Chapter 10

Infinite Groups

The groups we have carefully studied so far are finite groups. In this chapter, we will give a few examples of infinite groups, and revise some of the concepts we have seen in that context.

Let us recall a few examples of infinite groups we have seen:

- the group of real numbers (with addition),
- the group of complex numbers (with addition),
- the group of rational numbers (with addition).

Instead of the real numbers $\mathbb{R}$, we can consider the real plane $\mathbb{R}^2$. Vectors in $\mathbb{R}^2$ form a group structure as well, with respect to addition! Let us check that this is true. For that, we check our 4 usual properties: (1) the sum of two vectors is a vector (closure), (2) addition of vectors is associative, (3) there is an identity element, the vector $(0, 0)$, and (4) every vector $(x_1, x_2) \in \mathbb{R}^2$ has an inverse, given by $(-x_1, -x_2)$, since

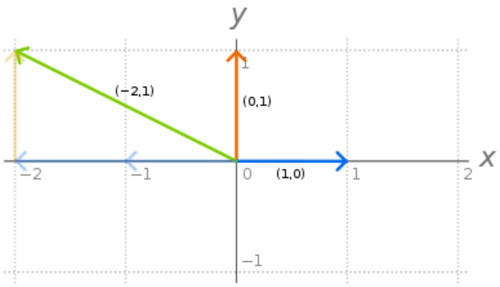
$$(x_1, x_2) + (-x_1, -x_2) = (0, 0).$$

Examples of Infinite Groups

- The real numbers
- The complex numbers
- The rational numbers

Anything else?

The 2-dimensional Real Plane



http://upload.wikimedia.org/wikipedia/commons/thumb/9/9a/Basis_graph_%28no_label%29.svg/400px-Basis_graph_%28no_label%29.svg.png

The example that we just saw with $\mathbb{R}^2$ is a special case of a vector space. Vector spaces are objects that you might have seen in a linear algebra course. Let us recall the definition of a vector space.

Definition 19. A set V is a vector space over a field (for us, we can take this field to be $\mathbb{R}$) if for all $u, v, w \in V$

1. $u + v \in V$ (closure property),
2. $u + v = v + u$ (commutativity),
3. $u + (v + w) = (u + v) + w$ (associativity),
4. there exists $0 \in V$ such that $u + 0 = 0 + u$,
5. there exists $-v$ such that $(-v) + v = 0$

and for all $x, y \in \mathbb{R}$ we have

1. $x(u + v) = xu + xv$,
2. $(x + y)u = xu + xu$,
3. $x(yu) = (xy)u$
4. $1u = u$, where 1 is the identity of $\mathbb{R}$.

We recognize that the first axioms of a vector space V are in fact requesting V to be an Abelian group!

Example 38. The n-dimensional real space $\mathbb{R}^n = \{(x_1, x_2, \ldots, x_n) \,|x_i \in \mathbb{R},\ i = 1, \ldots, n\}$ is a vector space over the reals.

Example 39. We already know that the set $\mathbb{C}$ of complex numbers forms a group. Now

$$\mathbb{C} = \{x + iy | x, y \in \mathbb{R}\}$$

is a vector space over $\mathbb{R}$, which gives another proof that $\mathbb{C}$ forms a group under addition.

Definition of Vector Space

A set V of vectors, a set F (field, say the real numbers) of scalars.

- **Associativity** of vector addition: $\mathbf{v_1} + (\mathbf{v_2} + \mathbf{v_3}) = (\mathbf{v_1} + \mathbf{v_2}) + \mathbf{v_3}$.
- **Commutativity** of vector addition: $\mathbf{v_1} + \mathbf{v_2} = \mathbf{v_2} + \mathbf{v_1}$.

We recognize the group definition!

- **Identity element** of vector addition: there exists $\mathbf{0} \in V$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v}$ for all $\mathbf{v} \in V$.
- **Inverse elements** of vector addition: for all $\mathbf{v} \in$ V, there exists $\mathbf{-v} \in V$ such that $\mathbf{v} + (\mathbf{-v}) = \mathbf{0}$.
- **Distributivity** of scalar multiplication w/r vector addition: $n(\mathbf{v_1} + \mathbf{v_2}) = n\mathbf{v_1} + n\mathbf{v_2}$.
- **Distributivity** of scalar multiplication w/r field addition : $(n_1 + n_2)\mathbf{v} = n_1\mathbf{v} + n_2\mathbf{v}$.
- Respect of scalar multiplication over field multiplication: $n_1 (n_2\, \mathbf{v}) = (n_1\, n_2)\mathbf{v}$.
- Identity element of scalar multiplication: $1\mathbf{v} = \mathbf{v}$, where 1 = multiplicative identity in F.

Definition of Vector Space Revisited

The word field can be easily replaced by real numbers if you don't know it.

A set V of vectors, a set F (field, say the real numbers) of scalars.

- **Vectors form an abelian group with respect to addition.**
- **Inverse elements** of vector addition: for all $\mathbf{v} \in$ V, there exists $\mathbf{-v} \in V$ such that $\mathbf{v} + (\mathbf{-v}) = \mathbf{0}$.
- **Distributivity** of scalar multiplication w/r vector addition: $s(\mathbf{v_1} + \mathbf{v_2}) = s\mathbf{v_1} + s\mathbf{v_2}$.
- **Distributivity** of scalar multiplication w/r field addition : $(n_1 + n_2)\mathbf{v} = n_1\mathbf{v} + n_2\mathbf{v}$.
- Respect of scalar multiplication over field multiplication: $n_1 (n_2\, \mathbf{s}) = (n_1\, n_2)\mathbf{s}$.
- Identity element of scalar multiplication: $1\mathbf{s} = \mathbf{s}$, where 1 = multiplicative identity in F.

A vector space is thus an Abelian group. What is the order of this group? It's infinity!

Now we might wonder what are the subgroups of this group. They are in fact subspaces, as follows from the definition of a subspace.

Definition 20. Let V be a vector space over some field F and U be a subset of V. If U is a vector space over F under the operations of V (vector addition and multiplication by elements of F), then U is called a subspace of V.

Let us recall the definition of a basis of a vector space.

Definition 21. A basis of V is a set of **linearly independent** vectors of V such that every element v is a linear combination of the vectors from this set.

Example 40. The set $\{(1,0),(0,1)\}$ is a basis of the two-dimensional plane $\mathbb{R}^2$. This means that every vector $x \in \mathbb{R}^2$ can be written as

$$x = x_1(1,0) + x_2(0,1),\ \ x_1, x_2 \in \mathbb{R}.$$

Now let us think of what happens in the above example if we keep the two basis vectors $(1,0)$ and $(0,1)$, but now restrict to integer coefficients x_1, x_2. We get a set of the form

$$\{x = x_1(1,0) + x_2(0,1),\ \ x_1, x_2 \in \mathbb{Z}\}.$$

If you plot it, you will see that you find an integer grid!

Group of Vectors

If we consider a vector space V, the vectors form an abelian group.

What is its order? It is infinite…

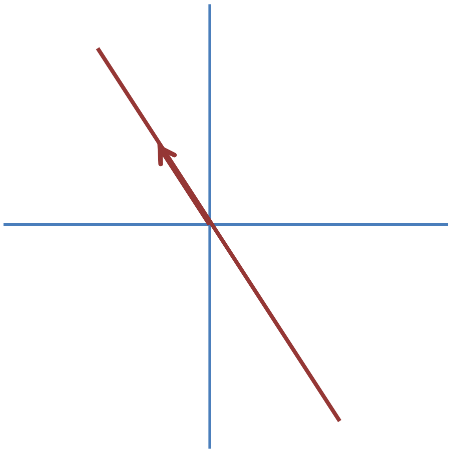
Subspace

When we have a group, we saw we can have subgroups.

Group ↔ **Vector space**

Subgroup ↔ **Subspace**

Subspaces of the 2-dimensional Plane



Subspace

A subset of a vector space which is also a vector space is called a **subspace**.

A subspace of V is thus a **subgroup** of the group V of vectors.

Basis of a Vector Space

A **basis** is a set of linearly independent vectors which span the whole vector space (any other vector can be written as a linear combination of the basis vectors).

Let **x** be a vector in V, a vector space over the real numbers with basis {$\mathbf{v_1}$, $\mathbf{v_2}$,…, $\mathbf{v_n}$}, then **x** = x_1 $\mathbf{v_1}$ + x_2 $\mathbf{v_2}$ + … + x_n $\mathbf{v_n}$ where x_1,…, x_n are real.

Example. The 2-dimensional real plane has for example basis {$\mathbf{v_1}$=(0,1), $\mathbf{v_2}$=(1,0)}.

Integer Linear Combinations?

Let **x** be a vector in V, with basis {$\mathbf{v_1}$, $\mathbf{v_2}$,…, $\mathbf{v_n}$} over the reals, then **x** = x_1 $\mathbf{v_1}$ + x_2 $\mathbf{v_2}$ + … + x_n $\mathbf{v_n}$ where x_1,…, x_n are real.

What happens if x_1,…, x_1 are in fact integers?

Example. The 2-dimensional plane has for example basis {$\mathbf{v_1}$=(0,1), $\mathbf{v_2}$=(1,0)}.

x= x_1(0,1) + x_2 (1,0) where x_1, x_2 are integers.

We might ask whether the integer grid

$$\{x = x_1(1,0) + x_2(0,1),\ x_1, x_2 \in \mathbb{Z}\}$$

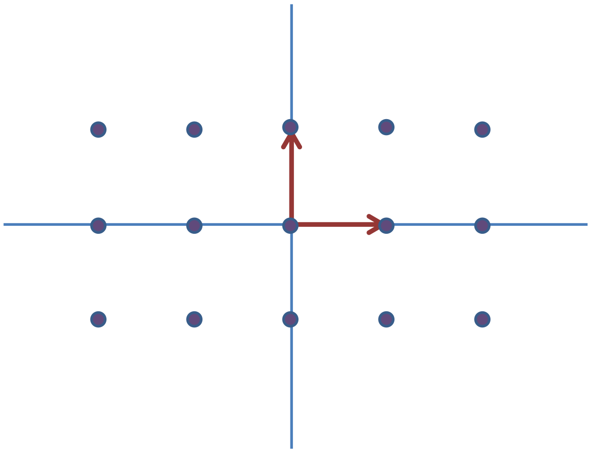
still has a group structure. In fact, we could ask the same question more generally. Suppose that we have two linearly independent vectors v_1, v_2, does the set

$$L = \{x = x_1 v_1 + x_2 v_2,\ x_1, x_2 \in \mathbb{Z}\}$$

form a group? We already know that addition of vectors is associative. If we take two vectors in L, their sum still is a vector in L (we need to make sure that the coefficients still are integers), so the closure property is satisfied. The identity element is the vector $(0,0)$, and every element has an inverse. Indeed, if we have a vector (x_1, x_2) with integer coefficients then $(-x_1, -x_2)$ also has integer coefficients, and their sum is $(0,0)$. In that case, L is called a lattice, and it forms an infinite Abelian group.

A subset of the lattice L which itself has a subgroup structure is called a sublattice.

1^{st} Example

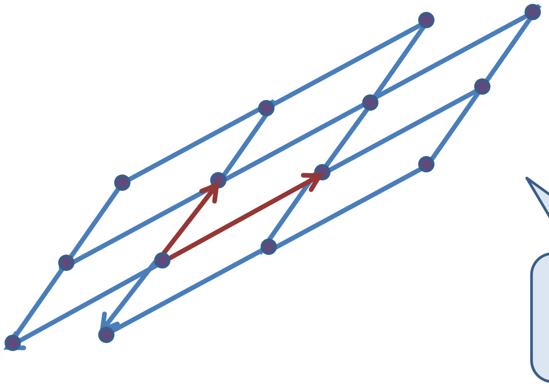


Group Structure?

Take two linearly independent vectors $\mathbf{v_1}$,$\mathbf{v_2}$ in the 2-dimensional real plane. Consider the set $\{x_1\mathbf{v_1}+x_2\mathbf{v_2}, x_1, x_2$ integers$\}$.

Does it form a group?

2nd Example



This forms an infinite group!

Lattice

Take two linearly independent vectors $\mathbf{v_1},\mathbf{v_2}$ in the 2-dimensional real plane. The set $L=\{x_1\mathbf{v_1}+x_2\mathbf{v_2}, x_1,x_2 \text{ integers}\}$ forms a **group** called a **lattice**.

- Addition of vectors is associative.
- Closure: $(x_1\mathbf{v_1}+x_2\mathbf{v_2})+(x_3\mathbf{v_1}+x_4\mathbf{v_2})= (x_1+x_3)\mathbf{v_1}+(x_2+x_4)\mathbf{v_2}$ is in L.
- Inverse: $-x_1\mathbf{v_1}-x_2\mathbf{v_2}$ is the inverse of $x_1\mathbf{v_1}+x_2\mathbf{v_2}$ is in L.
- Identity is the zero vector.

A lattice is an infinite abelian group.

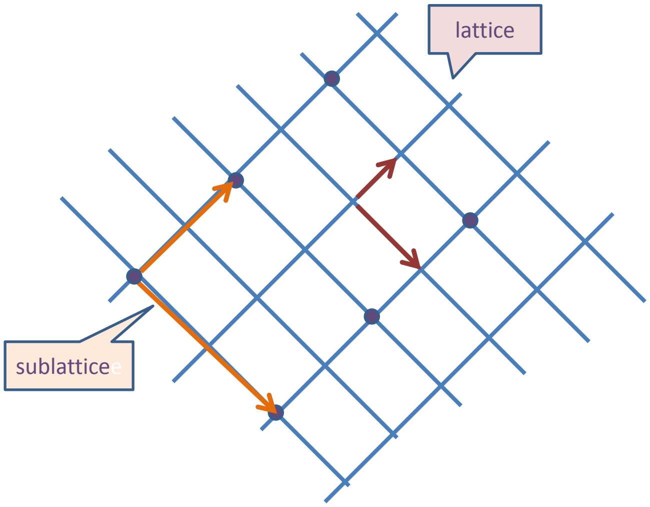
Sublattice

When we have a group, we saw we can have subgroups.

Group ⟺ **Lattice**

Subgroup ⟺ **Sublattice**

3rd Example



We spent quite some time at the beginning of theses lectures to study isometries of the plane. What happens with the isometries of the integer grid?

The isometries of $\mathbb{R}^2 \to \mathbb{R}^2$ were completely characterized and analyzed before and we know that a planar isometry φ is of the form

$$\begin{aligned} \varphi &: (x, y) \mapsto (x', y') \\ \begin{bmatrix} x' \\ y' \end{bmatrix} &= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & (-1)^{\varepsilon} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix}. \end{aligned}$$

Let us now consider the integer grid lattice

$$\mathbb{Z}^2 = \{(m, n) | m \in \mathbb{Z}, \, n \in \mathbb{Z}\}.$$

The isometries of the integer lattice, under the Euclidean distance defined over $\mathbb{R}^2$ will be a subgroup of the group of planar isometries, i.e., they will be of the form

$$\begin{aligned} \varphi_D &: (m, n) \mapsto (m', n') \\ \begin{bmatrix} m' \\ n' \end{bmatrix} &= R_{\theta_D} \begin{bmatrix} 1 & 0 \\ 0 & (-1)^{\varepsilon} \end{bmatrix} \begin{bmatrix} m \\ n \end{bmatrix} + \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix}_D. \end{aligned}$$

The restriction of having to map integer coordinate points to integer coordinate points immediately imposes the following constraints on θ_D and $[\beta_1, \beta_2]_D$:

1. $[\beta_1, \beta_2]_D \in \mathbb{Z}^2$
2. $\cos\theta$ and $\sin\theta$ must be integers or zero, hence their possibilities are $\{-1, 0, 1\}$ yielding $\theta = 0, 90^\circ, 180^\circ, 270^\circ, 360^\circ$.

Hence the set of isometries of the integer lattice/grid forms a group of planar transformations involving integer vector translations and rotations by multiples of 90°.

Isometries of the Plane

We already know:

<u>Theorem</u> An isometry H of the plane is necessarily of the form

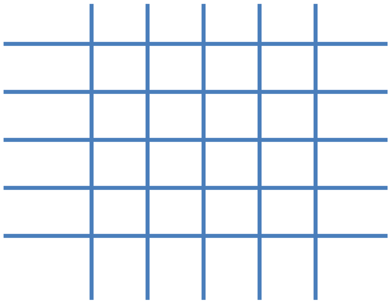
- $H(z)= \alpha z + \beta$, or
- $H(z)=\alpha\bar{z} + \beta$

with $|\alpha|=1$ and some complex number β.

In matrix form:
R_θ M **z** + **b**, where R_θ =rotation matrix by angle of θ,
M=reflection matrix, **b**=translation vector.

Isometries of the Integer Grid (I)

We keep the basis vectors (1,0) and (0,1), but now instead of the 2-dimensional plane, by taking integer coefficients, we get the integer grid.



Isometries of the Integer Grid (II)

What are the isometries of the integer grid?

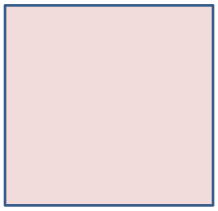
They are a subset (in fact subgroup) of the isometries of the plane, which **sends integer points to integer points.**

In matrix form:
$R_\theta M \mathbf{z} + \mathbf{b}$, where R_θ =rotation matrix by angle of θ,
M=reflection matrix, **b**=translation vector.

1. The translation vector **b** must be part of the integer grid.
2. cosθ and sinθ must be 0,+1 or -1.

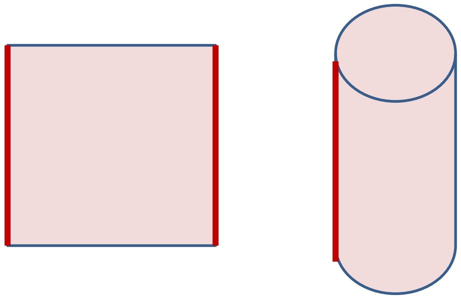
Quotient Group (I)

- The integer grid lattice is a subgroup H of the 2-dimensional real plane seen as an abelian group G.
- Since G is abelian, H satisfies that g+H = H+g. What is the quotient group G/H?



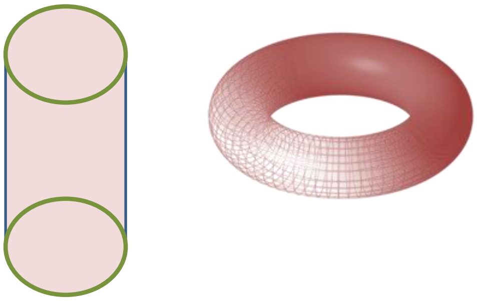
Take the unit square [0,1[x [0,1[.

Quotient Group (II)



Take the unit square [0,1[x [0,1[. In the quotient group, the two unit intervals in red are the same thing.

Quotient Group (III)



Take the cylinder obtained by gluing two sides of the unit square [0,1[x [0,1[. In the quotient group, the two unit circles in green are the same thing.

http://en.wikipedia.org/wiki/File:Zigzag_rhombic_lattice.png

Exercises for Chapter 10

Exercise 46.

- Show that the complex numbers $\mathbb{C}$ form a vector space over the reals.
- Give a basis of $\mathbb{C}$ over the reals.
- In the lecture, we saw for $\mathbb{R}^2$ that we can obtain a new group, called a lattice, by keeping a basis of $\mathbb{R}^2$ but instead considering integer linear combinations instead of real linear combinations. What happens for $\mathbb{C}$ if we do the same thing? (namely consider integer linear combinations).

Exercise 47. Consider the set $\mathcal{M}_2(\mathbb{R})$ of 2×2 matrices with real coefficients.

1. Show that $\mathcal{M}_2(\mathbb{R})$ forms a vector space over the reals.
2. Deduce that it has an abelian group structure.
3. Give a basis of $\mathcal{M}_2(\mathbb{R})$ over the reals.
4. What happens for $\mathcal{M}_2(\mathbb{R})$ if we keep a basis over the reals and consider only integer linear combinations instead of real linear combinations? Do we also get a new group? If so, describe the group obtained.