

Polynomials as a vector space (tags: vector spaces, polynomials)

A very important example involves treating a polynomial as a vector. A function $p : F \mapsto F$ is called a polynomial with coefficients in F if there exist $a_0, \dots, a_m \in F$ such that,

$$p(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m$$

for all $z \in F$.
Then we can define a vector space, $P(F)$, to be the set of all polynomials with coefficients in F.

Addition on $P(F)$ is defined as,

$$(p+q)(z) = p(z) + q(z) \qquad \text{for } p, q \in P(F), z \in F$$

whose associativity is clear from the definition and the commutativity can be shown by,

$$\begin{aligned}((p+q)+r)(z) &= (p+q)(z) + r(z)\\ &= p(z) + q(z) + r(z)\\ &= p(z) + (q+r)(z)\\ &= (p + (q+r))(z)\end{aligned}$$

Scalar multiplication on $P(F)$ is defined as,

$$(ap)(z) = ap(z) \qquad \text{for } p \in P(F), a, z \in F$$

whose associativity can be shown by substituting (ab) for a in the definition,

$$[(ab)p](z) = (ab)p(z)$$

Then, by the associativity of the multiplication of the elements of the field F we have,

$$(ab)p(z) = a[b(p(z)]$$

then we use the definition in reverse,

$$a[b(p(z)]) = a[(bp)(z)] = [a(bp)](z)$$

(compare with $(ab)\vec{\boldsymbol{v}} = a(b\vec{\boldsymbol{v}})$)

modeling Concretely, each $p(z) \in P(F)$ is a vector that could be modeled, say, as

$$\vec{\boldsymbol{p}} = \{\, (a_0, a_1, \ldots, a_m) \mid p(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m \in P(F) \,\}$$

Subspaces of vector spaces **(tags: vector spaces, polynomials, periodic functions)**

Definition of a Subspace **(tags: vector spaces)**

Definition. *A set U is a subspace of V if it is a subset of V and if the same addition and multiplication over U forms a vector space.*

Considering the required properties of a vector space, we can see that commutativity and associativity of the addition; associativity of the scalar multiplication; and distributivity of the scalar multiplication over the addition; will all be satisfied as we have the same addition and multiplication over a subset of the elements in V. That's to say, the vector space properties ensure that these properties hold $\forall \vec{\boldsymbol{v}} \in V$ and we have $\forall \vec{\boldsymbol{u}} \in U, \vec{\boldsymbol{u}} \in V$.
Furthermore, the multiplicative identity also holds $\forall \vec{\boldsymbol{v}} \in V$ so will also hold for every element of U.

So what remains to be proven to satisfy the requirements of a subspace?

- Existence of the additive identity
- Existence of an additive inverse for every element of U
- Closure of the addition and scalar multiplication over U

Note, however that - having proved in Proposition 25 that multiplication by -1 gives the additive inverse - closure of the scalar multiplication over U also implies the presence in U of the additive inverse of every element of U. So, actually, what we need to prove for U to be a subspace is only,

- $\vec{\mathbf{0}} \in U$
- Closure of the addition and scalar multiplication over U

A subspace of the polynomials (tags: vector spaces, polynomials)

An example of a subspace of the polynomials, $P(F)$ is,

$$\{\, p \in P(F) \mid p(3) = 0 \,\}$$

Members of this subspace include:

- $p(z) = 3 - z$
- $p(z) = 9 - z^2$
- $p(z) = 3 - z + 3z^2 - z^3$
- $p(z) = 12z - 4z^2$
- …etc.

To verify this we need to show that addition and multiplication are closed over this set and that $\vec{\mathbf{0}}$ is a member of the set. It's easy to see that $\vec{\mathbf{0}}$ is a member of the set as,

$$p(3) = 0 + 0(3) + 0(3)^2 + \cdots + 0(3)^m = 0$$

as required. Scalar multiplication is closed as,

$$ap(3) = a(0) = 0$$

whereas addition can be shown to be closed as,

$$(q + r)(3) = q(3) + r(3) = 0 + 0 = 0$$

Note that for values of $z \neq 3$, the closure of these functions is the same as for the general case of $P(F)$.

Sums and Direct Sums (tags: vector spaces)

Definition. *If $U_1, U_2, \dots, U_m$ are subspaces of V then their sum is defined as*

$$U_1+U_2+\cdots+U_m = \{\, \vec{\boldsymbol{u_1}} + \vec{\boldsymbol{u_2}} + \cdots + \vec{\boldsymbol{u_m}} \mid \vec{\boldsymbol{u_1}} \in U_1, \vec{\boldsymbol{u_2}} \in U_2, \dots, \vec{\boldsymbol{u_m}} \in U_m \,\}$$

The sum of the subspaces of V is also a subspace of V because,

- Closure of addition

$$\begin{aligned} &(\vec{\boldsymbol{u_1}} + \vec{\boldsymbol{u_2}} + \cdots + \vec{\boldsymbol{u_m}}) + (\vec{\boldsymbol{u'_1}} + \vec{\boldsymbol{u'_2}} + \cdots + \vec{\boldsymbol{u'_m}}) \\ =& (\vec{\boldsymbol{u_1}} + \vec{\boldsymbol{u'_1}}) + (\vec{\boldsymbol{u_2}} + \vec{\boldsymbol{u'_2}}) + \cdots + (\vec{\boldsymbol{u_m}} + \vec{\boldsymbol{u'_m}}) \\ =& \vec{\boldsymbol{v_1}} + \vec{\boldsymbol{v_2}} + \cdots + \vec{\boldsymbol{v_m}} \qquad \text{where } \vec{\boldsymbol{v_1}} \in U_1, \vec{\boldsymbol{v_2}} \in U_2, \dots, \vec{\boldsymbol{v_m}} \in U_m \end{aligned}$$

- Closure of scalar multiplication

$$\begin{aligned} &a(\vec{\boldsymbol{u_1}} + \vec{\boldsymbol{u_2}} + \cdots + \vec{\boldsymbol{u_m}}) \qquad \text{where } a \in F \\ =& a\vec{\boldsymbol{u_1}} + a\vec{\boldsymbol{u_2}} + \cdots + a\vec{\boldsymbol{u_m}} \\ =& \vec{\boldsymbol{v_1}} + \vec{\boldsymbol{v_2}} + \cdots + \vec{\boldsymbol{v_m}} \qquad \text{where } \vec{\boldsymbol{v_1}} \in U_1, \vec{\boldsymbol{v_2}} \in U_2, \dots, \vec{\boldsymbol{v_m}} \in U_m \end{aligned}$$

- Existence of $\vec{\mathbf{0}}$

$$\begin{aligned} & U_1, U_2, \dots, U_m \text{ are subspaces} \\ \implies & \vec{\mathbf{0}} \in U_1, \vec{\mathbf{0}} \in U_2, \dots, \vec{\mathbf{0}} \in U_m \\ \implies & \vec{\mathbf{0}} + \vec{\mathbf{0}} + \cdots + \vec{\mathbf{0}} \in U_1 + U_2 + \cdots + U_m \end{aligned}$$

  Note though, that this may not be the only way of producing $\vec{\mathbf{0}}$ from the sum of vectors of these subspaces. That's to say, there could be some $(\vec{\boldsymbol{u_1}} + \vec{\boldsymbol{u_2}} + \cdots + \vec{\boldsymbol{u_m}}) = \vec{\mathbf{0}}$ and this is a key difference from direct sums.

Proposition 26. *$U_1+U_2+\cdots+U_m$ is the smallest subspace of V containing $U_1, U_2, \dots, U_m$.*

Proof. $U_1+U_2+\cdots+U_m$ is a subspace of V that contains $U_1, U_2, \ldots, U_m$ because we can obtain U_i by setting all the u_j for $j \neq i$ to $\vec{\mathbf{0}}$.

If a subspace of V contains $U_1, U_2, \ldots, U_m$ then, by the closure of addition, it must also contain $U_1 + U_2 + \cdots + U_m$.

Therefore the smallest subspace of V that contains $U_1, U_2, \ldots, U_m$ is $U_1 + U_2 + \cdots + U_m$. □

Definition. *If $U_1, U_2, \ldots, U_m$ are subspaces of V then their **direct sum** is defined as,*

$$U_1 \oplus U_2 \oplus \cdots \oplus U_m = \{\, \vec{\boldsymbol{u_1}} + \vec{\boldsymbol{u_2}} + \cdots + \vec{\boldsymbol{u_m}} \mid \vec{\boldsymbol{u_1}} \in U_1, \vec{\boldsymbol{u_2}} \in U_2, \ldots, \vec{\boldsymbol{u_m}} \in U_m \,\}$$

such that,

$$\vec{\boldsymbol{u_1}} + \vec{\boldsymbol{u_2}} + \cdots + \vec{\boldsymbol{u_m}} = \vec{\mathbf{0}} \implies \vec{\boldsymbol{u_1}} = \vec{\mathbf{0}}, \vec{\boldsymbol{u_2}} = \vec{\mathbf{0}}, \ldots, \vec{\boldsymbol{u_m}} = \vec{\mathbf{0}}.$$

That the unique way of obtaining $\vec{\mathbf{0}}$ is for all of the vectors from each of the subspaces to be $\vec{\mathbf{0}}$ is equivalent to there only being a single unique way of obtaining each resultant vector from an addition of the vectors from the individual subspaces. This can be seen as,

$$\begin{aligned} \vec{\boldsymbol{u_1}} + \vec{\boldsymbol{u_2}} + \cdots + \vec{\boldsymbol{u_m}} &= \vec{\boldsymbol{u_1'}} + \vec{\boldsymbol{u_2'}} + \cdots + \vec{\boldsymbol{u_m'}} \\ (\vec{\boldsymbol{u_1}} + \vec{\boldsymbol{u_2}} + \cdots + \vec{\boldsymbol{u_m}}) - (\vec{\boldsymbol{u_1'}} + \vec{\boldsymbol{u_2'}} + \cdots + \vec{\boldsymbol{u_m'}}) &= \vec{\mathbf{0}} \\ (\vec{\boldsymbol{u_1}} - \vec{\boldsymbol{u_1'}}) + (\vec{\boldsymbol{u_2}} - \vec{\boldsymbol{u_2'}}) + \cdots + (\vec{\boldsymbol{u_m}} - \vec{\boldsymbol{u_m'}}) &= \vec{\mathbf{0}} \end{aligned}$$

Therefore, since vector spaces always contain $\vec{\mathbf{0}}$ and so we will always have the representation,

$$\vec{\mathbf{0}} + \vec{\mathbf{0}} + \cdots + \vec{\mathbf{0}} = \vec{\mathbf{0}}$$

if this is the unique representation of $\vec{\mathbf{0}}$ then it follows that,

$$\begin{aligned} (\vec{\boldsymbol{u_1}} - \vec{\boldsymbol{u_1'}}) = \vec{\mathbf{0}}, (\vec{\boldsymbol{u_2}} - \vec{\boldsymbol{u_2'}}) = \vec{\mathbf{0}}, \ldots, (\vec{\boldsymbol{u_m}} - \vec{\boldsymbol{u_m'}}) = \vec{\mathbf{0}} \\ \implies \vec{\boldsymbol{u_1}} = \vec{\boldsymbol{u_1'}}, \vec{\boldsymbol{u_2}} = \vec{\boldsymbol{u_2'}}, \ldots, \vec{\boldsymbol{u_m}} = \vec{\boldsymbol{u_m'}} \end{aligned}$$

which means that these are the same representation. And this clearly holds in reverse also as, if there is a single way of representing each resultant vector then there must be a single way of representing $\vec{\mathbf{0}}$ and due to the definition of a vector space we must always have the representation of all $\vec{\mathbf{0}}$. Therefore, this is the only representation of $\vec{\mathbf{0}}$.

Note that this is a condition on the contents of the subspaces and not on the way that the addition is performed. So, the difference between vector space sum $(U_1 + U_2)$ and vector space direct sum $(U_1 \oplus U_2)$ is not in the operator itself but in the operands they operate over.

For two subspaces, say, U_1, U_2 this condition on the subspaces reduces to the requirement that $U_1 \cap U_2 = \{\vec{\mathbf{0}}\}$ which can be seen as,

$$\begin{aligned} \vec{\boldsymbol{u_1}} + \vec{\boldsymbol{u_2}} &= \vec{\mathbf{0}} \\ \vec{\boldsymbol{u_1}} + -\vec{\boldsymbol{u}}_{\mathbf{1}} + \vec{\boldsymbol{u_2}} &= \vec{\mathbf{0}} + -\vec{\boldsymbol{u}}_{\mathbf{1}} \\ \vec{\boldsymbol{u_2}} &= -\vec{\boldsymbol{u}}_{\mathbf{1}} \\ \implies -\vec{\boldsymbol{u}}_{\mathbf{1}} \in U_2 &\implies \vec{\boldsymbol{u_1}} \in U_2 \end{aligned}$$

So, for two subspaces, obtaining $\vec{\mathbf{0}}$ as the sum of vectors from the subspaces implies a vector in common between them. So, for $\vec{\mathbf{0}} + \vec{\mathbf{0}}$ to be the only way of obtaining $\vec{\mathbf{0}}$ implies that $\vec{\mathbf{0}}$ is the only vector in common.

However, for more than two subspaces, say U_1, U_2, U_3, the situation is different as we could have,

$$\begin{aligned} \vec{\boldsymbol{u_1}} + \vec{\boldsymbol{u_2}} + \vec{\boldsymbol{u_3}} &= \vec{\mathbf{0}} \\ \iff \vec{\boldsymbol{u_1}} + -\vec{\boldsymbol{u}}_{\mathbf{1}} + \vec{\boldsymbol{u_2}} + -\vec{\boldsymbol{u}}_{\mathbf{2}} + \vec{\boldsymbol{u_3}} &= \vec{\mathbf{0}} + -\vec{\boldsymbol{u}}_{\mathbf{1}} + -\vec{\boldsymbol{u}}_{\mathbf{2}} \\ \iff \vec{\boldsymbol{u_3}} &= -\vec{\boldsymbol{u}}_{\mathbf{1}} + -\vec{\boldsymbol{u}}_{\mathbf{2}} \end{aligned}$$

which does not imply any vectors held in common.

Vector Space Problems (tags: vector problems)

Prove that $-(-\vec{\boldsymbol{v}}) = \vec{\boldsymbol{v}}$ for every $\vec{\boldsymbol{v}} \in V$ (tags: vector problems)

$$\begin{aligned} -(-\vec{\boldsymbol{v}}) &= -[(-1)\vec{\boldsymbol{v}}] && \text{using Proposition 25} \\ &= (-1)[(-1)\vec{\boldsymbol{v}}] && \text{using Proposition 25 again} \\ &= [(-1)(-1)]\vec{\boldsymbol{v}} && \text{using associativity of scalar multiplication} \\ &= \vec{\boldsymbol{v}} && \text{using field properties} \end{aligned}$$

Or, a quicker way is,

$$\begin{aligned} -\vec{\boldsymbol{v}} + -(-\vec{\boldsymbol{v}}) &= \vec{\mathbf{0}} && \text{using additive identity of } -\vec{\boldsymbol{v}} \\ (-\vec{\boldsymbol{v}} + \vec{\boldsymbol{v}}) + -(-\vec{\boldsymbol{v}}) &= \vec{\mathbf{0}} + \vec{\boldsymbol{v}} && \text{adding } \vec{\boldsymbol{v}} \text{ to both sides} \\ -(-\vec{\boldsymbol{v}}) &= \vec{\boldsymbol{v}} \end{aligned}$$

Prove that if $a \in F, \vec{\boldsymbol{v}} \in V$, and $a\vec{\boldsymbol{v}} = \vec{\mathbf{0}}$, then $a = 0$ or $\vec{\boldsymbol{v}} = \vec{\mathbf{0}}$. (tags: vector problems)

We follow a proof by cases.

Case $a \neq 0$:

$$\begin{aligned} a\vec{\boldsymbol{v}} = \vec{\mathbf{0}}, a \neq 0 \implies a^{-1}a\vec{\boldsymbol{v}} &= a^{-1}\vec{\mathbf{0}} && \text{using field properties} \\ \iff 1\vec{\boldsymbol{v}} &= b\vec{\mathbf{0}} && \text{where } b = a^{-1} \in F \\ \iff \vec{\boldsymbol{v}} &= \vec{\mathbf{0}} && \text{using Proposition 24 and multiplicative identity} \end{aligned}$$

Case $\vec{\boldsymbol{v}} \neq \vec{\mathbf{0}}$:

$$\begin{aligned} a\vec{\boldsymbol{v}} = \vec{\mathbf{0}}, \vec{\boldsymbol{v}} \neq \vec{\mathbf{0}} &\implies a\vec{\boldsymbol{v}} = a\vec{\boldsymbol{v}} + -a\vec{\boldsymbol{v}} \\ &\iff a\vec{\boldsymbol{v}} = (a + -a)\vec{\boldsymbol{v}} = 0\vec{\boldsymbol{v}} && \text{using field properties} \\ \text{Wrong! } a\vec{\boldsymbol{v}} = \vec{\mathbf{0}} &\implies a\vec{\boldsymbol{v}} = a\vec{\boldsymbol{v}} + -a\vec{\boldsymbol{v}} \\ &\text{without need for } \vec{\boldsymbol{v}} \neq \vec{\mathbf{0}} \end{aligned}$$

This indicates that you are proving something that doesn't need proving. In actual fact,

Case $a = 0$: Actually, in this case there is nothing to be proven as we know from Proposition 23 that $0\vec{\boldsymbol{v}} = \vec{\mathbf{0}}$. So we have collectively exhaustive cases by looking at $a = 0$ and $a \neq 0$ and we only need to show that $a \neq 0 \implies \vec{\boldsymbol{v}} = \vec{\mathbf{0}}$ which we have already done.

Give an example of a nonempty subset U of $\mathbb{R}^2$ such that U is closed under scalar multiplication but U is not a subspace of $\mathbb{R}^2$. **(tags: vector problems)**

For all $\lambda \in \mathbb{R}$ the set $\{\, \lambda\vec{\boldsymbol{v}} \mid \vec{\boldsymbol{v}} \in \{(1,1)(-1,1)\}\,\}$ is closed under scalar multiplication but not addition.

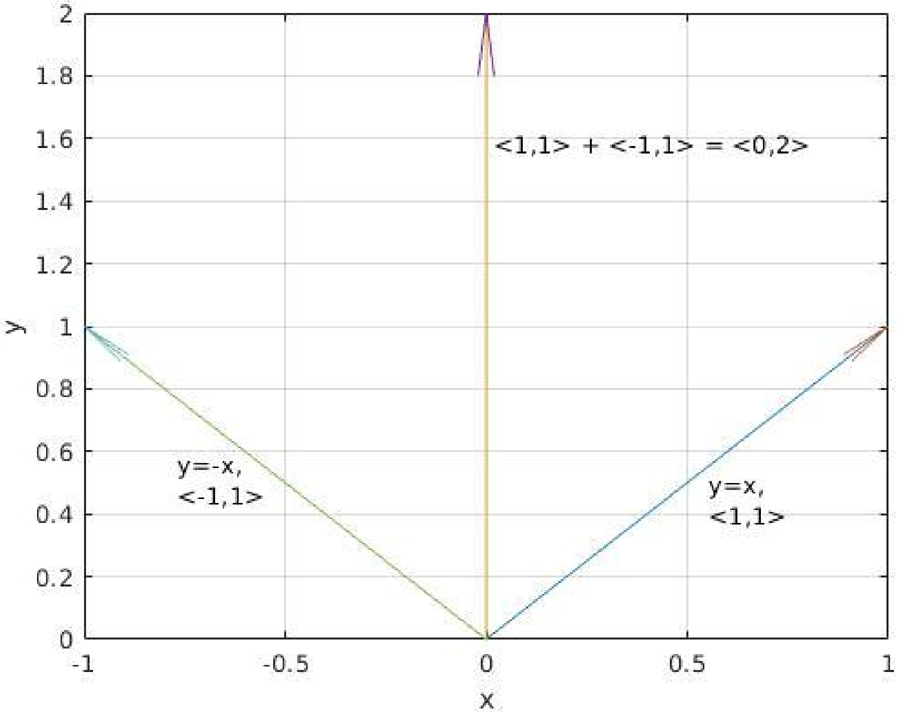


Figure 2: The blue arrows are vectors whose scalar multiples will all be in the same line as the blue arrows but the red arrow shows what happens if we add them; the result lies outside of both lines.

Is $\mathbb{R}^2$ a subspace of the complex vector space $\mathbb{C}^2$? **(tags: vector problems)**

The definition of a subspace of $\mathbb{C}^2$ is a set of vectors which is a subset of those in $\mathbb{C}^2$ and that forms a vector space under the same addition and scalar multiplication of $\mathbb{C}^2$. The scalar multiplication of the vector space $\mathbb{C}^2$ is multiplication by scalars $\lambda \in \mathbb{C}$.

For a vector, $\vec{\boldsymbol{v}} \in \mathbb{R}^2$, scaling it by a complex number, $\lambda\vec{\boldsymbol{v}}$ will result in a vector that is not necessarily in $\mathbb{R}^2$.

Is $\{\, (a, b, c) \in \mathbb{C}^3 \;|\; a^3 = b^3 \,\}$ a subspace of $\mathbb{C}^3$? **(tags: vector problems)**

For $x \in \mathbb{C}$, x^3 has roots, $1, \frac{-1+\sqrt{3}i}{2}, \frac{-1-\sqrt{3}i}{2}$ so we don't have $a = b$ as we would if we were ranging over the reals.
Concretely, we can have, $(1, \frac{-1+\sqrt{3}i}{2}, 0)$ and $(1, \frac{-1-\sqrt{3}i}{2}, 0)$ but,

$$(1, \frac{-1+\sqrt{3}i}{2}, 0) + (1, \frac{-1-\sqrt{3}i}{2}, 0) = (2, -1, 0)$$

where $(2, -1, 0) \notin \{\, (a, b, c) \in \mathbb{C}^3 \;|\; a^3 = b^3 \,\}$ meaning that addition over this set is not closed. Therefore, this is not a subspace.

Give an example of a non-empty subset U of $\mathbb{R}^2$ such that U is closed under addition and under taking additive inverses (meaning $-\vec{\boldsymbol{u}} \in U$ whenever $\vec{\boldsymbol{u}} \in U$), but U is not a subspace of $\mathbb{R}^2$. **(tags: vector problems)**

First thought might be $\mathbb{R}^2 - \{\vec{\boldsymbol{0}}\}$ but this is Wrong!. If the subset is closed under addition and under taking additive inverses then it means that $\vec{\boldsymbol{u}} + -\vec{\boldsymbol{u}} = \vec{\boldsymbol{0}} \in U$ and so the set $\mathbb{R}^2 - \{\vec{\boldsymbol{0}}\}$ is not closed under addition and taking additive inverses.
The set $\{\, (x, y) \in \mathbb{R}^2 \;|\; x, y \in \mathbb{Z} \,\}$ however, is closed under addition because integer addition is closed and under taking additive inverses but scalar multiplication where the scalars range over the reals, will produce non-integer values for x and y.

Is the set of periodic functions over the reals a subspace of $\mathbb{R}^R$? **(tags: vector problems, periodic functions)**

The definition of two periodic functions over the reals is

$$\exists p > 0 \in \mathbb{R} \cdot f(x) = f(x + p)$$
$$\exists q > 0 \in \mathbb{R} \cdot g(x) = g(x + q)$$

Then for their sum to be periodic we need,

$$\exists \alpha, \beta \in \mathbb{Z}, m \in \mathbb{R} \cdot (m = \alpha p) \wedge (m = \beta q)$$

$$\iff \frac{q}{p} = \frac{\alpha}{\beta} \in \mathbb{Q}$$

$$\therefore (f+g)(x) = (f+g)(x+m) = f(x+m) + g(x+m)$$

$$\iff \frac{q}{p} \in \mathbb{Q}.$$

Prove that the union of two subspaces of V is a subspace of V if and only if one of the subspaces is contained within the other. (tags: vector problems)

Let A, B be subspaces of V and $\vec{\boldsymbol{a}} \in A$, $\vec{\boldsymbol{b}} \in B$ and,

$$C = A \cup B = \{\, \vec{\boldsymbol{c}} \mid \vec{\boldsymbol{c}} \in A \ \vee \ \vec{\boldsymbol{c}} \in B \,\}.$$

Since $\vec{\boldsymbol{a}}, \vec{\boldsymbol{b}} \in C$ we have (C subspace of V) $\iff \forall \alpha, \beta \in F \cdot (\alpha\vec{\boldsymbol{a}} + \beta\vec{\boldsymbol{b}}) \in C$. Then,

$$\begin{aligned} \vec{\boldsymbol{b}} \in A &\implies \forall \alpha, \beta \in F \cdot (\alpha\vec{\boldsymbol{a}} + \beta\vec{\boldsymbol{b}}) \in A \text{ (by subspace properties)} \\ &\implies (\alpha\vec{\boldsymbol{a}} + \beta\vec{\boldsymbol{b}}) \in C. \end{aligned}$$

A similar argument holds for $\vec{\boldsymbol{a}} \in B$. Conversely,

$$\begin{aligned} \forall \alpha, \beta \in F \cdot (\alpha\vec{\boldsymbol{a}} + \beta\vec{\boldsymbol{b}}) \in C &\implies ((\alpha\vec{\boldsymbol{a}} + \beta\vec{\boldsymbol{b}}) \in A) \vee ((\alpha\vec{\boldsymbol{a}} + \beta\vec{\boldsymbol{b}}) \in B) \\ &\implies ((\alpha\vec{\boldsymbol{a}} - \alpha\vec{\boldsymbol{a}} + \beta\vec{\boldsymbol{b}}) = \beta\vec{\boldsymbol{b}} \in A) \vee ((\alpha\vec{\boldsymbol{a}} + \beta\vec{\boldsymbol{b}} - \beta\vec{\boldsymbol{b}}) = \alpha\vec{\boldsymbol{a}} \in B) \\ &\implies (\vec{\boldsymbol{b}} \in A) \vee (\vec{\boldsymbol{a}} \in B) \end{aligned}$$

$$\begin{aligned} \therefore \text{(C subspace of V)} &\iff \forall \alpha, \beta \in F \cdot (\alpha\vec{\boldsymbol{a}} + \beta\vec{\boldsymbol{b}}) \in C \\ &\iff (\vec{\boldsymbol{b}} \in A) \vee (\vec{\boldsymbol{a}} \in B) \\ &\equiv (B \subseteq A) \vee (A \subseteq B). \end{aligned}$$

Can a vector space over an infinite field be a finite union of proper subspaces? **(tags: vector problems)**

Assume that our vector space V is a finite union of proper subspaces, hence

$$V = \bigcup_{i=1}^{n} U_i.$$

Now, pick a non-zero vector $\vec{\boldsymbol{x}} \in U_1$, and pick another vector $\vec{\boldsymbol{y}} \in V \backslash U_1$.

There are infinitely many vectors $\vec{\boldsymbol{x}} + k\vec{\boldsymbol{y}}$, where $k \in K^*$ (K is our infinite field). Note that $\vec{\boldsymbol{x}} + k\vec{\boldsymbol{y}}$ is not in U_1, hence must be contained in some U_j where $j \neq 1$.

Then since $k \in K^*$, we can have $\vec{\boldsymbol{x}} + k_1\vec{\boldsymbol{y}}$, $\vec{\boldsymbol{x}} + k_2\vec{\boldsymbol{y}} \in U_j$, which implies that it also contains $\vec{\boldsymbol{y}}$ and hence also $\vec{\boldsymbol{x}}$, hence $U_1 \subset U_j$.

Explanation: There are infinitely many vectors $\vec{\boldsymbol{x}}+k\vec{\boldsymbol{y}}$ and only finitely many U_i so they cannot all be in different U_i so we have,

$$\begin{aligned} \exists\, k_1,\, k_2 \in K^* \cdot \vec{\boldsymbol{x}} + k_1\vec{\boldsymbol{y}},\, \vec{\boldsymbol{x}} + k_2\vec{\boldsymbol{y}} \in U_j \\ \implies (\vec{\boldsymbol{x}} + k_1\vec{\boldsymbol{y}}) - (\vec{\boldsymbol{x}} + k_2\vec{\boldsymbol{y}}) = (k_1 - k_2)\vec{\boldsymbol{y}} \in U_j \\ \implies \vec{\boldsymbol{y}} \in U_j \implies \vec{\boldsymbol{x}} \in U_j \end{aligned}$$

Hence

$$V = \bigcup_{i=2}^{n} U_i.$$

Evidently, this can be continued, hence a contradiction arises.

Prove or give a counterexample: if U_1, U_2, W are subspaces of V such that $V = U_1 \oplus W$ and $V = U_2 \oplus W$ then $U_1 = U_2$. **(tags: vector problems)**

Counter example: $V = \mathbb{F}^2$, $U_1 = \{\, (x, 0) \in \mathbb{F}^2 \mid x \in F \,\}$, $U_2 = \{\, (0, x) \in \mathbb{F}^2 \mid x \in F \,\}$, $W = \{\, (x, x) \in \mathbb{F}^2 \mid x \in F \,\}$.

Let U_e denote the set of real-valued even functions on $\mathbb{R}$ and let U_o denote the set of real-valued odd functions on $\mathbb{R}$. Show that $\mathbb{R}^R = U_e \oplus U_o$. (tags: vector problems)

Every function $f \in \mathbb{R}^R$ can be expressed as the sum of an even function and an odd function as,

$$f(x) = \frac{f(x) + f(-x)}{2} + \frac{f(x) - f(-x)}{2} = g(x) + h(x)$$

where $g(x) \in U_e$ and $h(x) \in U_o$. So, $U_e + U_o$ spans $\mathbb{R}^R$.
Furthermore,

$$\begin{aligned} f(x) \in (U_e \cap U_o) &\implies (f(-x) = f(x)) \wedge (f(-x) = -f(x)) \\ &\implies f(x) = -f(x) \\ &\implies f(x) = 0 \end{aligned}$$

Since $f(x) = 0$ is the additive identity of this space, this shows that the intersection is $\vec{\mathbf{0}}$. So, $\mathbb{R}^R = U_e \oplus U_o$.

Span, Dimension and Bases (tags: vector spaces)

Definition. *The* span *of a list of vectors* $\vec{\boldsymbol{v_1}}, \vec{\boldsymbol{v_2}}, \ldots, \vec{\boldsymbol{v_k}}$ *- written* $\operatorname{span}(\vec{\boldsymbol{v_1}}, \vec{\boldsymbol{v_2}}, \ldots, \vec{\boldsymbol{v_k}})$ *- is defined as*

$$\{\, \alpha_1\vec{\boldsymbol{v_1}} + \alpha_2\vec{\boldsymbol{v_2}} + \cdots + \alpha_k\vec{\boldsymbol{v_k}} \;|\; \alpha_1, \alpha_2, \ldots, \alpha_k \in F \,\}$$

Proposition 27. *The span of a list of vectors is the smallest subspace containing those vectors.*

Note that a vector space over $\mathbb{R}$ or $\mathbb{C}$ is an uncountable set as - while the dimensions of the vector space may be finite - closure under scalar multiplication means that the vectors in the space are continuously valued as the field providing the scalars is continuously valued.
This means that the notion of the *smallest* subspace cannot refer to the

cardinality of the set and must refer to ordering based on subset. So, the smallest subspace containing a list of vectors is a subspace that contains the list of vectors and, of which, there is no proper subset which also contains the list of vectors.

Proof.

$$\begin{aligned}\text{Let } S &:= \mathit{span}(\vec{\boldsymbol{v_1}}, \vec{\boldsymbol{v_2}}, \dots, \vec{\boldsymbol{v_k}})\\ &:= \{\, \alpha_1\vec{\boldsymbol{v_1}} + \alpha_2\vec{\boldsymbol{v_2}} + \dots + \alpha_k\vec{\boldsymbol{v_k}} \mid \alpha_1, \alpha_2, \dots, \alpha_k \in F \,\}\\ \text{and let } V &:= \text{ the smallest vector space containing } \vec{\boldsymbol{v_1}}, \vec{\boldsymbol{v_2}}, \dots, \vec{\boldsymbol{v_k}}.\end{aligned}$$

then S contains every linear combination of $\vec{\boldsymbol{v_1}}, \vec{\boldsymbol{v_2}}, \dots, \vec{\boldsymbol{v_k}}$ and nothing else and so is a vector space containing $\vec{\boldsymbol{v_1}}, \vec{\boldsymbol{v_2}}, \dots, \vec{\boldsymbol{v_k}}$,

$$V \subseteq S$$

Additionally, any vector space containing the vectors $\vec{\boldsymbol{v_1}}, \vec{\boldsymbol{v_2}}, \dots, \vec{\boldsymbol{v_k}}$ must contain all their linear combinations, $\mathit{span}(\vec{\boldsymbol{v_1}}, \vec{\boldsymbol{v_2}}, \dots, \vec{\boldsymbol{v_k}})$,

$$S \subseteq V$$

Therefore there is no proper subset of $\mathit{span}(\vec{\boldsymbol{v_1}}, \vec{\boldsymbol{v_2}}, \dots, \vec{\boldsymbol{v_k}})$ that is also a vector space containing $\vec{\boldsymbol{v_1}}, \vec{\boldsymbol{v_2}}, \dots, \vec{\boldsymbol{v_k}}$, and so $\mathit{span}(\vec{\boldsymbol{v_1}}, \vec{\boldsymbol{v_2}}, \dots, \vec{\boldsymbol{v_k}})$ is the smallest vector space containing $\vec{\boldsymbol{v_1}}, \vec{\boldsymbol{v_2}}, \dots, \vec{\boldsymbol{v_k}}$,

$$(V \subseteq S) \wedge (S \subseteq V) \iff V = S \qquad \square$$

Proposition 28. *Length of every linearly independent list in a space is less than or equal to the length of a spanning list in the same space.*

Proof. Let $U = \vec{\boldsymbol{u_1}}, \vec{\boldsymbol{u_2}}, \dots, \vec{\boldsymbol{u_m}}$ be a linearly independent list of vectors in V and $W = \vec{\boldsymbol{w_1}}, \vec{\boldsymbol{w_2}}, \dots, \vec{\boldsymbol{w_n}}$ be a spanning list of vectors in V.
If we take $\vec{\boldsymbol{u_1}}$ from U and add it to W then - since the other vectors in W are a spanning list - W must be linearly dependent. That's to say,

$$\begin{aligned}\exists\, \alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{R} \cdot \alpha_1\vec{\boldsymbol{w_1}} + \dots + \alpha_n\vec{\boldsymbol{w_n}} &= \vec{\boldsymbol{u_1}}\\ \iff \alpha_1\vec{\boldsymbol{w_1}} + \dots + \alpha_n\vec{\boldsymbol{w_n}} - \vec{\boldsymbol{u_1}} &= -\alpha_i\vec{\boldsymbol{w_i}}\\ \iff \frac{-\alpha_1}{\alpha_i}\vec{\boldsymbol{w_1}} + \dots + \frac{-\alpha_n}{\alpha_i}\vec{\boldsymbol{w_n}} + \frac{1}{\alpha_i}\vec{\boldsymbol{u_1}} &= \vec{\boldsymbol{w_i}}\end{aligned}$$

So, $\vec{\boldsymbol{w_i}}$ is in the span of $\vec{\boldsymbol{u_1}}, \vec{\boldsymbol{w_2}}, \ldots, \vec{\boldsymbol{w_n}}$ and we can drop $\vec{\boldsymbol{w_i}}$ from the list, W, and it will still span the vector space.
We can keep doing this with the remaining vectors in U - each time the vector to be removed will be some $\vec{\boldsymbol{w_i}}$ because all the $\vec{\boldsymbol{u_i}}$ are linearly independent - and all the while W remains a spanning list. We continue until we have replaced (potentially) all n vectors in W, which would happen if $m > n$. At this point we would have the spanning list $W = \vec{\boldsymbol{u_1}}, \vec{\boldsymbol{u_2}}, \ldots, \vec{\boldsymbol{u_n}}$ and $(m - n)$ remaining vectors in U.
Now, since W spans the space, the $(m - n)$ vectors that remain in U will be in the span of W. But, all the vectors that originally came from U were linearly independent, so it is impossible for any vectors in U to be in the span of W (which now comprises only vectors that originally came from U). We therefore conclude that there can be no remaining vectors in U and, consequently that m cannot be greater than n, i.e. $m \leq n$. □

Linear Algebra (tags: linear algebra)

Matrix Algebra (tags: linear algebra)

Basic properties of Matrix Algebra (tags: linear algebra)

Definition. *Matrix **equality** is defined component-wise so that if $A = B$ then A and B must have the same dimension as well as equal values in each component.*

Definition. *An **identity** element e is defined as $ea = ae = a$.*

The definition of an identity element above is in any context (not just for matrices). For matrices this has certain consequences.

Proposition 29. *Identity matrices must be square*

Proof. For a matrix A and an identity matrix I, $AI = IA = A$ which means that AI, IA and A must all have the same dimensions. If A is of dimension $m \times n$ then I must have dimension $n \times m$ but then AI has dimension $m \times m$ while IA has dimension $n \times n$. We conclude that $m = n$ and both matrices are square. □

If A, B, C are matrices s.t. $AB = AC$, can we, in general, conclude that $B = C$?

The answer is no, as the following example shows:

$$A = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & -1 \\ 3 & 5 \end{pmatrix}, \qquad C = \begin{pmatrix} 8 & 0 \\ -4 & 4 \end{pmatrix}$$

$$A = B = \begin{pmatrix} 0 & 0 \\ 4 & 4 \end{pmatrix}$$

This is because multiplication by A has no inverse (i.e. it's not a bijection and A^{-1} does not exist) as we can see by the fact that $|A| = 0$.

If A, B, C are matrices s.t. $A + 5B = A + 5C$, can we, in general, conclude that $B = C$?

The answer is yes because the matrix addition and scalar multiplication always have inverses. The inverse of $+A$ is $-A$ and the inverse of scalar multiplication by 5 is scalar multiplication by $\frac{1}{5}$. So we can say,

$$\begin{aligned} & A + 5B = A + 5C \\ \iff \quad & A + 5B - A = A + 5C - A \\ \iff \quad & 5B = 5C \\ \iff \quad & \left(\frac{1}{5}\right) 5B = \left(\frac{1}{5}\right) 5C \\ \iff \quad & B = C \end{aligned}$$

Matrix multiplication

Multiplication of matrices proceeds as a collection of dot-products of individual vectors. As a result, its properties are largely dependent on the properties of the dot-product. These are:

> If $\vec{\boldsymbol{x}} = (a, b)^T$ and $\vec{\boldsymbol{y}} = (e, g)^T$ then the dot-product $\langle \vec{\boldsymbol{x}}, \vec{\boldsymbol{y}} \rangle = ae + bg$ and,

- $\langle \vec{\boldsymbol{x}}, \vec{\boldsymbol{y}} \rangle = \langle \vec{\boldsymbol{y}}, \vec{\boldsymbol{x}} \rangle$
- $\alpha \langle \vec{\boldsymbol{x}}, \vec{\boldsymbol{y}} \rangle = \langle \alpha \vec{\boldsymbol{x}}, \vec{\boldsymbol{y}} \rangle = \langle \vec{\boldsymbol{x}}, \alpha \vec{\boldsymbol{y}} \rangle$
- $\langle \vec{\boldsymbol{x}} + \vec{\boldsymbol{y}}, \vec{\boldsymbol{z}} \rangle = \langle \vec{\boldsymbol{x}}, \vec{\boldsymbol{z}} \rangle + \langle \vec{\boldsymbol{y}}, \vec{\boldsymbol{z}} \rangle$
- $\langle \vec{\boldsymbol{x}}, \vec{\boldsymbol{x}} \rangle \geq 0$ and $\langle \vec{\boldsymbol{x}}, \vec{\boldsymbol{x}} \rangle = 0 \iff \vec{\boldsymbol{x}} = 0$

Matrix multiplication treats the two operand matrices as collections of vectors with the first matrix having the vectors as rows and the second having the vectors as columns.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix}$$

This difference in orientation of the vectors in the two operands results in the multiplication not being commutative - the order matters. So, the first property of the dot-product is not preserved but the others are preserved (albeit with a slight modification for the last one).

$$\alpha \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} \alpha a & \alpha b \\ \alpha c & \alpha d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} \alpha(ae+bg) & \alpha(af+bh) \\ \alpha(ce+dg) & \alpha(cf+dh) \end{bmatrix} = \alpha \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

$$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} = \begin{bmatrix} i\,(a+e)+k\,(b+f) & j\,(a+e)+l\,(b+f) \\ i\,(c+g)+k\,(d+h) & j\,(c+g)+l\,(d+h) \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}^T = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{bmatrix}$$

So, to summarize:

If A, B, C are matrices and α is a scalar then,

- $\alpha AB = (\alpha A)B = A(\alpha B) = \alpha(AB)$
- $(A+B)C = C(A+B) = AC + BC$
- AA^T is a symmetric matrix with positive values along the diagonal

Matrix transpose

Denote the ith row of the matrix A as $A[i :]$ and the jth column of the matrix B as $B[j :]$ and a matrix whose components at (i, j) are the dot-products of the ith row of the matrix A with the jth column of the matrix B as $(\langle A[i :], B[: j]\rangle)$. Then,

$$\begin{aligned} (AB)^T &= (\langle A[i :], B[: j]\rangle)^T = (\langle A[j :], B[: i]\rangle) \\ B^T A^T &= (\langle B^T[i :], A^T[: j]\rangle) = (\langle B[: i], A[j :]\rangle) \end{aligned}$$

So, $(AB)^T = B^T A^T$. A consequence of this is that,

$$\begin{aligned} & & I = AA^{-1} = (AA^{-1})^T = (A^{-1})^T A^T \\ \iff & & I(A^T)^{-1} = (A^{-1})^T A^T (A^T)^{-1} \\ \iff & & (A^T)^{-1} = (A^{-1})^T \end{aligned}$$

Matrix inverse

Definition. *Inverse property is if $\exists$ a matrix B s.t. $AB = BA = I$ then B is the **inverse** of A.*

This definition is inherently bound up with the definition of the identity ($\exists$ a matrix I s.t. $AI = IA = A$) and both define the identity and inverse elements as commutatively producing their result under matrix multiplication. Since matrix multiplication is not, in general, commutative there is no guarantee that if $AB = I$ then $BA = I$. An example of this failing is,

$$A = \begin{bmatrix} 1 & 2 \end{bmatrix}, B = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$AB = \begin{bmatrix} 1 \end{bmatrix} = I_1, BA = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix} \neq I_2$$

But we could have guessed this because Proposition 29 showed that identity matrices must be square and its product with a matrix must be defined from both the left and the right, i.e. $IA = AI = A$ meaning that the matrix A must have the same dimensions as I. So, for non-square matrices, no identity can exist. If there is no identity, then the inverse is not defined either.

Proposition 30. *If the inverses of the matrices A and B both exist then so does the inverse of the product AB and it is equal to $B^{-1}A^{-1}$.*

Proof.

$$\begin{aligned} & & (AB)(AB)^{-1} = I \\ \iff & & (A^{-1}A)B(AB)^{-1} = A^{-1}I \\ \iff & & (B^{-1}B)(AB)^{-1} = B^{-1}A^{-1} \\ \iff & & (AB)^{-1} = B^{-1}A^{-1} \end{aligned}$$

and since B^{-1} and A^{-1} both exist then their product exists. Furthermore, this holds for a product of any finite sequence of invertible matrices $A_1A_2\cdots A_n$ which can easily be shown by induction on the associative product. □

Matrices as linear transformations (tags: linear algebra)

Multiplying a vector by a matrix on the left: $A\vec{\boldsymbol{x}} = \vec{\boldsymbol{y}}$

Left multiplication of a matrix A of dimension $m \times n$ on a column vector $\vec{\boldsymbol{x}}$ of dimension $n \times 1$ transforms it to a column vector $\vec{\boldsymbol{y}}$ of dimension $m \times 1$.

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix}$$

This can be thought of a function from the space of n-dimensional vectors from which $\vec{\boldsymbol{x}}$ is drawn to the space of m-dimensional vectors in which $\vec{\boldsymbol{y}}$ resides. So, for real-valued vectors, the function would be a function $f : \mathbb{R}^n \mapsto \mathbb{R}^m$ such that,

$$f(x_1, \cdots, x_n) = \vec{\boldsymbol{y}} = \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix}$$

Or else, this could be thought of as m n-ary functions of the form $f : \mathbb{R}^n \mapsto \mathbb{R}$,

$$\begin{aligned} f_1(x_1, \cdots, x_n) &= a_{11}x_1 + \cdots + a_{1n}x_n = y_1 \\ &\vdots \\ f_m(x_1, \cdots, x_n) &= a_{m1}x_1 + \cdots + a_{mn}x_n = y_m \end{aligned}$$

In this case, each row of the matrix is a real-valued function in n variables. Each of these functions is *homogenous linear* (a function of the form $a_1x_1 + \cdots + a_kx_k + c$ for scalars $a_1, \cdots, a_k, c$ and $c = 0$) and so the system of functions is called a *linear transformation*.

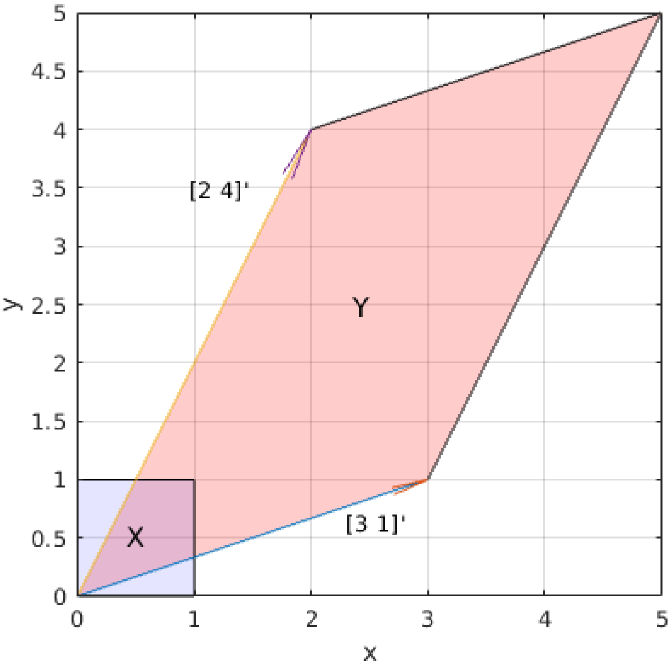
Multiplying a matrix of vectors by a matrix on the left: $AX = Y$

Looking at the matrix as a linear transformation from one co-ordinate space to another, consider $AX = Y$ where X is a matrix - which may be considered a collection of vectors - transformed by the matrix A into the matrix - or collection of vectors - Y.

We transform the unit square in the source space, X in $\mathbb{R}^2$, using the 2D transformation matrix A, into its image in the destination space, Y in $\mathbb{R}^2$.

$$A = \begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}, \; X = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$AX = Y = \begin{bmatrix} 0 & 3 & 5 & 2 \\ 0 & 1 & 5 & 4 \end{bmatrix}$$



Types of Transformations

There are 3 basic types of transformation:

- **Rigid body** - preserves distances and angles.

  Examples: translation and rotation.

- **Conformal** - preserves angles.

  Examples: translation, rotation and uniform scaling.

- **Affine** - preserves parallelism.

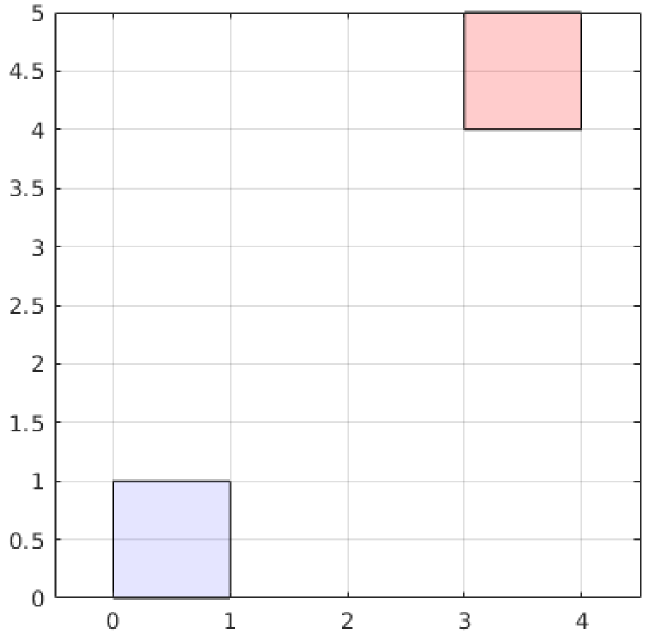
  Examples: translation, rotation, uniform and non-uniform scaling, shearing and reflection.

Rigid Body

Translation So as to perform the translation as multiplication by a transformation matrix we take the approach of homogeneous coordinates (see:`https://en.wikipedia.org/wiki/Homogeneous_coordinates`) so we form matrix with the identity in the first two columns and then a third column with the translation vector. Then, we add a row of ones to the vectors we will translate and the output vectors also have a 1 in the third row that is ignored.

$$A = \begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix}, \; X = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

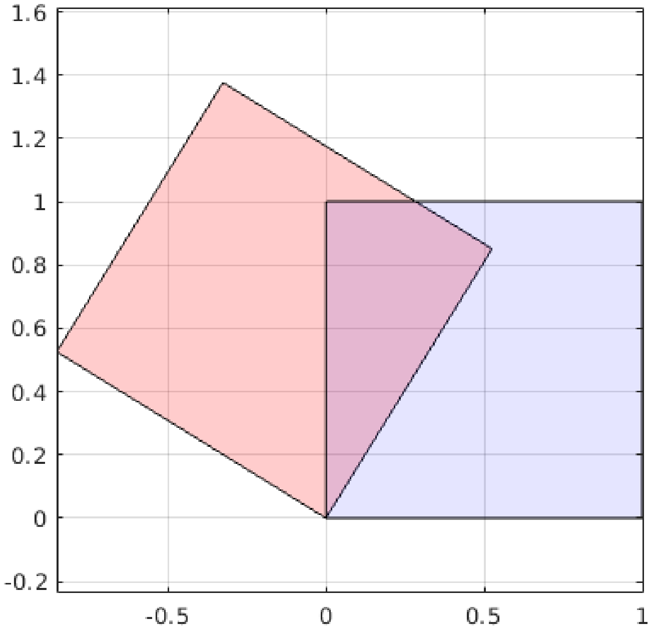
$$AX = Y = \begin{bmatrix} 3 & 4 & 4 & 3 \\ 4 & 4 & 5 & 5 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$



Rotation

$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix},\ X = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$AX = Y = \begin{bmatrix} 0 & 0.5253 & -0.3256 & -0.8509 \\ 0 & 0.8509 & 1.3762 & 0.5253 \end{bmatrix}$$

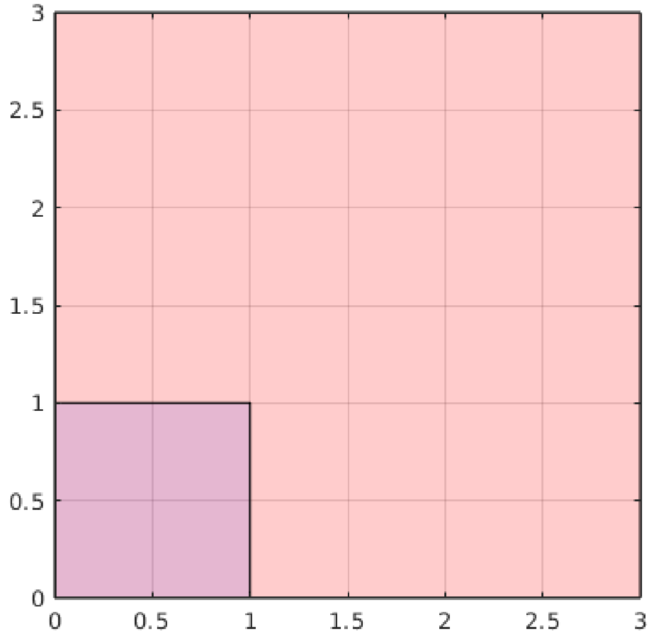


Conformal

Uniform Scaling

$$A = \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix},\ X = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$AX = Y = \begin{bmatrix} 0 & 3 & 3 & 0 \\ 0 & 0 & 3 & 3 \end{bmatrix}$$

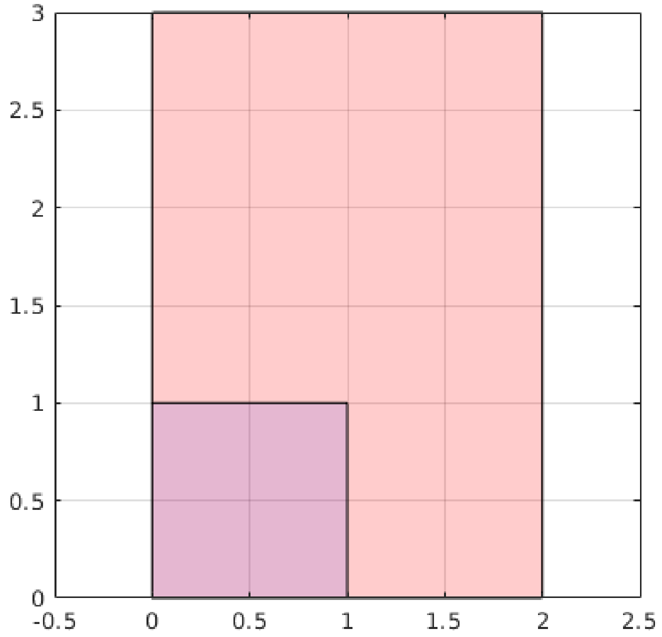


Affine

Non-uniform Scaling

$$A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix},\ X = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

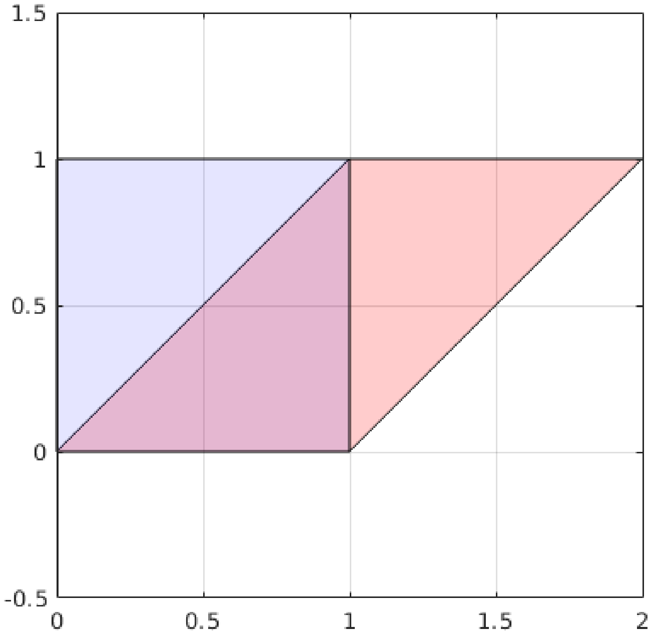
$$AX = Y = \begin{bmatrix} 0 & 2 & 2 & 0 \\ 0 & 0 & 3 & 3 \end{bmatrix}$$



Shearing

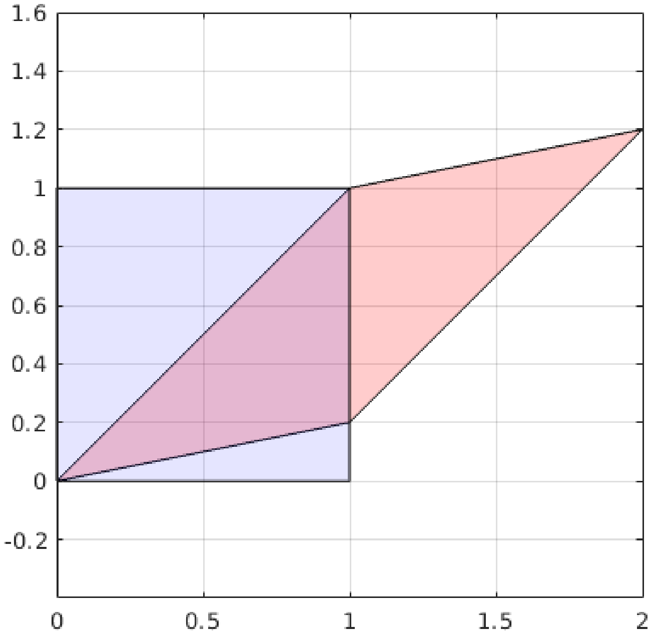
$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},\ X = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$AX = Y = \begin{bmatrix} 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$



$$A = \begin{bmatrix} 1 & 1 \\ 0.2 & 1 \end{bmatrix},\ X = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

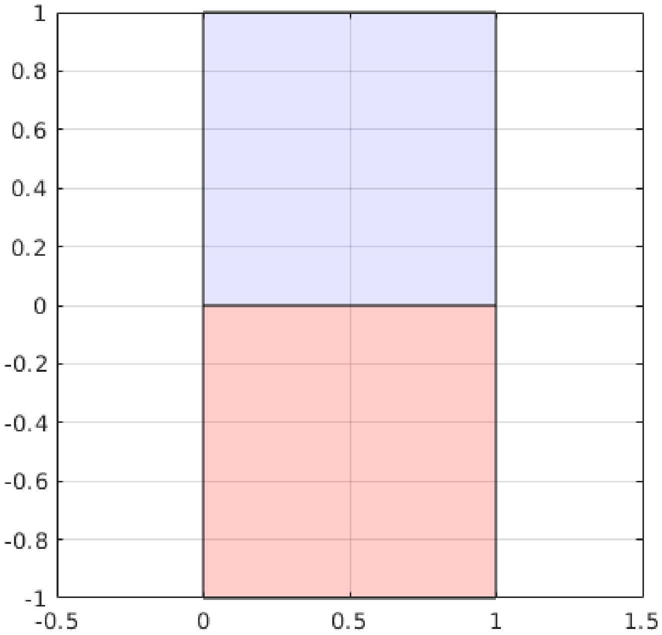
$$AX = Y = \begin{bmatrix} 0 & 1 & 2 & 1 \\ 0 & 0.2 & 1.2 & 1 \end{bmatrix}$$



Reflection

$$A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ X = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$AX = Y = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & -1 \end{bmatrix}$$


1
0.8
0.6
0.4
0.2
0
-0.2
-0.4
-0.6
-0.8
-1
-0.5
0
0.5
1
1.5

Elementary Matrices and Row Operations **(tags: linear algebra)**

Notation. The **matrix units** - matrices with a single non-zero component whose value is 1 are traditionally named $\boldsymbol{e_{ij}}$ where i, j is the matrix coordinate of the 1.

An arbitrary matrix $A = (a_{ij})$ may be expressed as a sum of such unit matrices as $A = a_{11}e_{11} + \cdots + a_{nn}e_{nn}$.

$$e_{ij} = \begin{bmatrix} \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots \\ \cdots & 1 & \cdots \\ \vdots & \vdots & \vdots \\ \cdots & \cdots & \cdots \end{bmatrix}$$

So matrix units can be used to analyse matrix addition but to analyse matrix multiplication some square matrices called **elementary matrices** are more useful.

Multiplying a matrix from the left (so doing row operations), there are 3 types of elementary matrix:

Adding rows: $\boldsymbol{I + ae_{ij}}$ **for** $\boldsymbol{i \neq j}$

$$\begin{bmatrix} 1 & & & \\ & \cdot & a & \\ & & \cdot & \\ & & & 1 \end{bmatrix}$$

This adds a times some row to another row.

Swapping rows: $\boldsymbol{I + e_{ij} + e_{ji} - e_{ii} - e_{jj}}$ **for** $\boldsymbol{i \neq j}$

$$\begin{bmatrix} 1 & & & \\ & 0 & 1 & \\ & 1 & 0 & \\ & & & 1 \end{bmatrix}$$

This swaps the rows i and j.

Scalar-multiplying a row: $\boldsymbol{I + (c-1)e_{ii}}$ for $\boldsymbol{c \neq 0}$

$$\begin{bmatrix} 1 & & & \\ & \cdot & & \\ & & c & \\ & & & 1 \end{bmatrix}$$

This multiplies row i by c.

Proposition 31. *Elementary matrices are invertible and their inverses are also elementary matrices.*

Proof. Proceed by cases on the 3 elementary types of elementary matrices.

Case $\boldsymbol{I + ae_{ij}}$ If R_i is row i and R_j is row j, then this matrix performs $R_i + aR_j$. Clearly this can be "undone" by performing $R_i - aR_j$. So the matrix, $I - ae_{ij}$ is the inverse and clearly this is also an elementary matrix of the same type.

Case $\boldsymbol{I - e_{ii} - ejj + e_{ij} + e_{ji}}$ This matrix swaps 2 rows in a permutation that is its own inverse.

Case $\boldsymbol{I + (c-1)e_{ii}}$ This matrix performs cR_i and so it is "undone" by performing $c^{-1}R_i$ (which for a real-valued matrix would be $\left(\frac{1}{c}\right) R_i$) and this inverse matrix is also an elementary matrix of the same type. □

Proposition 32. *Suppose $AX = B$ and a series of elementary row operations on $[A \mid B]$ produces $[A' \mid B']$, then the solutions of $A'X = B'$ are the same as those of $AX = B$.*

Proof. First note that the series of elementary row operations is described as multiplication on the left by a series of elementary matrices say, $E_1, E_2, \cdots, E_n$ so that,

$$[A' \mid B'] = [(E_n \cdots E_2 E_1)A \mid (E_n \cdots E_2 E_1)B]$$

Now, let $(E_n \cdots E_2 E_1) = E$ and notice that, since each of the individual E_i is invertible the product of them is also invertible by Proposition 30 so,

$$A'X = B' \iff EAX = EB$$

and the existence of the inverse E^{-1} means that the law of cancellation is in effect so,

$$EAX = EB \iff AX = B$$

$$\therefore A'X = B' \iff AX = B$$

□

Proposition 33. *Let A be a square matrix. The following conditions are equivalent:*

- *A can be reduced to the identity by a sequence of elementary row operations.*
- *A is a product of elementary matrices.*
- *A is invertible.*
- *The system of homogeneous equations $AX = 0$ has only the trivial solution $X = 0$.*

Proof. If A can be reduced to the identity by a sequence of elementary row operations then,

$$(E_n \cdots E_2 E_1)A = I$$

and by Proposition 31 and Proposition 30 the matrix $(E_n \cdots E_2 E_1)$ is invertible so,

$$A = (E_n \cdots E_2 E_1)^{-1} I = (E_n \cdots E_2 E_1)^{-1} = {E_1}^{-1} {E_2}^{-1} \cdots {E_n}^{-1}$$

and, also by Proposition 31, A is a product of elementary matrices and is invertible.
Furthermore, if $AX = 0$ then $X = A^{-1}0 = 0$ - i.e. the only solution to $AX = 0$ is $X = 0$. □

Determinants (tags: linear algebra)

1×1

The determinant of a 1×1 matrix is just its unique component entry,

$$det \begin{bmatrix} a \end{bmatrix} = a$$

2×2

The determinant of a 2×2 matrix is given by the formula,

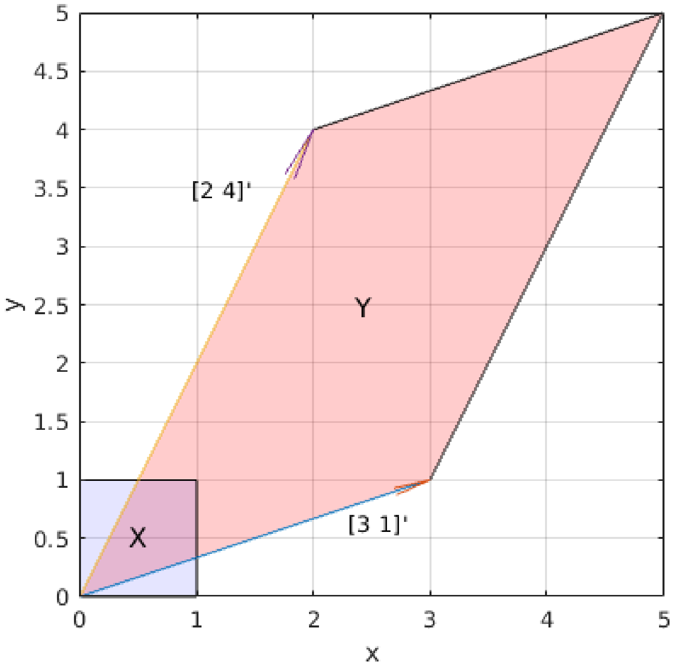
$$det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc$$

Returning to our example of a 2d operator:

We transform the unit square in the source space, X in $\mathbb{R}^2$, using the 2D transformation matrix A, into its image in the destination space, Y in $\mathbb{R}^2$.

$$A = \begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}, \; X = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$AX = Y = \begin{bmatrix} 0 & 3 & 5 & 2 \\ 0 & 1 & 5 & 4 \end{bmatrix}$$



We see that $det\ A = 10$ and the parallelogram, Y, that is the image of the unit square, X, under the transformation represented by A has area,

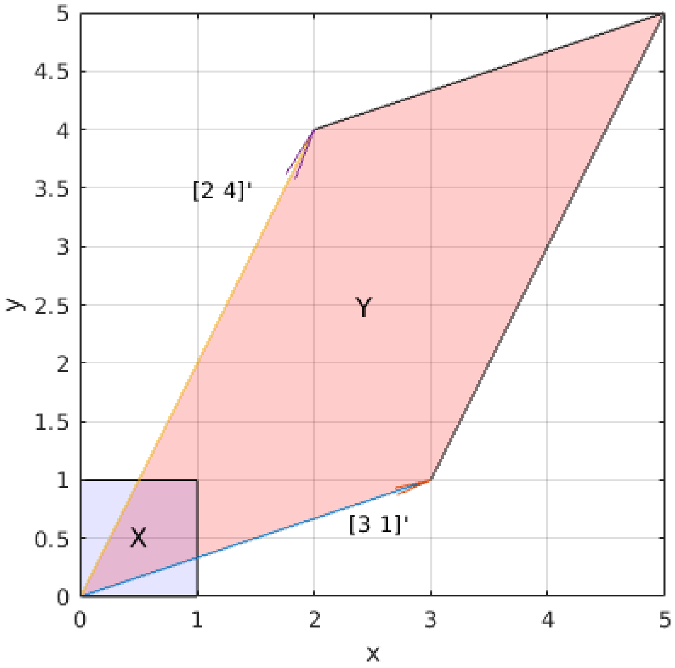
$$\text{area } = b \cdot h = |\langle 3, 1\rangle| \cdot |\langle 2-3, 4-1\rangle| = \sqrt{10} \cdot \sqrt{10} = 10$$

And the determinant would be 0 in the case that the columns were proportional (representing co-linear vectors) and the determinant would be negative if the orientation of the output vectors were reversed w.r.t. the input vectors.
So, if we swap either the columns or the rows of the transformation matrix, A, the determinant comes out -10.

Swapping the columns:

$$A_c = \begin{bmatrix} 2 & 3 \\ 4 & 1 \end{bmatrix},\ X = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$AX = Y = \begin{bmatrix} 0 & 2 & 5 & 3 \\ 0 & 4 & 5 & 1 \end{bmatrix}$$

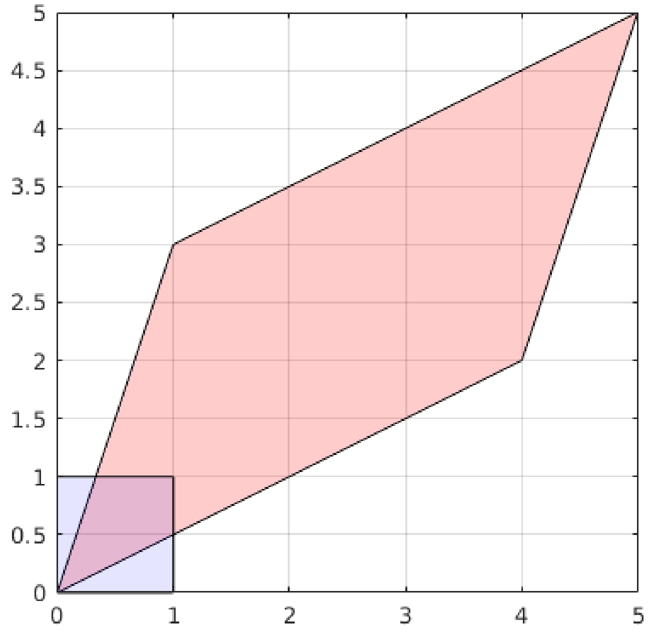


Note that the result looks exactly the same - it's just that now the x-vector $\langle 1, 0\rangle$, produces $\langle 4, 2\rangle$ and the y-vector, $\langle 0, 1\rangle$ produces $\langle 3, 1\rangle$.

Swapping the rows:

$$A_r = \begin{bmatrix} 1 & 4 \\ 3 & 2 \end{bmatrix}, \; X = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$AX = Y = \begin{bmatrix} 0 & 1 & 5 & 4 \\ 0 & 3 & 5 & 2 \end{bmatrix}$$



Note that if we swap **both** the columns and the rows then we get back to a transformation with determinant 10.

$$A_{rc} = \begin{bmatrix} 4 & 1 \\ 2 & 3 \end{bmatrix},\ X = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$AX = Y = \begin{bmatrix} 0 & 4 & 5 & 1 \\ 0 & 2 & 5 & 3 \end{bmatrix}$$

which produces the same parallelogram as the previous one but with columns reversed.

Summary So we find that,

$$\begin{bmatrix}3 & 2\\1 & 4\end{bmatrix}, \begin{bmatrix}4 & 1\\2 & 3\end{bmatrix} \text{ have determinant } > 0$$

$$\begin{bmatrix}2 & 3\\4 & 1\end{bmatrix}, \begin{bmatrix}1 & 4\\3 & 2\end{bmatrix} \text{ have determinant } < 0$$

If the product of the components on the diagonal of the matrix is greater than the components on the bottom-left to top-right diagonal then the determinant is > 0, if the reverse is true then the determinant is < 0, and if they are equal then the determinant $= 0$.
Note that, for the determinant to be 0 in our example, we need something like $detA = (4\times3)-(4\times3)$ which, due to the commutativity of multiplication can be achieved by both,

$$\begin{bmatrix}4 & 3\\4 & 3\end{bmatrix}, \begin{bmatrix}4 & 4\\3 & 3\end{bmatrix}$$

but in both cases the columns are proportional and therefore co-linear.

$n \times n$

The determinant of an $n \times n$ matrix is defined recursively as:

- if $n = 1$ then $det\,A = a_{11}$, i.e. the determinant is equal to the sole component.
- else if $n > 1$ then, defining A_{ij} as the matrix formed by leaving out the ith row and the jth column,

$$det\,A = a_{11}det\,A_{11} - a_{12}det\,A_{12} + \cdots \pm a_{1n}det\,A_{1n}$$

In the $n = 2$ case, each $det\,A_{ij}$ has $n = 1$ and so is simply equal to the sole component that is neither on the same row or column as the component a_{ij} that is multiplying it. This feature of the determinant calculation continues recursively for higher dimension matrices so that the calculation is always comprised of terms that are a product of components on each of the different

columns and rows. In fact, it comprises the products of all such possible combinations of components.
For example, when $n = 2$ the only combinations are,

$$\{a_{11}, a_{22}\} \text{ and } \{a_{12}, a_{21}\}$$

so there are only 2 terms in the determinant calculation.
When $n = 3$ the possible combinations are,

$$\begin{gathered}\{a_{11}, a_{22}, a_{33}\},\ \{a_{11}, a_{32}, a_{23}\},\\ \{a_{12}, a_{21}, a_{33}\},\ \{a_{12}, a_{31}, a_{23}\},\\ \{a_{13}, a_{21}, a_{32}\},\ \{a_{13}, a_{31}, a_{22}\}\end{gathered}$$

so there are 6 terms in the determinant calculation. Notice that each term is generated by a different permutation of the columns while holding the rows fixed in ascending order and that the sign of each term is governed by how many permutations the permutation of columns is away from ascending order, $1, 2, \cdots, n$.

$$\begin{aligned}\begin{vmatrix}a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{vmatrix} &= a_{11}(a_{22}a_{33} - a_{32}a_{23}) - a_{12}(a_{21}a_{33} - a_{31}a_{23}) + a_{13}(a_{21}a_{32} - a_{31}a_{22})\\ &= a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}\end{aligned}$$

Consequences

From this feature of the calculation we can see a number of the important properties of the determinant.

Proposition 34. *$det\, I = 1$*

Proof. Whatever the dimension of the identity matrix there will be only one combination of rows and columns that is the diagonal along which the 1s of the identity matrix reside. So, there will be a single term of the determinant calculation that is a product of 1s and all other terms will contain at 0s. In addition, the term that is along the diagonal has a positive sign in the determinant calculation. Therefore the result is 1. □

Proposition 35. *$det\, A$ is linear in the rows of the matrix*

Proof. If p and q are row vectors and we have matrices A_p, A_q, A_{pq} in which are present, respectively, the row vector p, the one q, and the row $p+q$, then linearity implies that $det\, A_{pq} = det\, A_p + det\, A_q$. This can be seen since every term of the determinant calculation of A_{pq} will contain one of the components in the row $p+q$. So each term of the calculation will take the form,

$$(p+q)a_{ij}\cdots a_{mn} = p(a_{ij}\cdots a_{mn}) + q(a_{ij}\cdots a_{mn})$$

The other implication of linearity is that - if a row is multiplied by a scalar, c, to produce A_c then $det\, A_c = c\, det\, A$. Using a similar reasoning to the previous argument we have each term of the determinant taking the form,

$$c\, a_{ij}\cdots a_{mn}$$

which obviously results in the determinant being multiplied by c. □

Proposition 36. *If two columns are exchanged in the matrix then the determinant is multiplied by* -1

Proof. If columns p and q are exchanged then the components of p and q appear in terms with signs reversed. Since the components of p and q appear in every term of the determinant calculation, every term has the sign reversed. So the determinant is multiplied by -1. □

Proposition 37. $det\, A = 0$ *if there are two identical columns in the matrix*

Proof. If column p is identical to column q then we can swap columns p and q and we will have the same matrix so the determinant must also remain the same. But Proposition 36 proved that swapping two columns causes the determinant to be multiplied by -1. So, if A_{pq} is the matrix A after swapping the columns,

$$det\, A_{pq} = det\, A = -det\, A \iff det\, A = 0$$

□

Proposition 38. *Adding a multiple of one column to another leaves the determinant unchanged*

Proof. By combining Proposition 35 and Proposition 37 we find that if the columns of A are,

$$\vec{\boldsymbol{x_1}}, \vec{\boldsymbol{x_2}}, \cdots, \vec{\boldsymbol{x_p}}, \vec{\boldsymbol{x_q}}, \cdots, \vec{\boldsymbol{x_n}}$$

and the columns of A_c are,

$$\vec{\boldsymbol{x_1}}, \vec{\boldsymbol{x_2}}, \cdots, \vec{\boldsymbol{x_p}} + c\vec{\boldsymbol{x_q}}, \vec{\boldsymbol{x_q}}, \cdots, \vec{\boldsymbol{x_n}}$$

then,

$$\begin{aligned} det\, A_c &= det\,(\vec{\boldsymbol{x_1}}, \vec{\boldsymbol{x_2}}, \cdots, \vec{\boldsymbol{x_p}}, \vec{\boldsymbol{x_q}}, \cdots, \vec{\boldsymbol{x_n}}) + c \cdot det\,(\vec{\boldsymbol{x_1}}, \vec{\boldsymbol{x_2}}, \cdots, \vec{\boldsymbol{x_q}}, \vec{\boldsymbol{x_q}}, \cdots, \vec{\boldsymbol{x_n}}) \\ &= det\,(\vec{\boldsymbol{x_1}}, \vec{\boldsymbol{x_2}}, \cdots, \vec{\boldsymbol{x_p}}, \vec{\boldsymbol{x_q}}, \cdots, \vec{\boldsymbol{x_n}}) + c \cdot 0 \\ &= det\, A \end{aligned}$$

□

Better formulation **(from Rudin's Principles of Mathematical Analysis)**

Let $a(i, j)$ be the component in the ith row and jth column of the matrix A and,

$$sign(x) = \begin{cases} -1 & x < 0 \\ 0 & x = 0 \\ 1 & x > 0 \end{cases}$$

$$s(j_1, \cdots, j_n) = \prod_{p<q} sign(j_q - j_p)$$

Then the determinant,

$$det\, A = \sum_i s(j_1, \cdots, j_n) a(i, j_1) \cdots a(i, j_n)$$

defined over all n-tuples of n distinct values, $j_1, \cdots, j_n$ with $1 \leq j_r \leq n$ (i.e, permutations of $[1, n] \subset \mathbb{N}$) with each term being produced by a different permutation.

From this we can see that,

- **The determinant of the identity matrix is 1**
  Every term of the determinant will contain at least one 0 apart from the term that traverses the main diagonal, which is all 1s. We can see that there is only one such term because the main diagonal has $i = j$ and so there is only one such $j_1, \cdots, j_n$ that satisfies this.

- **The determinant is linear in the rows or columns of the matrix, holding the others constant**
  If a column, j_r, is multiplied by a scalar α and another column, j_k, is added to it, then the resulting determinant takes the form,

$$\begin{aligned} & det\,A = \sum_i s(j_1, \cdots, j_n)a(i, j_1) \cdots (\alpha a(i, j_r) + a(i, j_k)) \cdots a(i, j_n) \\ \iff & det\,A = \alpha a(i, j_r) \sum_i s(j_1, \cdots, j_n)a(i, j_1) \cdots a(i, j_n) + \\ & \qquad\qquad a(i, j_k) \sum_i s(j_1, \cdots, j_n)a(i, j_1) \cdots a(i, j_n) \end{aligned}$$

- **If two columns are exchanged then the determinant is multiplied by -1**
  If columns p and q are exchanged then this is equivalent to swapping j_p and j_q in the n-tuple so that $s(j_1, j_2, \cdots, j_n)$ changes sign and so the determinant is multiplied by -1.

- **If two columns are equal then the determinant will be 0**
  If two columns are the same then this is equivalent to a repetition of a value in the tuple $j_1, \cdots, j_n$ and so,

$$\exists\, p, q \text{ s.t. } sign(j_q - j_p) = 0 \implies s(j_1, \cdots, j_n) = 0$$

  which results in every term of the determinant being 0.
  This can also be proven by using the previous property that tells us that the determinant is multiplied by -1 when we exchange the identical columns but - since the columns are identical - the resultant matrix is the same - which means that the determinant remains unchanged. Therefore, the determinant must be 0.

Proposition 39. *If A and B are $n \times n$ matrices, then*

$$det\,BA = det\,A\;det\,B$$

Proof. Let the columns of A be the vectors, $\vec{\boldsymbol{x_1}}, \vec{\boldsymbol{x_2}}, \cdots, \vec{\boldsymbol{x_n}}$ so that for each column j,

$$\vec{\boldsymbol{x_j}} = \sum_i a(i, j)\vec{\boldsymbol{e_i}}$$

and define,

$$\Delta_B(\vec{\boldsymbol{x_1}}, \vec{\boldsymbol{x_2}}, \cdots, \vec{\boldsymbol{x_n}}) = \Delta_B(A) = det\, BA$$

so that,

$$det\,(B\vec{\boldsymbol{x_1}}, B\vec{\boldsymbol{x_2}}, \cdots, B\vec{\boldsymbol{x_n}}) = \Delta_B(\vec{\boldsymbol{x_1}}, \vec{\boldsymbol{x_2}}, \cdots, \vec{\boldsymbol{x_n}})$$

Since $B\vec{\boldsymbol{x_j}}$ is linear in $\vec{\boldsymbol{x_j}}$, $\Delta_B(\vec{\boldsymbol{x_1}}, \vec{\boldsymbol{x_2}}, \cdots, \vec{\boldsymbol{x_n}})$ is linear in each $\vec{\boldsymbol{x_j}}$ and so,

$$\begin{aligned}\Delta_B(\vec{\boldsymbol{x_1}}, \vec{\boldsymbol{x_2}}, \cdots, \vec{\boldsymbol{x_n}}) &= \Delta_B(\sum_i a(i,1)\vec{\boldsymbol{e_i}}, \vec{\boldsymbol{x_2}}, \cdots, \vec{\boldsymbol{x_n}}) \\ &= \sum_i a(i,1)\Delta_B(\vec{\boldsymbol{e_i}}, \vec{\boldsymbol{x_2}}, \cdots, \vec{\boldsymbol{x_n}}) \\ &= \sum_{i_1} a(i_1,1) \sum_{i_2} a(i_2,2) \cdots \sum_{i_n} a(i_n,n)\, \Delta_B(\vec{\boldsymbol{e_{i_1}}}, \vec{\boldsymbol{e_{i_2}}}, \cdots, \vec{\boldsymbol{e_{i_n}}}) \\ &= \sum a(i_1,1)a(i_2,2)\cdots a(i_n,n)\, \Delta_B(\vec{\boldsymbol{e_{i_1}}}, \vec{\boldsymbol{e_{i_2}}}, \cdots, \vec{\boldsymbol{e_{i_n}}})\end{aligned}$$

the sum being extended over all n-tuples, $(i_1, \cdots, i_n)$ such that $1 \le i_j \le n$. Also, by referring again to the properties of the determinant we see that,

$$\Delta_B(\vec{\boldsymbol{e_{i_1}}}, \vec{\boldsymbol{e_{i_2}}}, \cdots, \vec{\boldsymbol{e_{i_n}}}) = t(i_1, i_2, \cdots, i_n)\Delta_B(\vec{\boldsymbol{e_1}}, \vec{\boldsymbol{e_2}}, \cdots, \vec{\boldsymbol{e_n}})$$

where $t(i_1, i_2, \cdots, i_n) = 1, 0, -1$ similar to the function s previously. So, we end up with,

$$det\, BA = \sum a(i_1,1)a(i_2,2)\cdots a(i_n,n)t(i_1, i_2, \cdots, i_n)\, det\, B = det\, A\, det\, B$$

□

Proposition 40. *A linear operator A on $\mathbb{R}^n$ is invertible if and only if $det\, A \neq 0$*

Proof. If A is invertible then, $AA^{-1} = I$ and, using Proposition 34 and Proposition 39, we have,

$$det\, AA^{-1} = det\, A \cdot det\, A^{-1} = 1$$

so $det\, A$ cannot be 0.

Furthermore, if the columns of A are not independent then there is some linear combination of the columns that produces $\vec{\mathbf{0}}$. Since, by Proposition 38 we know that adding multiples of columns to other columns leaves the determinant unchanged, this means that the determinant is equal to the determinant of a matrix with $\vec{\mathbf{0}}$ as a column. Such a matrix has determinant 0, so the determinant of A is also 0. □

Corollary 9. *For invertible matrices,*

$$det\, A^{-1} = \frac{1}{det\, A}$$

Corollary 10. *The determinant is the only function that has the described properties.*

Proof. Every matrix, A, can be transformed by multiplication by elementary matrices to a row-reduced form, R, which is either the identity matrix - in the case that A is invertible - or a matrix with the last row zeroes - in the case where A is not invertible. So, the determinant of the row-reduced matrix, R, is either 1 or 0. Meanwhile, the determinants of the elementary matrices are:

- Add multiple of row to another row - determinant is 1 because this operation maintains the determinant of the identity.
- Swap two rows - determinant is -1 - determinant is -1 because this operation multiplies the determinant of the identity by -1.
- Multiply a row by some scalar c - determinant is c because this operation multiplies the determinant of the identity by c.

So, we have,

$$R = E_1 E_2 \cdots E_n A \implies det\, R = det\, E_1 E_2 \cdots E_n \cdot det\, A$$

where $det\, E_1 E_2 \cdots E_n$ is a known, non-zero quantity - say d_e. Since the determinant of R is either 0 or 1 this leaves the determinant of A being either 0 or $\frac{1}{d_e}$.

So, the value of the determinant of an arbitrary matrix, A, is wholly determined by the properties described. □

Permutation Matrices (tags: linear algebra)

Definition. *A permutation p is a bijective map from a set S to itself. If a matrix P is the matrix associated with a permutation p then:*

- *the jth column of the matrix is the basis vector $e_{p(j)}$,*
- *P is a sum of the matrix units, $P = e_{p(1)1} + e_{p(2)2} + \cdots + e_{p(n)n} = \sum_j e_{p(j)j}$.*

Proposition 41. *If P, Q are permutation matrices associated with the permutations p, q then the matrix that corresponds to the permutation $p \circ q$ is PQ*

Proof. $pq(i) = p(q(i))$ and $PQX = P(QX)$ □

Proposition 42. *A permutation matrix P is invertible and its inverse is the transpose, $P^{-1} = P^T$*

Proof. A left-multiplying permutation matrix for a permutation, p, maps each row from the input matrix using a column j in the permutation matrix, to the output row, $p(j)$. Since the permutation, by definition, is bijective, we know that this mapping is one-to-one and invertible. If we transpose the matrix P to P^T, swapping rows and columns in the permutation matrix, then the new matrix, P^T maps input rows $p(j)$ into output rows j which is clearly the inverse permutation. □

Since a permutation matrix is a the result of permuting the rows of the identity matrix, clearly, its determinant is ±1. A permutation is referred to as *odd* or *even* depending on whether its determinant is -1 or 1 respectively. Its determinant is called the *sign of the permutation*,

$$sign\, p = det\, p = \pm 1$$

The determinant of an arbitrary $n \times n$ matrix can be described as,

$$\begin{aligned} det\,A &= \sum_p \left[det\,\sum_j a_{p(j)j} e_{p(j)j} \right] \\ &= \sum_p \left[(a_{p(1)1} \cdots a_{p(n)n}) \cdot \; det\,\sum_j e_{p(j)j} \right] \\ &= \sum_p \Big[(a_{p(1)1} \cdots a_{p(n)n}) \cdot \; det\,P \Big] \\ &= \sum_p \Big[(sign\,p)(a_{p(1)1} \cdots a_{p(n)n}) \Big] \end{aligned}$$

This is the same formula as earlier and is known as the *complete expansion* of the determinant.

Cramer's Rule (tags: linear algebra)

Expansion by minors on the jth column:

$$det\,A = (-1)^{j+1} a_{1j}\, det\, A_{1j} + (-1)^{j+2} a_{2j}\, det\, A_{2j} + \cdots + (-1)^{j+n} a_{nj}\, det\, A_{nj}$$

Expansion by minors on the ith row:

$$det\,A = (-1)^{i+1} a_{i1}\, det\, A_{i1} + (-1)^{i+2} a_{i2}\, det\, A_{i2} + \cdots + (-1)^{i+n} a_{in}\, det\, A_{in}$$

Definition. *If we form a matrix with elements $\alpha_{ij} = (-1)^{i+j}\, det\, A_{ij}$ and then transpose it we get the* ***adjoint matrix****.*

Notation. The adjoint of A is denoted $adj\ A$.

Following we use $[x]$ to denote a matrix as distinguished from a scalar.

Let $d = det\,A$. Then, if we multiply the adjoint matrix of $[A]$ by $[A]$ we get,

$$[adj\ A][A] = \begin{bmatrix} d & & & & & \\ & d & & & & \\ & & \cdot & & & \\ & & & \cdot & & \\ & & & & \cdot & \\ & & & & & d \end{bmatrix}$$

The off-diagonal elements come out zero because they involve a determinant calculation that involves the same row (or column) repeated and so those determinants are zero.

Theorem 4.

$$[adj\ A][A] = (det\,A)[I] = [A][adj\ A]$$

Corollary 11.

$$\frac{1}{det\,A}[adj\ A][A] = [I] \iff [A^{-1}] = \frac{1}{det\,A}[adj\ A]$$

This formulation of the inverse of a matrix can be used to write the solution to a system of linear equations (reverting to the normal notation) $AX = B$ as, multiplying on the left by A^{-1},

$$X = A^{-1}B = \frac{1}{det\,A}(adj\;A)B$$

so that X is a vector whose components, x_j, are expressed as,

$$\begin{aligned} x_j &= \frac{1}{det\,A}(b_1\alpha_{1j} + \cdots + b_n\alpha_{nj}) \\ &= \frac{1}{det\,A}(b_1(-1)^{1+j}\,det\,A_{1j} + \cdots + b_n(-1)^{n+j}\,det\,A_{nj}) \end{aligned}$$

which is the expansion by minors of A on the jth column but with the components a_{ij} of A replaced with the components of the vector B, divided by the determinant of A.

Relations on matrices (tags: linear algebra)

Let X be the set of $n \times n$ real matrices. Define a relation $\sim$ on X by:

$$M \sim N \iff \exists \text{ an invertible } P \in X \text{ s.t. } N = P^{-1}MP.$$

Prove that $\sim$ is an equivalence relation. (tags: linear algebra, equivalence relations)

Reflexivity:

$$\begin{aligned} N &= I^{-1}NI \\ \therefore N &\sim N \end{aligned}$$

Symmetry:

$$\begin{array}{rc} & N = P^{-1}MP \\ \iff & NP^{-1} = P^{-1}M(PP^{-1}) \\ \iff & NP^{-1} = P^{-1}M \\ \iff & PNP^{-1} = (PP^{-1})M \\ \iff & PNP^{-1} = M \\ \iff & R^{-1}NR = M, \quad R \in X \\ \therefore & N \sim M \iff M \sim N \end{array}$$

Transitivity:

$$\begin{array}{rc} & N = P^{-1}MP, \quad M = Q^{-1}AQ \\ \Longrightarrow & N = P^{-1}(Q^{-1}AQ)P \\ \iff & N = (P^{-1}Q^{-1})A(QP) \\ \iff & N = R^{-1}AR, \quad R \in X \\ \therefore & (N \sim M) \wedge (M \sim Q) \iff (N \sim Q) \end{array}$$

Linear Algebra of Polynomials (tags: linear algebra, polynomials)

If we look for quadratic polynomials, $p\,(x)$, that pass throught the 3 points (1, 3), (3, 1) and (5, 2):

./figure_0-eps-converted-to.pdf

Then the first has roots at $x = 1, 3$ and passes through the point (5, 2). So, we have:

$$p(1) = p(3) = 0, p(5) = 2$$

meaning that $(x - 1)$and $(x - 3)$are factors. Therefore,

$$\begin{aligned} p(x) &= \alpha(x-1)(x-3) \\ &= \alpha(x^2-4x+3) \end{aligned}$$

$$\begin{array}{rcl} & p(5) & = 2 \\ \Longrightarrow & \alpha(5^2-4(5)+3) & = 2 \\ \Longleftrightarrow & 8\alpha & = 2 \\ \Longleftrightarrow & \alpha & = \frac{1}{4} \end{array}$$

$$\therefore p(x) = \frac{1}{4}(x^2-4x+3)$$

./figure_1-eps-converted-to.pdf

The second has roots at $x = 1, 5$ and passes throught the point (3, 1):

$$\begin{aligned} p(x) &= \alpha(x-1)(x-5) \\ &= \alpha(x^2 - 6x + 5) \end{aligned}$$

$$\begin{array}{ccc} & p(3) & = 1 \\ \implies & \alpha(3^2 - 6(3) + 5) & = 1 \\ \iff & -4\alpha & = 1 \\ \iff & \alpha & = -\frac{1}{4} \end{array}$$

$$\therefore p(x) = -\frac{1}{4}(x^2 - 6x + 5)$$

./figure_2-eps-converted-to.pdf

The third has roots at $x = 3, 5$ and passes through the point (1, 3):

$$\begin{aligned} p(x) &= \alpha(x-3)(x-5) \\ &= \alpha(x^2 - 8x + 15) \end{aligned}$$

$$\begin{array}{rcl} & p(1) & = 3 \\ \implies & \alpha(1^2 - 8(1) + 15) & = 3 \\ \iff & 8\alpha & = 3 \\ \iff & \alpha & = \tfrac{3}{8} \end{array}$$

$$\therefore p(x) = \frac{3}{8}(x^2 - 8x + 15)$$

./figure_3-eps-converted-to.pdf

Adding them together we get,

$$\begin{aligned}
&\tfrac{1}{4}(x^2-4x+3)-\tfrac{1}{4}(x^2-6x+5)+\tfrac{3}{8}(x^2-8x+15)\\
=\;&(\tfrac{1}{4}-\tfrac{1}{4}+\tfrac{3}{8})x^2+(-1+\tfrac{6}{4}-3)x+(\tfrac{3}{4}-\tfrac{5}{4}+\tfrac{45}{8})\\
=\;&\tfrac{3}{8}x^2-\tfrac{10}{4}x+\tfrac{41}{8}
\end{aligned}$$

./figure_4-eps-converted-to.pdf

Integration Techniques

High-level Strategy

- If the power of an expression in parentheses is low, we can multiply it out. Single terms - however high the powers are - can always be integrated. What prevents us from doing this with high powers is that the number of terms explodes.

- If the power of an expression in parentheses is high, we need to look for a substitution or simplification.

- If we can manipulate the integrand so that we achieve a multiplication by f'(x) for some f(x) in the integrand, then we can make a u-substitution of f(x).

- In particular, if we can achieve $\frac{f'(x)}{f(x)}$ then we can integrate to $\ln|x|$.

- If the integrand involves something that we can't integrate but can differentiate, then use integration by parts.

- If the integral includes a term that will be "reduced" by differentiation, then use integration by parts.

U-substitution

$\int (x+3)(x-1)^5 dx$:

$$\begin{aligned}
&= \int (u+4)u^5 du && (u = x-1) \\
&= \int u^6 + 4u^5 du \\
&= \frac{u^7}{7} + \frac{2}{3}u^6 + c \\
&= \frac{(x-1)^7}{7} + \frac{2}{3}(x-1)^6 + c \\
&= (x-1)^6 \left(\frac{(x-1)}{7} + \frac{2}{3} \right) + c \\
&= \frac{1}{7}(x-1)^6 \left(x + \frac{11}{3} \right) + c
\end{aligned}$$

Can also be done using integration by parts:

$$\begin{aligned}
&\int (x+3)(x-1)^5 dx \\
&= \frac{1}{6}(x+3)(x-1)^6 - \frac{1}{6}\int (x-1)^6 dx + c && (uv - \int u'v dx) \\
&= \frac{1}{6}(x-1)^6 \left[(x+3) - \frac{1}{7}(x-1) \right] + c \\
&= \frac{1}{6}(x-1)^6 \left(\frac{6x}{7} + \frac{22}{7} \right) + c \\
&= \frac{1}{7}(x-1)^6 (x + \frac{11}{3}) + c
\end{aligned}$$

$\int \frac{x+5}{2x+3} dx$**:**

$$
\begin{aligned}
&= \frac{1}{2}\int \frac{u+7}{2u} du & (u = 2x+3; x = \frac{u-3}{2}; du = 2dx) \\
&= \frac{1}{2}\int \frac{u}{2} du + \frac{1}{2}\int \frac{7}{2u} du \\
&= \frac{u}{4} + \frac{7}{4}\ln|u| + c \\
&= \frac{2x+3}{4} + \frac{7}{4}\ln|2x+3| + c
\end{aligned}
$$

$\int \frac{x^2+4}{x+2} dx$**:**

$$
\begin{aligned}
&= \int \frac{(x+2)^2 - 4x}{x+2} dx \\
&= \int x+2 \ dx - \int \frac{4x}{x+2} dx \\
&= \frac{x^2}{2} + 2x - \int \frac{4u-8}{u} du + c & (u = x+2, x = u-2) \\
&= \frac{x^2}{2} + 2x - \int \frac{4u}{u} du + \int \frac{8}{u} du + c \\
&= \frac{x^2}{2} + 2x - 4x - 8 + 8\ln|x+2| + c \\
&= \frac{x^2}{2} - 2x - 8 + 8\ln|x+2| + c
\end{aligned}
$$

$\int \frac{(3+\ln x)^2(2-\ln x)}{4x}\ dx$**:**

slow way:

$$= \int \frac{(3+u)^2(2-u)}{4}\ du \qquad (u = \ln x,\ du = \frac{1}{x}\ dx)$$

$$= \frac{1}{4}\int (9+6u+u^2)(2-u)\ du$$ (Note: can just multiply this out because of the low power)

$$= \frac{1}{4}\int 18+12u+2u^2-9u-6u^2-u^3\ du$$

$$= \frac{1}{4}\int -u^3-4u^2+3u+18\ du$$

$$= \frac{1}{4}\left(\frac{-u^4}{4}-\frac{4u^3}{3}+\frac{3u^2}{2}+18u\right)$$

$$= -\frac{1}{4}\left(\frac{1}{4}(\ln x)^4-\frac{4}{3}(\ln x)^3+\frac{3}{2}(\ln x)^2+18\ln x\right)+c$$

$$= -\frac{1}{16}(\ln x)^4-\frac{1}{3}(\ln x)^3+\frac{3}{8}(\ln x)^2+\frac{9}{2}\ln x+c$$

faster way:

$$= \int \frac{u^2(5-u)}{4}\ du \qquad (u = \ln x,\ du = \frac{1}{x}\ dx)$$

$$= \frac{1}{4}\int 5u^2-u^3\ du$$

$$= \frac{1}{4}\left(\frac{5}{3}(3+\ln x)^3-\frac{1}{4}(3+\ln x)^4\right)+c$$

$\int_0^9 \sqrt{4-\sqrt{x}}\ dx$:

$$\begin{aligned}
&= -2\int_4^1 \sqrt{u}(4-u)\ du && (u = 4-\sqrt{x},\ du = -\frac{1}{2\sqrt{x}}\ dx)\\
&= 2\int_1^4 4u^{\frac{1}{2}} - u^{\frac{3}{2}}\ du\\
&= 2\left[\frac{8}{3}u^{\frac{3}{2}} - \frac{2}{5}u^{\frac{5}{2}}\right]_1^4 + c\\
&= 2\left[\left(\frac{8}{3}4^{\frac{3}{2}} - \frac{2}{5}4^{\frac{5}{2}}\right) - \left(\frac{8}{3} - \frac{2}{5}\right)\right]_1^4 + c\\
&= 2\left(\frac{64}{3} - \frac{64}{5} - \frac{8}{3} + \frac{2}{5}\right) + c\\
&= 2\left(\frac{56}{3} - \frac{62}{5}\right) + c\\
&= \frac{188}{15} + c
\end{aligned}$$

Note: if the substitution were $\sqrt{x}$

then we wouldn't get rid of the radical as:

$$\int_0^9 \sqrt{4-\sqrt{x}}\ dx = 2\int_0^3 \sqrt{4-u}(u)\ du \qquad (u = \sqrt{x})$$

$\int \sin 3x \cos 4x \; dx$**:**

$$\begin{aligned}
&= \frac{1}{4}\sin 3x \sin 4x - \frac{3}{4}\int \cos 3x \sin 4x \; dx \\
&= \frac{1}{4}\sin 3x \sin 4x - \frac{3}{4}\left[-\frac{1}{4}\cos 3x \cos 4x - \frac{3}{4}\int \sin 3x \cos 4x \; dx\right] \\
&= \frac{1}{4}\sin 3x \sin 4x + \frac{3}{16}\cos 3x \cos 4x + \frac{9}{16}\int \sin 3x \cos 4x \; dx \\
\iff \quad \frac{7}{16}\int \sin 3x \cos 4x \; dx &= \frac{1}{4}\sin 3x \sin 4x + \frac{3}{16}\cos 3x \cos 4x \\
\iff \quad \int \sin 3x \cos 4x \; dx &= \frac{4}{7}\sin 3x \sin 4x + \frac{3}{7}\cos 3x \cos 4x
\end{aligned}$$

Integration By Parts

Derivation

$$\begin{aligned}
& & \frac{d}{dx}(uv) &= \frac{du}{dx}v + u\frac{dv}{dx} \\
&\implies & uv &= \int v\frac{du}{dx} \; dx + \int u\frac{dv}{dx} \; dx \qquad \text{(integrating wrt. } x\text{)} \\
&\iff & uv &= \int u \; dv + \int v \; du \\
&\iff & \int u \; dv &= uv - \int v \; du
\end{aligned}$$

Usage

$$\begin{aligned}
\int f(x)\frac{dg}{dx}\ dx &= f(x)(g(x)+c) - \int (g(x)+c)\frac{df}{dx}\ dx \\
&= f(x)g(x) + cf(x) - \int g(x)\frac{df}{dx}\ dx + c\int \frac{df}{dx}\ dx \\
&= f(x)g(x) + cf(x) - \int g(x)\frac{df}{dx}\ dx + cf(x) \\
&= f(x)g(x) - \int g(x)\frac{df}{dx}\ dx
\end{aligned}$$

$\int x \sin x \cos x\ dx$

$$\begin{aligned}
& \text{(slow method)} \\
&= \cos(-x\cos x + \int \cos x\ dx) - \\
&\qquad \int -\sin x(-x\cos x + \int \cos x\ dx)\ dx + c \\
&= \cos(-x\cos x + \sin x) - \int -\sin x(-x\cos x + \sin x)\ dx + c \\
&= -x\cos^2 x + \sin x\cos x - \int x\sin x\cos x\ dx + \int \sin^2 x\ dx + c \\
&= \sin x\cos x - x\cos^2 x + \frac{1}{2}\int 1 - \cos 2x\ dx - \\
&\qquad \int x\sin x\cos x\ dx + c \\
&= \sin x\cos x - x\cos^2 x + \frac{1}{2}(x - \frac{1}{2}\sin 2x) - \int x\sin x\cos x\ dx + c \\
\iff \int x\sin x\cos x\ dx &= \frac{1}{2}\sin x\cos x - \frac{1}{2}x\cos^2 x + \frac{1}{4}x - \frac{1}{8}\sin 2x
\end{aligned}$$

(fast method)

$$\begin{aligned}
&= \frac{1}{2}x\sin^2 x - \frac{1}{2}\int \sin^2 x \ dx + c \\
&= \frac{1}{2}x\sin^2 x - \frac{1}{4}\int 1 - \cos 2x \ dx + c \\
&= \frac{1}{2}x\sin^2 x - \frac{1}{4}\left(x - \frac{1}{2}\sin 2x\right) + c \\
&= \frac{1}{2}x\sin^2 x - \frac{1}{4}x + \frac{1}{8}\sin 2x + c
\end{aligned}$$

(alternative fast method)

$$\begin{aligned}
&= \int x\left(\frac{1}{2}\sin 2x\right) \ dx \\
&= -\frac{1}{4}x\cos 2x + \frac{1}{4}\int \cos 2x \ dx + c \\
&= -\frac{1}{4}x\cos 2x + \frac{1}{8}\sin 2x + c \\
&= -\frac{1}{4}x(1 - 2\sin^2 x) + \frac{1}{8}\sin 2x + c
\end{aligned}$$

$\int \frac{\ln x}{x^5} \ dx$:

Note: we know how to differentiate $\ln x$

but not how to integrate it $\Longrightarrow$ integration by parts

$$\begin{aligned}
&= -\frac{1}{4}x^{-4}\ln x + \frac{1}{4}\int x^{-5} \ dx + c \\
&= -\frac{1}{4}x^{-4}\ln x + -\frac{1}{16}x^{-4} + c
\end{aligned}$$

$\int \arcsin 3x \;\; dx$**:**

$$\begin{aligned}
&= \int (1)(\arcsin 3x) \\
&= x \arcsin 3x - \int \frac{3x}{\sqrt{1-9x^2}} \; dx \\
&= x \arcsin 3x + \frac{1}{6} \int \frac{1}{\sqrt{u}} \; du \qquad\qquad (u = 1-9x^2, \; du = -18x \; dx) \\
&= x \arcsin 3x + \frac{1}{6}(2\sqrt{u}) + c \\
&= x \arcsin 3x + \frac{1}{3}\sqrt{1-9x^2} + c
\end{aligned}$$

Exponentials

$\int_0^1 \frac{3^x+4^x}{5^x} dx$**:**

$$\begin{aligned}
&= \int_0^1 \left(\frac{3}{5}\right)^x dx + \int_0^1 \left(\frac{4}{5}\right)^x dx \\
&= \frac{\left(\frac{3}{5}\right)^x}{\ln(\frac{3}{5})} + \frac{\left(\frac{4}{5}\right)^x}{\ln(\frac{4}{5})} \\
&= \frac{\frac{3}{5}-1}{\ln(\frac{3}{5})} + \frac{\frac{4}{5}-1}{\ln(\frac{4}{5})} \\
&= \frac{\frac{-2}{5}}{\ln(\frac{3}{5})} + \frac{\frac{-1}{5}}{\ln(\frac{4}{5})}
\end{aligned}$$

$\int 30e^{-3x}(1+3e^{-x})^5 \ dx$**:**

$$= \int 10e^{-2x}\Big(1+3e^{-x}\Big)^5(3e^{-x}) \ dx$$

$$= -10\int\left(\frac{u-1}{3}\right)^2 u^5 \ du \qquad \left(u = 1+3e^{-x} \iff e^{-x} = \frac{u-1}{3}; \ du = -3e^{-x}\right)$$

$$= -10/9\int\Big(u^2-2u+1\Big)\,u^5 \ du$$

$$= -10/9\int\Big(u^7-2u^6+u^5\Big) \ du$$

$$= -10/9\left(\frac{u^8}{8}-\frac{2u^7}{7}+\frac{u^6}{6}\right)+c$$

$$= -10/9\left(\frac{(1+3e^{-x})^8}{8}-\frac{2(1+3e^{-x})^7}{7} \quad +\frac{(1+3e^{-x})^6}{6}\right)+c$$

Trigonometric Functions

$\int (2+\tan x)^2 \ dx$**:**

$$= \int 4+4\tan x+\tan^2 x \ dx$$

$$= \int 4+4\tan x+(\sec^2 x-1) \ dx$$

$$= 4x+4\ln|\sec x|+\tan x-x+c$$

$$= 3x+4\ln|\sec x|+\tan x+c$$

$\int \sin^3 x \ dx$:

$$= \int (1-\cos^2 x)\sin x \ dx$$

$$= -\int 1-u^2 \ du \qquad\qquad (u=\cos x,\ du=-\sin x \ dx)$$

$$= \frac{u^3}{3} - u + c$$

$$= \frac{\cos^3 x}{3} - \cos x + c$$

$\int \frac{\cos^2 x}{1+\sin x} \ dx$:

$$= \int \frac{1-\sin^2 x}{1+\sin x} \ dx$$

$$= \int \frac{(1+\sin x)(1-\sin x)}{1+\sin x} \ dx$$

$$= \int 1-\sin x \ dx$$

$$= x + \cos x + c$$

$\int \frac{\sin x}{1+\sin x}\ dx$:

$$= \int \frac{\sin x(1-\sin x)}{(1+\sin x)(1-\sin x)}\ dx$$

$$= \int \frac{\sin x - \sin^2 x}{1-\sin^2 x}\ dx$$

$$= \int \frac{\sin x}{\cos^2 x}\ dx - \int \tan^2 x\ dx$$

$$= \int \sec x \tan x\ dx - \int \sec^2 x - 1\ dx$$

$$= \sec x - \tan x - x + c$$

$\int (\csc 3x + \cot 3x)^2\ dx$:

$$= \int \csc^2 3x + 2\csc 3x \cot 3x + \cot^2 3x\ dx$$

$$= \int \csc^2 3x + 2\int \csc 3x \cot 3x + \int \csc^2 3x - 1\ dx$$

$$= 2\int \csc^2 3x + 2\int \csc 3x \cot 3x - \int 1\ dx$$

$$= 2(-\frac{\cot 3x}{3})) + 2(-\frac{\csc 3x}{3})) - x + c\ dx$$

$$= \frac{-2}{3}(\csc 3x + \cot 3x) - x + c$$

$\int \tan^5 x \ dx$:

$$= \int \tan^3 x(\sec^2 x - 1) \ dx$$

$$= \int \tan^3 x \sec^2 x \ dx - \int \tan^3 x \ dx$$

$$= \int \tan^3 x \sec^2 x \ dx - \int \tan x(\sec^2 -1) \ dx$$

$$= \int \tan^3 x \sec^2 x \ dx - \int \tan x \sec^2 \ dx - \int \tan x \ dx$$

$$= \frac{1}{4} \tan^4 x - \frac{1}{2} \tan^2 x - \ln|\sec x| + c$$

$\int \sec x\sqrt{\sec x + \tan x} \ dx$:

$$= \int \frac{\sec x\sqrt{\sec x + \tan x}}{\sec x(\sec x + \tan x)} \ dx \quad (u = \sec x + \tan x,\ du = \sec x \tan x + \sec^2 x)$$

$$= \int \frac{\sqrt{u}}{u} \ du$$

$$= \int \frac{1}{\sqrt{u}} \ du$$

$$= 2u^{\frac{1}{2}} + c$$

$$= 2\sqrt{\sec x + \tan x} + c$$

$\int \frac{\sin 2x - \cos 2x}{\sin 2x + \cos 2x}\ dx$**:**

wrong way:

$$= \int \frac{(\sin 2x - \cos 2x)(\sin 2x + \cos 2x)}{(\sin 2x + \cos 2x)^2}\ dx$$

$$= \int \frac{\sin^2 2x - \cos^2 2x}{2 \sin 2x \cos 2x}\ dx \qquad \left(= \int \frac{f(x)}{\frac{1}{2}f'(x)}\ dx\right) \text{ Wrong!}$$

another wrong way:

$$= \frac{1}{2} \int u \frac{dx}{du}\ dx \text{ Wrong!} \qquad (u = \sin 2x - \cos 2x)$$

right way:

$$= -\frac{1}{2} \int \frac{1}{u} \frac{du}{dx}\ dx \qquad (u = \sin 2x + \cos 2x)$$

$$= -\frac{1}{2} \int \frac{1}{u} \frac{du}{dx}\ dx \qquad (u = \sin 2x + \cos 2x)$$

$$= -\frac{1}{2} \int \frac{1}{u} du\ dx \qquad (u = \sin 2x + \cos 2x)$$

$$= -\frac{1}{2} \ln |u| + c$$

$$= -\frac{1}{2} \ln |\sin 2x + \cos 2x| + c$$

Trig-substitution

$\int_1^b \frac{\sqrt{x^2+1}}{x}dx$:

$$
\begin{aligned}
&\int_1^b \frac{\sqrt{x^2+1}}{x}dx \\
&= \int_1^b \frac{\sqrt{\tan^2\theta+1}}{\tan\theta}\ d\tan\theta \\
&= \int_{\arctan 1}^{\arctan b} \frac{\sec^3\theta}{\tan\theta}\ d\theta \\
&= \int_{\arctan 1}^{\arctan b} \frac{\sec\theta}{\tan\theta}(1+\tan^2\theta)\ d\theta \\
&= \int_{\arctan 1}^{\arctan b} \frac{\sec\theta}{\tan\theta}\ d\theta + [\sec\theta]_{\arctan 1}^{\arctan b} \\
&= \int_{\arctan 1}^{\arctan b} \frac{\sec\theta}{\tan\theta}\ d\theta + (\sqrt{b^2+1}-\sqrt{2}) \qquad\qquad (wrt.\ \theta : opp = b, adj = 1, hyp = \sqrt{b^2+1}) \\
&= \int_{\arctan 1}^{\arctan b} \csc\theta\ d\theta + (\sqrt{b^2+1}-\sqrt{2}) \\
&= [-\ln|\csc\theta+\cot\theta|]_{\arctan 1}^{\arctan b} + \sqrt{b^2+1}-\sqrt{2} \\
&= \left[\left(-\ln\left|\frac{\sqrt{b^2+1}}{b}+\frac{1}{b}\right|\right) - \left(-\ln\left|\sqrt{2}+1\right|\right)\right] \\
&\qquad + \sqrt{b^2+1}-\sqrt{2} \\
&= \ln|b| - \ln\left|\sqrt{b^2+1}+1\right| + \ln\left|\sqrt{2}+1\right| \\
&\qquad + \sqrt{b^2+1}-\sqrt{2}
\end{aligned}
$$

Limits

Limits

$\lim_{x\to\infty}\left[(x^3+x^2)^{\frac{1}{3}}-x\right]$

(tags: finding limits, difference of cubes)

$$\text{Using }\left(a^3-b^3\right)=(a-b)\left(a^2+b^2+ab\right):$$

$$\begin{aligned}
\left[\left(x^3+x^2\right)^{\frac{1}{3}}-x\right] &= \left[\left(x^3+x^2\right)^{\frac{1}{3}}-x\right]\cdot\frac{\left[(x^3+x^2)^{\frac{2}{3}}+x^2+x\,(x^3+x^2)^{\frac{1}{3}}\right]}{\left[(x^3+x^2)^{\frac{2}{3}}+x^2+x\,(x^3+x^2)^{\frac{1}{3}}\right]}\\
&= \frac{(x^3+x^2)-x^3}{(x^3+x^2)^{\frac{2}{3}}+x^2+x\,(x^3+x^2)^{\frac{1}{3}}}\\
&= \frac{x^2}{(x^3+x^2)^{\frac{2}{3}}+x^2+x\,(x^3+x^2)^{\frac{1}{3}}}\\
&= \frac{\frac{1}{x^2}}{\frac{1}{x^2}}\cdot\frac{x^2}{(x^3+x^2)^{\frac{2}{3}}+x^2+x\,(x^3+x^2)^{\frac{1}{3}}}\\
&= \frac{1}{\left(1+\frac{1}{x}\right)^{\frac{2}{3}}+1+\frac{1}{x}\,(x^3+x^2)^{\frac{1}{3}}}\\
&= \frac{1}{\left(1+\frac{1}{x}\right)^{\frac{2}{3}}+1+\left(1+\frac{1}{x}\right)^{\frac{1}{3}}}\\
\therefore \lim_{x\to\infty}\left[\left(x^3+x^2\right)^{\frac{1}{3}}-x\right] &= \lim_{x\to\infty}\frac{1}{\left(1+\frac{1}{x}\right)^{\frac{2}{3}}+1+\left(1+\frac{1}{x}\right)^{\frac{1}{3}}}\\
&= \frac{1}{3}
\end{aligned}$$

$\frac{1-\cos 2x}{2x^2}$

(tags: finding limits, taylor series)

For the function,

$g(x) = \begin{cases} 1 & x = 0 \\ \frac{1-\cos 2x}{2x^2} & x \neq 0 \end{cases}$

using the definition of the derivative and the Taylor series for cosine, find g′(0).

$g'(0) = \lim_{x \to 0} \frac{g(x) - g(0)}{x - 0} = \lim_{x \to 0} \frac{\frac{1-\cos 2x}{2x^2} - 1}{x}$

Taylor series for cos(2x)

Taylor Series

Derivation of Taylor's Theorem

Rolle's Theorem

Taken from `https://en.wikipedia.org/wiki/Rolle%27s_theorem#Standard_version_of_the_theorem`

If a real-valued function f is continuous on a closed interval $[a, b]$ and differentiable on the open interval (a, b) and $f(a) = f(b)$, then there exists at least one $c \in (a, b)$ such that $f'(c) = 0$.

Mean Value Theorem

Based on `https://en.wikipedia.org/wiki/Mean_value_theorem#Proof`

If a real-valued function f is continuous on a closed interval $[a, b]$ and differentiable on the open interval (a, b) and $f(a) \neq f(b)$, then we can define a number $M \in \mathbb{R}$ such that,

$$f(b) = f(a) + M(b - a)$$

then let $g(x) = f(x) - f(a) - M(x - a)$ so that $g'(x) = f'(x) - M$. Now, since by the definition of M, $g(a) = g(b) = 0$, we can apply Rolle's theorem so that,

$$\begin{aligned}
g'(c) &= 0 \text{ for some } c \in (a,b) \\
\implies 0 &= f'(c) - M \\
\iff M &= f'(c) \\
\therefore f(b) &= f(a) + f'(c)(b-a) \text{ for some } c \in (a,b)
\end{aligned}$$

Taylor's Theorem

Taken from *Walter Rudin, Principles of Mathematical Analysis.*

Suppose f is a real-valued function on $[a,b]$, n, is a positive integer, $f^(n-1)$ is continuous on $[a,b]$, $f^(n)$ exists for every $t \in (a,b)$. Let α, β be distinct points of [a, b], and define

$$P(t) = \sum_{k=0}^{n-1} \frac{f^{(k)}(\alpha)}{k!}(t-\alpha)^k.$$

Then there exists a point between α and β such that

$$f(\beta) = P(\beta) + \frac{f^{(n)}(x)}{n!}(\beta-\alpha)^n.$$

Note that if $n = 0$ this degenerates to the Mean Value Theorem:

$$\begin{aligned}
f(\beta) &= \sum_{k=0}^{0} \frac{f^{(k)}(\alpha)}{k!}(t-\alpha)^k + \frac{f^{(1)}(x)}{1!}(\beta-\alpha)^1 \\
&= \frac{f^{(0)}(\alpha)}{0!}(t-\alpha)^0 + \frac{f^{(1)}(x)}{1!}(\beta-\alpha)^1 \\
&= f(\alpha) + f'(x)(\beta-\alpha)
\end{aligned}$$

Proof

Let M be the number defined by

$$f(\beta) = P(\beta) + M(\beta-\alpha)^n$$

and put

$$g(t) = f(t) - P(t) - M(t-\alpha)^n \qquad (a \leq t \leq b).$$

We have to show that $n!M = f^{(n)}(x)$ for some x between α and β. Taking the nth derivative of $g(t)$,

$$g^{(n)}(t) = f^{(n)}(t) - n!M \qquad (a < t < b).$$

The proof will be complete if we can show that $g^{(n)}(x) = 0$ for some x between α and β. Since $P^{(k)}(\alpha) = f^{(k)}(\alpha)$ for $k = 0, \ldots, n-1$ we have

$$g(\alpha) = g'(\alpha) = \ldots = g^{(n-1)}(\alpha) = 0.$$

Our choice of M shows that $g(\beta) = 0$, so that $g'(x_1) = 0$ for some $x_1 \in (\alpha, \beta)$ by the Mean Value Theorem. Since $g'(\alpha) = 0$ we conclude similarly that $g''(x_2) = 0$ for some $x_2 \in (\alpha, \beta)$. After n steps we arrive at the conclusion that $g^{(n)}(x_n) = 0$ for some $x_n \in (\alpha, x_{n-1})$, that is, between α and β.

Examples of Taylor Series

$\cos x$ for x close to 0

Note: Taylor series at zero are also called Maclaurin series.

$$\begin{aligned}\cos x &= \cos 0 + (-\sin 0)x + \frac{(-\cos 0)}{2!}x^2 + \ldots \\ &= 1 - \frac{x^2}{2} + \ldots\end{aligned}$$

$\cos 2h$ for h close to 0

$$\cos 2h \approx 1 - \frac{(2h)^2}{2} = 1 - 2h^2$$

Note that if we choose to differentiate wrt. h rather than (2h) then we get the same result,

$$\begin{aligned}\cos 2h &= \cos 0 + (-2\sin 0)h + \frac{(-4\cos 0)}{2!}h^2 + \ldots \\ &= 1 - 2h^2 + \ldots\end{aligned}$$

Finite Maclaurin Series and the Binomial Theorem

Further Calculus exam notes

Verify that $\int_0^1 \sin x^p dx$ is convergent for all p.

(tags: convergence)

$p = 0$: When $p = 0$ the integral is constant and so the integral is convergent in this case.

$p \neq 0$: For the cases where $p \neq 0$, we make the substitution $y = x^p$ so that $x = y^{\frac{1}{p}}$ and $dx = \frac{1}{p}y^{\frac{1}{p}-1}$ to see that:

When $p > 0$, we have

$$\int_0^1 \sin{(x^p)} dx = \frac{1}{p}\int_0^1 \sin{(y)} y^{\frac{1}{p}-1} dy$$

We now note that near $y = 0$, the integrand is positive and, if we compare with $y^{\frac{1}{p}}$, then we have

$$\lim_{y \to 0^+} \frac{\sin y}{y} = 1$$

and so, as $p > 0 \implies \frac{1}{p} > 0$ and so the integral

$$\int_0^1 y^{\frac{1}{p}} dy$$

is convergent, by the LCT, the given integral is convergent.

When $p < 0$, we have

$$\int_0^1 \sin x^p dx = \frac{1}{p}\int_\infty^1 \sin(y) y^{\frac{1}{p}-1} dy = -\frac{1}{p}\int_1^\infty \sin(y) y^{\frac{1}{p}-1} dy$$

Since, for all $y \geq 1$

$$|\sin(y) y^{\frac{1}{p}-1}| \leq y^{\frac{1}{p}-1}$$

and so, as $p < 0$ we have

$$\int_1^\infty y^{\frac{1}{p}-1} dy = \left[p y^{\frac{1}{p}}\right]_1^\infty = p$$

which is finite and so the given integral is absolutely convergent.

Show that, for $\beta > 0$, the function $f(t) = t^\beta \ln t$ is of exponential growth at most γ for any $\gamma > 0$

(tags: exponential growth)

Need to show that for any $\gamma > 0$

$$|t^\beta \ln t| \leq M e^{\gamma t}$$

for some $M > 0$. First note that for any $\gamma > 0$,

$$\begin{aligned}\lim_{t\to\infty} \frac{t^\beta \ln t}{e^{\gamma t}} &= \left(\lim_{t\to\infty} \frac{t^\beta}{e^{\frac{\gamma t}{2}}}\right)\left(\lim_{t\to\infty} \frac{\ln t}{e^{\frac{\gamma t}{2}}}\right) \\ &= \left(\lim_{t\to\infty} \frac{\beta!}{\left(\frac{\gamma}{2}\right)^\beta e^{\frac{\gamma t}{2}}}\right)\left(\lim_{t\to\infty} \frac{1}{t\left(\frac{\gamma}{2}\right) e^{\frac{\gamma t}{2}}}\right) \\ &= (0)(0) = 0\end{aligned}$$

This means that there is some value of t, say T, which, if $t > T$, then

$$t^\beta \ln t < e^{\gamma t}$$

Note, in this question $f(t) = 0$ as a continuity "fix". In addition to that $t^\beta \ln t$ is continuous for $t \geq 0$ as t^β and $\ln t$ are both continuous for $t > 0$. This means that for $0 \leq t \leq T$ we can find the maximum value of $|f(t)|$ over this interval and denote it M_T. Then, since $e^{\gamma t} \geq 1$ for any $t \geq 0$ we have,

$$|f(t)| \leq Me^{\gamma t}$$

where $M = max 1, M_T$. Consequently, for $t \geq 0$, $f(t)$ does indeed have exponential growth at most γ for any $\gamma > 0$.