$2\langle 1, 2\rangle$

Advanced Linear Algebra - Valenza, 2017

Trevor Klar

January 23, 2018

1 Functions

Theorem. **(1.4)** *a function $f : S \to T$ is invertible iff it is bijective.*

2 Groups and group homomorphisms

For a nonempty set S, a *binary operation* on S is a function

$$S \times S \to S$$

$$(s, t) \mapsto s \star t \text{ , where } s, t \in S$$

Basically, you take two numbers, and do something to them to get a third number, acccording to a rule.

Definition. We say that the binary operation $\star$ is *associative* if:

$$(s \star t) \star u = s \star (t \star u)$$

For any $s, t, u \in S$.

Definition. We say that the binary operation $\star$ is *commutative* if:

$$s \star t = t \star s$$

For any $s, t \in S$.

Definition. We say that an element $e \in S$ is an *identity* for $\star$ if $e \star s = s = s \star e \quad \forall s \in S$.

Definition. A group $(G, \star)$ is a pair where G is a nonempty set and $\star$ is a binary operator on G such that

1. $\star$ is associative (associative axiom).
2. $\exists e \in G$ that is an identity under $\star$ (identity axiom).
3. $\forall s \in G$, $\exists t \in G$ such that $s \star t = e = t \star s$ (inverse axiom).

Definition. A group is called *commutative* or *abelian* if

$$s \star t = t \star s \quad \forall s, t \in G.$$

2.1 General Properties of Groups

Definition. (Cancellation Property)
Suppose $(G, \star)$ is a group and $s, t, u \in G$. Then

$$st = su \implies t = u$$

$$st = ut \implies s = u$$

(note: st means $s \star t$.)

Proposition. *Suppose $(G, \star)$ is a group. Then,*

1. *The identity element e in G is unique.*

   Proof $e = ee' = e'$, so $e = e'$ ■

2. *For any $s \in G$, the inverse of s is unique. (And we denote it s^{-1}.)*

   Proof Suppose $t, u \in G$ such that $ts = e$ and $us = e$. Then $ts = us$, so $t = u$ by cancellation. ■

3. *If $st = e$, then s is the inverse of t (and t is the inverse of s).*

   Proof

   $$st = e$$

   $$tst = te = t$$

   $$tst = (ts)t$$

   so,

   $$(ts)t = t$$

   $$ts = e, \text{ by cancellation.}$$

   ■

4. $\forall s \in G, (s^{-1})^{-1} = s.$

5. $\forall s, t \in G, (st)^{-1} = t^{-1}s^{-1}$

   Proof

$$(st)^{-1}(st) = e$$
$$(st)^{-1}(st)t^{-1} = et^{-1}$$
$$(st)^{-1}(ss^{-1} = t^{-1}s^{-1}$$
$$(st)^{-1} = t^{-1}s^{-1}$$

■

6. *If $s \in G$, then $ss = s \iff s = e$.*

Definition. Suppose $(G, \star)$ is a group, and H is a subset of G. We say H is a *subgroup* of G if $(H, \star)$ is a group.

This means:

- $\star$ is a binary operator on H, that is, H is closed under $\star$
- $\star$ is associative for elements in H. (Clearly, since this also hold for all of G)
- There is an identity e' in H such that $e'h = h = he'$ for any $h \in H$.
- Every element $s \in H$ has an inverse in H, i.e. there should be an element $t \in H$ such that $s \star t = e = t \star s$.

  Remark 2.1. t is the same as the inverse of s taken in G. (We leave the proof as an excercise.)

Proposition. ***(Subgroup criterion)*** *Suppse $(G, \star)$ is a group, and H is a* nonempty *subset of G. Then*

$$H \text{ is a subgroup of } G \iff \text{for any } s, t \in H, \quad s \star t^{-1} \in H.$$

Example. Consider the group $(\mathbb{Z}, +)$. For any $n \in \mathbb{Z}^+$,
$n\mathbb{Z} = \{nz : z \in \mathbb{Z}\} = \{\text{all integer multiples of } n\}$.
$1n \in n\mathbb{Z}$, so $n\mathbb{Z} \neq \emptyset$.
Now, apply the subgroup criterion:
Take any two elements $s, t \in \mathbb{Z}$.
then $s = na$ and $t = nb$, where $a, b \in \mathbb{Z}$
so $s + (-t) = na - nb = n(a - b) \in n\mathbb{Z}$.
Therefore, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Exercise 2.1. Prove that $I' := \{f \in \mathscr{C}^0(\mathbb{R}) : f(0) = 1\}$ is *not* a subgroup of $\mathscr{C}^0(\mathbb{R})$.

2.2 Group homomorphisms

Definition. Suppose $(G_1, \star_1), (G_2, \star_2)$ are groups. A funcion $f : G_1 \to G_2$ is called a *group homomorphism* if:

$$\forall s, t \in G_1, \quad f(s \star_1 t) = f(s) \star_2 f(t)$$

Example. Consider the group $(\mathbb{Z}, +)$. The function $f : \mathbb{Z} \to \mathbb{Z}$ where $n \mapsto 3n$ is a group homomorphism.

Proof Take any $s, t \in \mathbb{Z}$. We want $f(s+t) = f(s) + f(t)$.

$$f(s+t) = 3(s+t) = 3s + 3t = f(s) + f(t)$$

This completes the proof. ■

Properties of group homomorphisms:

Proposition. *Suppose $f : G_1 \to G_2$ is a group homomorphism. Then,*

(i) $f(e_1) = e_2$

Proof $f(e_1) = f(e_1 e_1) = f(e_1) f(e_1)$.
Then, by cancellation, $e_2 = f(e_1)$. ■

(ii) For any $s \in G$, $\quad f(s^{-1}) = (f(s))^{-1}$

Proof We need to prove that $f(s^{-1})$ is the inverse of $f(s)$. It suffices to prove that $f(s^{-1}) f(s) = e_2$.
$f(s^{-1}) f(s) = f(s^{-1} s) = f(e_1) = e_2$. ■

Definition. If $\phi : H \to G$ is a bijective function from the group H to the group G, then we say it is a *group isomorphism* and write $G \cong H$.

Lemma 2.2. *If $\phi : G \to H$ is a group isomorphism, then $\phi^{-1} : H \to G$ is also a group isomorphism.*

Proposition. *Given group homomorphisms $\phi : G \to H$, $\psi : H \to I$, the composition $\psi\phi : G \to I$ is also a group homomorphism.*

Corollary 2.3. *If ψ, ϕ above are both isomorphisms, then $\psi\phi$ is also a group isomorphism.*

Definition. Suppose we have a function $f : S \to T$.

- For any $t \in T$, the *inverse image* (or the *preimage*) of t, denoted $f^{-1}(t)$, is the set

$$f^{-1}(t) \equiv \{x \in S : f(x) = t\}$$

- For any subset $W \subset T$, the *inverse image* (or the *preimage*) of t, denoted $f^{-1}(W)$, is the set

$$f^{-1}(W) \equiv \{x \in S : f(x) \in W\}$$

Definition. Given a group homomorphism $\phi : G \to H$,

- the *kernel* o fϕ is

$$\ker \phi := \{x \in G : \phi(x) = e_H\} = \phi^{-1}(e_H)$$

- the *image* of ϕ is

$$\text{im } \phi := \{\phi(x) : x \in G\}$$

Proposition. *For a group homomorphism $\phi : G \to H$,*

$$\ker \phi \textit{ is a subgroup of } G,$$
$$\textit{im } \phi \textit{ is a subgroup of } H.$$

Lemma 2.4. *For a group homomorphism $\phi : G \to H$, then*

$$\phi \textit{ is injective} \iff \ker \phi = \{e_G\}$$

Definition. Let G_0, G_1 be groups. The *direct product* of G_0 and G_1 is the set

$$G_0 \times G_1 = \{(s_0, s_1) : s_0 \in G_0, s_1 \in G_1\}$$

equipped with an operation on $G_0 \times G_1$ as follows:

$$(s_0, s_1)(t_0, t_1) = (s_0 t_0, s_1 t_1) \quad \forall s_0, t_0 \in G_0, s_1, t_1 \in G_1$$

This is just the Cartesian product of the two sets G_0 and G_1, equipped with the same operations, applied componentwise.

Definition. Let G_0, G_1 be groups. A *projection map* is a function

$$\begin{aligned} \rho_0 : G_0 \times G_1 &\to G_0 \\ (s_0, s_1) &\mapsto s_0 \end{aligned}$$

Definition. Consider the special case of the direct product $G \times G$ of a group G with itself. Define a subset D of $G \times G$ by

$$D = \{(s, s) : s \in G\}$$

That is, D consists of all elements with both coordinates equal. This is called the *diagonal subgroup.*

2.3 Rings and Fields

Definition. A *ring* is a triple $(A, +_A, \bullet_A)$, where A is a nonempty set, $+_A$ is some 'addition' operation, and $\bullet$ is some 'multiplication' operation such that:

- $(A, +_A)$ is an abelian group. (We use additive notation for the inverse and identity of this operation)
- $(A, \bullet_A)$ is a "monoid", that is, $\bullet_A$ has the associative and identity properties, but not necessarily the inverse property or the commutative property.
- $\bullet_A$ distributes over $+_A$ from the right and the left (distributive property).

Definition. If $\bullet_A$ is also commutative, then we say A is a *commutative ring.* We often write ab to denote $a \bullet_A b$.

If k is a commutative ring, $k* := k - \{0_k\}$.

Definition. A commutative ring k where $(k*, \bullet_k)$ is a group is called a field. (That is, it is a ring where $\bullet$ has commutativity and an inverse)

Proposition. *Suppose* $(A, +, \bullet)$ *is a ring. Then,* $\forall a, b \in A$,

1. $0a = 0 = a0$
2. *a(-b)=-(ab)=(-a)b*
3. *(-a)(-b)=ab*
4. *(-1)a=-a*
5. *(-1)(-1)=1*

3 Vector Spaces and Linear Transformations

3.1 Vector Spaces and Subspaces

Fix a field k (e.g. $\mathbb{R}, \mathbb{C}, \mathbb{Q} etc.$)

Definition. A *vector space over* k (or a k-*vector space*) is a set V, together with a binary opeation $+$ on V, and a *scalar multiplication.*

Vector fields have the following properties:
$\forall \lambda, \mu \in k, \forall v, w \in V$,

(i) $(V, +)$ is an abelian group.

(ii) $(\lambda\mu)\vec{v} = \lambda(\mu)\vec{v}$
That is, scalar multiplication is associative.

(iii) $(\lambda + \mu)\vec{v} = \lambda\vec{v} + \mu\vec{v}$
That is, vectors distribute over scalars.

(iv) $\lambda(\vec{v} + \vec{w}) = \lambda\vec{v} + \lambda\vec{w}$
That is, scalars distribute over vectors.

(v) $1_k\vec{v} = \vec{v}$
That is, the identity of the field is also the identity of the vector space.

Proposition 3.1. *Let V be a vector space over a field k. Then the following assertions hold:*

(i) $\lambda\vec{0} = \vec{0} \quad \forall \lambda \in k$

(ii) $0\vec{v} = \vec{0} \quad \forall \vec{v} \in V$

(iii) $(-\lambda)\vec{v} = -(\lambda\vec{v}) \quad \forall \lambda \in k, \vec{v} \in V$

(iv) $\lambda\vec{v} = \vec{0} \iff (\lambda = 0 \text{ or } v = \vec{0}) \quad \forall \lambda \in k, \vec{v} \in V$

Definition. A subset W of a vector space V over a field k is called a *subspace of* V if it constitutes a vector space over k in its own right with respect to the additive and scalar operations defined on V.

Proposition 3.2. ***(Subspace Criterion)*** *Let W be a <u>nonempty</u> subset of the vector space V. Then W is a subspace of V if and only if it is closed under addition and scalar multiplication.*

Definition. Let $v_1 \ldots, v_n$ be a family of vectors in the vector space V defined over a field k. Then an expression of the form

$$\lambda_1\vec{v_1} + \lambda_2\vec{v_2} + \ldots + \lambda_n\vec{v_n} \quad (\lambda_1, \lambda_2, \ldots \lambda_n \in k)$$

is called a *linear combination* of the vectors $v_1 \ldots, v_n$. The set of all such linear combinations is called the *span* of $v_1 \ldots, v_n$ and denoted $\mathrm{Span}(v_1 \ldots, v_n)$.

Proposition 3.3. *Let $v_1 \ldots, v_n$ be a family of vectors in the vector space V defined over a field k. Then $W =$Span$(v_1 \ldots, v_n)$ is a subspace of V.*

3.2 Linear Transformations

Definition. Let V and V' be vector space over a common field k. Then a function $V \to V'$ is called a *linear transformation* if it satisfies the following conditions:

(i) $T(v+w) = T(v) + T(w) \quad \forall v, w \in V$

(ii) $T(\lambda v) = \lambda T(v) \quad \forall v \in V, \lambda \in k$

One also says that T is *k-linear* or a *vector space homomorphism.*

Note that the first condition states that T is a homomorphism of additive groups, and therefore all of our previous theory of group homomorphisms applies. In particular, we have the following derived properties:

(iii) $T(\vec{0}) = \vec{0}$

(iv) $T(-\vec{v}) = -T(\vec{v}) \quad \forall v \in V$

Proposition 3.4. *The composition of linear transformations is a linear transformation.*

Proposition 3.5. *The kernel and image of a linear transformation are subspaces of their ambient vector spaces.*

Definition. A bijective linear transformation $T : V \to V'$ is called an *isomorphism* of vector spaces.

4 •

Theorem 4.1. *In any vector space,*

- *Every linearly independent set of vectors can be extended to a basis.*
- *Every spanning set can be contracted to a basis.*
- *Every vector space has a basis*

Corollary 4.2. *Suppose V is a finite-dimensional k-vector space with* $\dim(V) = n$. *Then,*

- *No subset of V with more than n vectors can be linearly independent.*
- *No subset of V with less than n vectors can span V.*

Proof (i) Suppose $\mathscr{B}$ is a collection of ℓ vectors in V, and suppose $\ell > n$. Suppose also that $\mathscr{B}$ is linearly independent. By part (i) of the Thm, $\mathscr{B}$ can be extended to a basis $\mathscr{B}'$ for V.

$$\ell = |\mathscr{B}| \leq |\mathscr{B}'| = n$$

which is a contradiction. ∎

Corollary 4.3. *Suppose V has dimension n and S is a collection of n vectors in V. The following are equivalent:*

- *S is linearly independent.*
- *S spans V.*
- *S is a basis for V.*