Napkin Notes

Anachthonic

27 February 2025

Contents

I

Starting out: Groups and metrics

1 Starting out, groups

§1.1 Introduction to Groups

A group is a set G put together with a binary operation on that set $\star$, such that it satisfies some properties:

- (Identity) There exists $1 \in G$ such that for all $g \in G$, $1 \star g = g \star 1 = g$.
- (Inverses) For any $g \in G$ there exists $g^{-1} \in G$ such that $g \star g^{-1} = g^{-1} g \star = 1$.
- (Associativity) For $a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$. Because of this, we denote this product simply as $a \star b \star c$.

Example 1.1.1 (Integers under addition)

The pairing $\mathbb{Z} = (\mathbb{Z}, +)$ satisfies the group axioms.

- $0 \in \mathbb{Z}$ satisfies $0 + x = x + 0 = x$.
- For any $a \in \mathbb{Z}$ there exists $-a \in \mathbb{Z}$ such that $a + (-a) = (-a) + a = 0$.
- Associativity is satisfied.

so it is a group.

Example 1.1.2 (Nonzero rationals)

Denote by $\mathbb{Q}^\times$ the set $\mathbb{Q} \setminus \{0\}$. Then the pairing $\mathbb{Q}^\times = (\mathbb{Q}^\times, \cdot)$ is a group:

- $1 \in \mathbb{Q}^t imes$ such that $1 \cdot q = q \cdot 1 = q$.
- For any $q \in \mathbb{Q}$, there exists q^{-1} such that $q \cdot q^{-1} = q^{-1} \cdot q = 1$.
- Associativity is satisfied.

Remark 1.1.3. A group whose operation is commutative is called **abelian**. A noncommutative group is called **nonabelian**.

Example 1.1.4 (Non-examples of groups)

Here are some pairings that are not groups.

- The pairing $(\mathbb{Q}, \cdot)$ does not form a group since 0 has no inverse.
- The pairing $(\mathbb{Z}, \cdot)$ does not form a group because no elements other than 1 and -1 have inverses.
- Real 2×2 matrices do not form a group, the zero matrix, and any other matrices that have 0 determinant, have no inverse.

Example 1.1.5

Let S^1 denote the complex numbers z with modulus 1. Then $(S^1, \cdot)$ is a group, since

- $1 \in S^1$ is an identity.
- Each complex number z has an inverse $\bar{z}$.

Example 1.1.6 (Addition mod n)

The integers modulo n form a group under addition, since x has inverse $n - x$, and 0 acts as an identity.

Example 1.1.7 (Multiplication mod p)

Define $(\mathbb{Z}/p\mathbb{Z})^\times$ to be the nonzero integers mod p. Then the pairing of this set with multiplication is a group, since each nonzero number mod p has an inverse and 1 acts as an identity.

Remark 1.1.8. We need that p is prime, because if p is composite, $\mathbb{Z}/p\mathbb{Z}$ has zero divisors. Zero divisors do not have multiplicative inverses.

Example 1.1.9 (General linear)

Let n be a positive integer. Then $\mathrm{GL}_n(\mathbb{R})$ is defined as the set of $n \times n$ matrices with nonzero determinant that take values in $\mathbb{R}$. This does form a group with matrix multiplication, and it is nonabelian.

Example 1.1.10 (Special linear)

Then $\mathrm{SL}_n(\mathbb{R})$ is defined similarly as a set of some matrices, this time with determinant 1. $(\mathrm{SL}_n, \times)$ does form a group.

Example 1.1.11 (Symmetric group)

Let S_n be the set of permutations of $\{1, 2, 3, \ldots, n\}$. Viewing these as bijections from this set to itself leads us to consider compositions of permutations. $(S_n, \circ)$ is actually a group, since the identity permutation defined by $\tau(k) = k$ as well as an inverse permutation $\tau(\tau^{-1}(k)) = \tau^{-1}(\tau(k)) = k$ both exist (bijective functions are invertible, and inverses of bijections are bijections).

Example 1.1.12 (Dihedral group)

Denote by D_{2n} the group of symmetries on a regular n-gon. The usual representation of D_{2n} is this:

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}.$$

Where r is a rotation, and s is a reflection about the line between the center and first vertex. Note that this isn't commutative. For example $rs = sr^{n-1}$.

Example 1.1.13 (Product group)

Let $G = (G, \star)$ and $H = (H, *)$ be groups. Define the product group $G \times H = (G \times H, \cdot)$ where $\cdot$ does this:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \star g_2, h_1 * h_2).$$

The identity in this group is $(1_G, 1_H)$ and the inverse of (g, h) is (g^{-1}, h^{-1}).

Example 1.1.14 (Trivial group)

The trivial group $\mathbf{1}$ (or sometimes $\mathbf{0}$) is the group $(\{1\}, \cdot)$.

Example 1.1.15

Exercise 1.1.18:

(a) Rational numbers with odd denominators, under addition. This forms a group since closure, inverses and identity are satisfied.

(b) Rational numbers with denominators at most 2, under multiplication. This does not form a group since $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$.

(c) Rational numbers with denominators at most 2, under addition. This does form a group, since identity, closure and inverses are satisfied.

(d) Nonnegative integers, under addition. This does not form a group since 1 does not have an inverse.

§1.2 Properties of groups

Remark 1.2.1. From now on, we use some shorthand. We abbreviate $(G, \star)$ to G (whenever only one $\star$ really makes sense), and $a \star b$ to ab. We also abbreviate

$$g^n = \underbrace{g \star \cdots \star g}_{n \text{ times}}$$

and $g^{-n} = (g^{-1})^n$.

Proposition 1.2.2

Let G be a group. Then the following hold:

- The identity of the group is unique.
- The inverse of any element is unique.
- For any $g \in G$, we have $(g^{-1})^{-1} = g$

Proof. For the first one, suppose that two identities 1 and 0 exist. Then by definition, $1 \star 0 = 1 = 0$. For the second, if g is an element, suppose h and f are inverses. Then

$fgh = h = f$. For the third, since the inverse of g^{-1} is unique, and $g^{-1} \star g = 1$, then g must be its inverse. □

Proposition 1.2.3

Let G be a group, and $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. $(ab)(ab)^{-1} = 1 \implies b(ab)^{-1} = a^{-1}$, by left multiplication on both sides. Again by left multiplication on both sides, we have $(ab)^{-1} = b^{-1}a^{-1}$. □

Lemma 1.2.4 (Left multiplication is bijective)

Let G be a group, and g be an element of that group. Then the map $G \to G$ given by $x \to gx$ is bijective.

Proof. We give a direct inverse: $g^{-1}x$. Since the function is invertible, it is bijective. Another way is to show injectivity and surjectivity in the usual way. Surjectivity is easy since for any y we can give $g^{-1}y$. Injectivity is handled because the axiom of substitiution shows that $gx = gy$ implies $x = y$ by left multiplication with g^{-1}. □

The fact that this map is injective is usually called the **cancellation law**.

§1.3 Isomorphism

An isomorphism a way to understand when two groups are "essentially" equal. Consider the two groups $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$, and $10\mathbb{Z} = \{\dots, -10, 0, 10, \dots\}$. We can see that these are "equal" modulo multiplication by 10. So we formalize this intuiton thusly.

Definition 1.3.1. A bijection $\phi : G \to H$ between two groups $(G, \star)$ and $(H, *)$ is an **isomorphism** if it satisfies the following property for all $a, b \in G$:

$$\phi(a \star b) = \phi(a) * \phi(b)$$

Two groups are called **isomorphic** if there is an isomorphism between them. Notice that both groups must have the same order.
When two groups G and H are isomorphic we write $G \cong H$.

Example 1.3.2 (Examples of isomorphisms)

Some examples of isomorphisms follow:

- There is an isomorphism between $G \times H$ and $H \times G$ given by $(g, h) \to (h, g)$
- The identity map $\mathrm{id} : G \to G$ is an isomorphism, so $G \cong G$.
- There is another isomorphism from $\mathbb{Z} \to \mathbb{Z}$, and that is $x \to -x$.

Example 1.3.3

A nontrivial example is the case of primitive roots modulo 7, giving that $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/7\mathbb{Z})^\times$. And in general extending to any prime p. First take a primitive root, which in our case is 3. Take the function:

$$\phi(\bar{a}) = 3^a \pmod 7.$$

This is a bijection since the order of 3 mod 7 is 6. Moreover, $\phi(a+b) = \phi(a)\phi(b)$.

Example 1.3.4 (Primitive roots)

In general, there exists an element $g \in (\mathbb{Z}/p\mathbb{Z})^\times$. Such that $1, g, g^2, \ldots, g^{p-2}$ are all different modulo p. In similar general shape to the proof above, we can prove that $\mathbb{Z}/(p-1)\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^\times$, for all primes p.

§1.4 Orders and Lagrange

Definition 1.4.1. The **order of a group** is the number of elements within the group.

Definition 1.4.2. The **order of an element** g within a group is the smallest n such that $g^n = 1$. The order is ∞ if no such n exists. This is denoted by $\operatorname{ord} g$.

Example 1.4.3

A primitive root is an element g of $(\mathbb{Z}/p\mathbb{Z})^\times$ whose order is $p-1$.

Proposition 1.4.4

If $g^n = 1$ then $\operatorname{ord} g \mid n$.

Proof. Suppose $\operatorname{ord} g$ doesn't divide n. By the Euclidean algorithm, Write $n = q(\operatorname{ord} g)+d$ where $d < \operatorname{ord} g$ is nonzero. Consider $g^n = g^{(\operatorname{ord} g)^q} \cdot g^d = g^d = 1$. This implies $\operatorname{ord} g$ isn't the real order, since there is a smaller one. □

We also have that any finite group has finite orders for all of its elements.

Theorem 1.4.5 (Lagrange's theorem for orders)

Let G be any finite group. Then $x^{|G|} = 1$ for any $x \in G$.

Proof. We shall prove this for abelian groups. Consider the coset $xG = G$. Thus the product of all of its elements must be the same. This implies that $x^{|G|} g_1 g_2 \ldots g_{|G|} = g_1 g_2 \ldots g_{|G|}$ and that $x^{|G|} = 1$. □

§1.5 Subgroups

Definition 1.5.1. Let $G = (G, \star)$ be a group. A subgroup of G is a subset of G that forms a group (with the same identity and operation, obviously.) A subgroup H of G is

proper if $H \neq G$.

Example 1.5.2

- $2\mathbb{Z}$ is a (proper) subgroup of $\mathbb{Z}$, that is isomorphic to itself.
- Consider S_n, the symmetric group on n elements. Let T be the set of permutations τ for which $\tau(n) = n$, i.e. consider the group of permutations that fix n. Then this is a subgroup of S_n that is isomorphic to S_n.
- Take the group $G \times H$, and consider the subgroup $G \times \{1_H\}$. This is isomorphic to G by $(g, 1) \to g$.

Example 1.5.3 (Pathological subgroups)

The groups G and the trivial group $\{1_G\}$ are subgroups of G.

Example 1.5.4 (Generated subgroup)

Consider the set $\langle x \rangle = \{\dots, x^{-2}, x^{-1}, 1, x, x^2, \dots\}$. This is also a subgroup of G, the one generated by x.

§1.6 Problem solutions

Problem 1C. We give the isomorphism explicitly, as $\phi(r) = (1\ \ 2\ \ 3)$ (an element of order 3) and $\phi(s) = (1\ 2)(3)$ (an element of order 2). We should also prove that $\phi(sr) = \phi(r)^2\phi(s)$. One can just check using their own diagram. So this works.

In D_{24}, there are elements with order 12, while the greatest order possible for an S_4 element is 4.

Problem 1D. Suppose we have a group G_p that is not isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Note that the orders for each of the elements must divide p, meaning they must either be 1 or p. 0 (the identity) is the only element that can have order 1, so all other elements must have order p. Suppose then x is a member of G_p, such that it has order p. Then we can generate the group as $\{0, x, 2x, \dots, (p-1)x\}$. Now map $ax \to \bar{a}$. This is an isomorphism, so $G_p = \mathbb{Z}/p\mathbb{Z}$.

Problem 1E. We can do $\phi(r) = (1\ 2\ 3\ 4)$ and $\phi(s) = (1\ 2)(3\ 4)$, fixing all the other elements S_8 acts on. Next we prove that $\phi(s)\phi(r) = \phi(r)^3\phi(s)$. One can check that both functions take $(1, 2, 3, 4)$ to $(3, 2, 1, 4)$.

Problem 1F. Take $n = |G|$.

(a) We can think of each element of G as a function $x \to gx$. This is a bijection, so it is a permutation. Just take this to be the permutation!

(b) This time, let's think of each element as a matrix and a vector. Gx, when x is a vector, should equal (gx), where (gx) is the vector. Then ABx would be $A(bx) = (abx)$. One way to do that is to think of the vectors as encoding placement. For example, say $g_m = (0, 0, \dots, 1, \dots, 0, 0)$. where the 1 is at position m. Then we can make the matrices have exactly one 1 on each column and row so that they map exactly to the right thing. In general the first column of matrix G_m should have a 1 at the mth position. The rest will cycle through, so for example $G_2 g_2 = g_3$. (?)

2 Starting out, metrics

§2.1 Definition of a metric space

Definition 2.1.1. A metric space is a pairing (M, d) consisting of a set of points M and a distance function d that must obey the following:

- d is symmetric, i.e. $d(x, y) = d(y, x)$.
- d is **positive definite** which means $d(x, y) \geq 0$ and $d(x, y) = 0$ only when $x = y$.
- d satisfies the triangle inequality, i.e.

$$d(x, y) + d(y, z) \geq d(x, z).$$

Remark 2.1.2. Just like with groups, whenever the metric is obvious, we will just write M instead of (M, d).

Example 2.1.3 (Metric spaces on $\mathbb{R}$ and friends)
There are many metric spaces on extensions of the real numbers.

- The real line $\mathbb{R}$ is a metric space under $d(x) = |x - y|$.
- The interval $[0, 1]$ is also a metric space, with the metric inherited from $\mathbb{R}$.
- Any subset S of $\mathbb{R}$ is a metric space under the same metric.
- $\mathbb{R}^2$ is a metric space under $d((x_1, y_1), (x_2, y_2)) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$
- Any subset of $\mathbb{R}^2$ is a metric space under the same metric.

Example 2.1.4 (Taxicab on $\mathbb{R}^2$)
Define $d((x_1, y_1), (x_2, y_2)) = |x_1 - x_2| + |y_1 - y_2|$.

Example 2.1.5 (Metric spaces on $\mathbb{R}^n$)
There are some metrics on $\mathbb{R}^n$

(a) Define the Euclidean metric as

$$d((a_1, \ldots, a_n), (b_1, \ldots, b_n)) = \sqrt{(a_1 - b_1)^2 + \cdots + (a_n - b_n)^2}$$

(b) The open **unit ball** B^n is the subset of $\mathbb{R}^n$ consisting of the points $(x_1, \ldots, x_n)$ such that $x_1^2 + \cdots + x_n^2 < 1$.

(c) The open **unit sphere** S^{n-1} is the subset of $\mathbb{R}^n$ consisting of the points $(x_1, \ldots, x_n)$ such that $x_1^2 + \cdots + x_n^2 = 1$, with the inherited metric.

Example 2.1.6 (Function space)

Let M be the space of continuous functions $f : [0, 1] \to \mathbb{R}$, and define the metric by $d(f, g) = \int_0^1 |f - g| dx$.

Example 2.1.7 (Discrete space)

Let S be a set of points. We can make S into a discrete space using the function

$$d(x, y) = \begin{cases} 0 & x = y \\ 1 & x \neq y \end{cases}$$

If $|S| = 4$ this is visualizable as the vertices of a regular tetrahedron living in $\mathbb{R}^3$.

Example 2.1.8

Graphs can be made into metric spaces with the space being the set of vertices and the distance being the graph-theoretic distance between them. (When G is a complete graph you get a discrete space.)

§2.2 Convergence in metric spaces

Definition 2.2.1. Let $(x_n)_{n\geq 1}$ be a sequence of points in metric space M. We say that x_n converges to x if the following holds: For all $\varepsilon > 0$, there exists an integer N_ε such that $d(x_n, x) < \varepsilon$ for each $n \geq N$. We write

$$x_n \to x$$

or more verbosely,

$$\lim_{n\to\infty} x_n = x.$$

Example 2.2.2

The sequence $x_1 = 1$, $x_2 = 1.4$, $x_3 = 1.41$, *dots*.

- If we see this as a sequence in $\mathbb{R}$, it converges to $\sqrt{2}$.
- If this is a sequence in $\mathbb{Q}$, it doesnt converge, despite all of its elements being members of $\mathbb{Q}$.

Remark 2.2.3. The convergent sequences in a discrete space are those which are eventually all one element. ($\varepsilon = \frac{1}{2}$ will show this).

§2.3 Continuous maps

Definition 2.3.1. Let $M = (M, d_m)$ and $N = (N, d_n)$ be metric spaces. A function $f : M \to N$ is continuous at $p \in M$ if for every $\varepsilon > 0$ there exists $\delta > 0$ such that $d_m(x, p) < \delta \implies d_n(f(x), f(p)) < \epsilon$.

We give another equivalent condition.

Theorem 2.3.2

A function $f : M \to N$ is continuous at p iff for all sequences (x_n) that converge to p, $(f(x_n))$ converges to $f(p)$.

Proof. Define **"eventually ε apart"** to mean that a sequence has all its points after some N within distance ε of a point or a sequence.

We first prove that continuous maps preserve sequential convergence. Suppose $x_n \to p$ and f is a continuous function at p. Let $\varepsilon > 0$. We know that there exists δ such that if x_n and p are eventually δ apart, then $f(x_n)$ and $f(p)$ are eventually ε apart. Since x_n and p will eventually be δ apart, by virtue of convergence, we are done.

Next we prove that if a function preserves sequential convergence, then it is continuous. Suppose we have that it's not. Then there exists $\varepsilon > 0$ such that no matter what δ we choose, there is a point x within δ of p such that $f(x)$ is not within ε of p. Take, for example, $\delta = \frac{1}{2^n}$ and choose one point within δ of p that satisfies this property, calling it x_n. However, this means that $x_n \to p$ while $f(x_n) \not\to p$, which is a contradiction. □

Proposition 2.3.3 (Composition preserves continuity)

Let $f : M \to N$ and $g : N \to L$ be continuous functions. Then $h = g \circ f : M \to L$ is continuous.

Proof. This first condition tells us that for all $\varepsilon > 0$ there exists δ such that if x and p are δ apart then $f(x)$ and $f(p)$ are ε apart. Moreover, for all $\zeta > 0$ there exists ε such that if $f(x)$ and $f(p)$ are ε apart then $g(f(x))$ and $g(f(p))$ are ζ apart. The existence of δ is guaranteed, so we are done.

An easier method: Notice that for any convergent sequence x_n, $f(x_n)$ is also convergent. Then so is $g(f(x_n))$. So h preserves convergence, so we are done. □

Remark 2.3.4. A map from a discrete space to a metric space is always continuous, since the only convergent sequences are the ones that are all eventually p. Then the resulting sequence is all eventually $f(p)$, so convergent sequences are maintained.

§2.4 Homeomorphism

Definition 2.4.1. A function $f : M \to N$ between metric spaces is a **homeomorphism** if it is a bijection, and both f and f^{-1} (which exists) are both continuous. We say that M and N are homeomorphic.

Homeomorphism is an equivalence relation. (As we have proved earlier, transitivity holds.)

Example 2.4.2 (Homeomorphism $\neq$ continuous bijection)

There is a continuous bijection from $[0, 1)$ to the circle, but it has no continuous inverse.

Let M be a discrete space with size $|\mathbb{R}|$. There is a continuous function $f : M \to \mathbb{R}$ but it does not have a continuous inverse.

Example 2.4.3

Some examples of homeomorphisms follow:

- Any space M is homeomorphic to itself, through the identity map.
- It is a famous example that a donut (torus) is homeomorphic to a coffee cup.
- The unit circle is homeomorphic to the boundary of the square.

Example 2.4.4 (Unit circle metrics)

There are two ways to define a metric on the unit circle S^1. The chord distance (inherited from $\mathbb{R}^2$) and the circumferential distance. One can prove that these metrics are homeomorphic, meaning it doesn't matter whichever one we choose. (Map an arc to its chord and vice versa)

Example 2.4.5 (Non-size preserving homeomorphisms)

The open interval $(-1, 1)$ is homeomorphic to the real line, by the bijection

$$x \mapsto \tan(x\pi/2)$$

§2.5 Product metric

Let $M = (M, d)$ and $N = (N, e)$ be metric spaces. We want to define the product metric $f : M \times N \to \mathbb{R}$. Let $p_i = (m_i, n_i)$. We have a couple of choices when it comes to the metric we want:

$$f_1(p_1, p_2) = \max\{d(m_1, m_2), e(n_1, n_2)\}$$

$$f_2(p_1, p_2) = \sqrt{d(m_1, m_2)^2 + e(n_1, n_2)^2}$$

$$f_3(p_1, p_2) = d(m_1, m_2) + e(n_1, n_2)$$

Which are the maximum, Euclidean and taxicab metrics respectively.

Proposition 2.5.1

$$f_1(p_1, p_2) \leq f_2(p_1, p_2) \leq f_3(p_1, p_2) \leq 2f_1(p_1, p_2),$$

which means a product metric taking any of these as metrics are homeomorphic.

Proof. $f_2 \le f_3$ is very obvious by squaring both sides. Squaring both sides also shows $f_1 \le f_2$. Next, since twice the maximum is bigger than the sum, we have $f_3 \le 2f_1$.

Call the metrics taking these as M_1, M_2, and M_3. Prove first that M_1 and M_2 are homeomorphic:

Fix ε. So there must exist δ such that $f_1(p_1, p_2) < \delta \implies f_2(p_1, p_2) < \varepsilon$. For this side, we can pick $\delta = \varepsilon/2$. The other side requires $\delta = \varepsilon$. This also works for f_3 and f_1, so we are done. □

Example 2.5.2

If we take $M = N = \mathbb{R}$, we get the metric on $\mathbb{R}^2$. We principally pick the Euclidean metric, but we have now shown that all others are homeomorphic, and thus this choice is arbitrary. (although well motivated)

Proposition 2.5.3

We have $(x_n, y_n) \to (x, y)$ iff $x_n \to x$ and $y_n \to y$.

Proof. Let's take the maximum metric. Fix $\varepsilon > 0$. If there exists δ such that $f((x_n, y_n), (x, y)) < \varepsilon$, then both $d(x_n, x)$ and $e(y_n, y)$ are less than ε. So if (x_n, y_n) converges, then so do (x_n) and (y_n). Instead assume that (x_n) and (y_n) converge, and let $\varepsilon > 0$. Then there exists δ such that both $d(x_n, x)$ and $e(y_n, y)$ are less than ε. Thus their maximum is also less than ε. □

Proposition 2.5.4

Addition and multiplication are continuous maps $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$.

Proof. We first prove that $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is continuous using the maximum metric is a continuous map. Fix $\varepsilon > 0$. We have to find δ such that if $\max\{|x - a|, |y - b|\} < \delta \implies |(x + y) - (a + b)| < \varepsilon$. However, since $|(x - a) + (y - b)| \le |x - a| + |y - b| < 2\delta$, picking $\varepsilon = \delta/2$ is enough.

Next is to prove that $\times : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is continuous. We use sequential continuity. Let $x_n \to x$ and $y_n \to y$. Then $x_n y_n = (x + (x_n - x))(y + (y_n - y)) = xy + y(x_n - x) + x(y_n - y) + (x_n - x)(y_n - y)$. It is easy to see that this value tends to xy, but we can also say that $|x_n y_n - xy| \le |y||x_n - x| + |x||y - n - y| + |x_n - x||y_n - y| < (x + y)\delta + \delta^2$. Solving the equation $\varepsilon = (x + y)\delta + \delta^2$ will get us our desired result. □

§2.6 Open sets

Definition 2.6.1. Let M be a metric space. For each real number r and point $p \in M$ we define

$$M_r(p) = \{x \in M \mid d(x, p) < r\}.$$

We call this the *r*-**neighborhood** around p in M.

A sequence x_n converges to x if each r-neighborhood around x contains all eventual points (i.e. all points after some $n = N$) of x_n.

Remark 2.6.2. A function f is continuous at p if the preimage of each ε-neighborhood around $f(p)$ contains some δ-neighborhood around p.

Definition 2.6.3. A set $U \subset M$ is **open** in M if for each $p \in M$, some r-neighborhood around p is contained within U.

Example 2.6.4

Here are some examples of open sets

- Each r-neighborhood is open.
- Open intervals in $\mathbb{R}$ are open, hence the name.
- The unit ball B^n is open in $\mathbb{R}^n$
- The interval $(0, 1)$ is open in $\mathbb{R}$ but not open in $\mathbb{R}^2$.
- The empty set $\emptyset$ and M are open in M for vacuous and tautological reasons respectively.

Example 2.6.5

Some non-examples of open sets follow.

- The closed interval $[0, 1]$ is not open in $\mathbb{R}$. No neighborhood around 0 is fully contained within it.
- The unit circle S^1 is not open in $\mathbb{R}^2$.

Remark 2.6.6. Each subset of a discrete space is open.

Proposition 2.6.7

The intersection of finitely many open sets is open, and the union of open sets is open, even when there are infinitely many.

Proof. Let $p \in U_1 \cap U_2 \cap \cdots \cap U_n$. There exists r such that $M_r(p)$ is a subset of U_m for each m. Pick the smallest such r, call it R. Then $M_R(p) \subseteq M_r(p) \subseteq U_m$ for all m.

Let p be a member of a union of open sets U. Let U_1 be (one of, if not) the set that p is a part of. There is some r such that $M_r(p) \subseteq U_1 \subseteq U$. □

Theorem 2.6.8

A function $f : M \to N$ of metric spaces is continuous iff the pre-image of every open set in N is open in M.

Proof. Suppose the preimage of each open set in N is open in M. Then the preimage of an ε-neighborhood aronud $f(p)$ is an open set in M that contains p. Thus there exists δ such that the δ-neighborhood around p is fully inside that preimage. So f is continuous.

Now assume f is continuous. Suppose V is an open subset of N, and let $U = f^{-1}(V)$. Pick $x \in U$, so that $y = f(x) \in V$. Since V is open, take a ε-neighborhood around y which is fully contained within V. We have a δ-neighborhood around x that fully lands in the ε-neighborhood around y, and thus is fully contained in U, because of continuity. Since this holds for all x, we have that U is open. □

§2.7 Closed sets

Definition 2.7.1. Let M be a metric space. $S \subseteq M$ is **closed** in M if each convergent sequence converges to a point inside S. (limit completeness)

Let $\lim S := \{p \in M : \exists (x_n) \in S \text{ such that } x_n \to p\}$. A set is closed if $\lim S = S$.

Remark 2.7.2. $\lim S$ is closed. Let x_n be a sequence in $\lim S$ converging to x. Let E_n be a sequence in S that is ε away from x_n. (We can achieve this since x_i are limit points). We now know that E_n is 2ε away from x, so $x \in \lim S$.

Example 2.7.3 (Examples of closed sets)

Some examples of closed sets follow.

- The empty set *emptyset* is closed in M.
- M is closed in M.
- The closed interval $[0, 1]$ is closed in $\mathbb{R}$ and $\mathbb{R}^2$.

Theorem 2.7.4

Let M be a metric space, and $S \subseteq M$ be a subset. Then these are equivalent:

- S is open in M.
- $M \setminus S = S^c$ is closed in M.

Proof. Let S be an open set, and suppose there is some limit point x of S^c that is a member of S. However, there will always be members of S^c around x, a contradiction.

Suppose S is a closed set, and suppose there is some point in S^c that always contains some points from S around it. However, if a point always contains points from S no matter how small the neighborhood, that means it is a limit point of S and thus S is not closed, a contradiction. □

§2.8 Problem solutions

Problem 2A. Fix $\varepsilon > 0$. Then we must find δ such that $\max\{d(a,b), d(x,y)\} < \delta$ implies $|d(a,b) - d(x,y)| < \varepsilon$. However, just pick $\delta = \frac{\varepsilon}{2}$.
Problem 2B. Let f be a continuous bijection $f : \mathbb{Q} \to \mathbb{N}$. Fix $\varepsilon < 1$. There must exist δ such that $|x - y| < \delta \implies |f(x) - f(y)| < \varepsilon$. This implies that $f(x) = f(y)$, and that $x = y$. A contradiction.
Problem 2C. $f(x, y) = g(x, -y)$ where g is known to be continuous. So is $-x$, so f is continuous. $f(x, y) = xf(y)$ where multiplication is continuous, so we must show

$f : \mathbb{R}_{>0} \to \mathbb{R}$ defined by the reciprocal is continuous. Let p be a point and $\varepsilon > 0$ be fixed. There must exist δ such that if $|x - p| < \delta$ then $|\frac{1}{x} - \frac{1}{p}| = |\frac{x-p}{xp}| < \frac{2}{p^2}|p - x| < \frac{2\delta}{p^2}$, so we are done.

Problem 2D. Consider the function

$$f(x) = \begin{cases} x & x \in \mathbb{Q} \\ 0 & x \in \mathbb{R} \setminus \mathbb{Q} \end{cases}$$

Problem 2E. Suppose we have a function $f : \mathbb{R} \to \mathbb{R}$ such that $x > y \implies f(x) > f(y)$ and is continuous nowhere.

II

Basic Abstract Algebra

3 Homomorphisms and quotient groups

§3.1 Generators and group presentations

Definition 3.1.1. Let S be a subset of group G. The subgroup generated by S, $\langle S \rangle$, is the set of elements that can be written as a finite product of the elements of S (and their inverses). If $\langle S \rangle = G$, we say that S is a set of generators for G.

> **Remark 3.1.2.** The "(and their inverses)" condition is not necessary when we are dealing with a finite group, because $x^{-1} = x^{|G|-1}$, as follows from uniqueness of inverses.

Example 3.1.3

$\langle 1 \rangle$ generates $\mathbb{Z}$ because all integers can be written as finite sums of 1 and -1.

Definition 3.1.4. The representation of groups given by generator elements and their relations is also called **group presentation**. For example, $\langle x \mid x^{100} = 1 \rangle$ is the presentation for $\mathbb{Z}/100\mathbb{Z}$.

Example 3.1.5 (Dihedral group)

The dihedral group of order $2n$ is given by

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, sr = r^{-1}s \rangle .$$

Example 3.1.6 (Klein four)

The **Klein four group**, given by $(\mathbb{Z}/2\mathbb{Z})^2$ has the presentation

$$\langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle .$$

Example 3.1.7

The **Free group** on n elements, F_n is given by the presentation

$$F_n = \langle x_1, x_2, \ldots, x_n \rangle .$$

§3.2 Homomorphisms

Definition 3.2.1. Let $G = (G, \cdot)$ and $H = (H, \star)$ be groups. A **group homomorphism** is a function $\phi : G \to H$ such that

$$\phi(g_1 \cdot g_2) = \phi(g_1) \star \phi(g_2).$$

Example 3.2.2

Let G and H be groups.

- Any isomorphism is a homomorphism. The identity map $G \to G$ is a homomorphism.
- The trivial homomorphism $G \to H$ sends everything to 1_H.
- There is a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}/100\mathbb{Z}$ by modding everything out by 100.
- There is a homomorphism $\mathbb{Z} \to \mathbb{Z}$ defined by $x \mapsto 10x$ which is injective but not surjective.
- There is a homomorphism from S_n to S_{n+1} by "embedding": every permutation on n elements is a permutation on $n+1$ elements by fixing the $n+1$st element.
- $\phi : D_{12} \to D_6$ given by $s_{12} \mapsto s_6$ and $r_{12} \mapsto r_6$. This is a homomorphism.
- Specifying a homomorphism $\mathbb{Z} \to G$ is the same as giving $\phi(1)$.

Definition 3.2.3. The **kernel** of a homomorphism $\phi : G \to H$ is defined by

$$\ker \phi = \{g \in G : \phi(g) = 1_H\}.$$

Remark 3.2.4. $\ker \phi$ is a subgroup of G because it includes the identity of G, and any inverses: $1_H = \phi(g \star g^{-1}) = \phi(g) * \phi(g^{-1}) = 1_H * \phi(g^{-1})$.

Proposition 3.2.5

The map ϕ is injective iff $\ker \phi = \{1_G\}$.

Proof. Suppose ϕ is injective. We know that $\phi(1_G) = 1_H$, and there can be no other elements of the kernel. Now suppose $\ker \phi = \{1_G\}$, and further suppose that $f(a) = f(b)$ where $a \neq b$. Now consider $1_H = \phi(a)\phi(b)^{-1} = \phi(ab^{-1}) \neq \phi(1_G) = 1_H$, a contradiction. □

Example 3.2.6 (Examples of kernels)

Let G and H be groups.

- The kernel of an isomorphism $G \to H$ is $\{1_G\}$.
- The kernel of the trivial homomorphism $G \to H$ is G.
- The kernel of the homomorphism $\mathbb{Z} \to \mathbb{Z}/100\mathbb{Z}$ by $n \to \bar{n}$ is $100\mathbb{Z}$.
- The kernel of the map $\mathbb{Z} \to \mathbb{Z}$ given by $x \mapsto 10x$ is $\{0\}$.

Remark 3.2.7. Fix $g \in G$. Suppose we have $\mathbb{Z} \to G$ by $n \to g^n$. Let $x = \operatorname{ord} g$. The kernel is $x\mathbb{Z}$.

Remark 3.2.8. Let $\phi : G \to H$ be a homomorphism. Then the image $\phi(G)$ is a subgroup of H. We have identity 1_H, and the inverse is inherited.

§3.3 Cosets and modding out

Let G and Q be groups, and suppose we have a surjective homomorphism $\phi : G \twoheadrightarrow Q$.

Let's look at the special case of $\phi : \mathbb{Z} \to \mathbb{Z}/100\mathbb{Z}$, modding out by 100. We know that $\ker \phi = 100\mathbb{Z}$.

Definition 3.3.1. Give an equivalence relation $x \equiv y$ if $\phi(x) = \phi(y)$.

Call $N = \ker \phi$.

Remark 3.3.2. $x \equiv y$ if and only if $x = yn$ for some $n \in N$. The first direction is painfully obvious, so let's do the other part. Suppose $x \equiv y$. This means $\phi(x) = \phi(y)$. This means that $\phi(xy^{-1}) \in N$, so that $xy^{-1} = n$ for some $n \in N$. This immedieately follows.

Thus, the equivalence class that contains x is given by $xN = \{xn : n \in N\}$.

Definition 3.3.3. Let H be a subgroup of G. Then a set of the form gH for some $g \in G$ is called a **left coset** of H.

Definition 3.3.4. A subgroup N of G is called **normal** if it is the kernel of some homomorphism. We write $N \trianglelefteq G$.

Definition 3.3.5. Let G be a group and N a normal subgroup. We define a **quotient group**, denoted G/N, (read "G mod N") using the following heuristics:

- We want each element of G/N to be a coset of N.
- In this light, we wish to define the product of two cosets. Let q_1 be the value associated with coset C_1 and similarly with q_2 and C_2. We want $C_1 \cdot C_2$ to contain $q_1 q_2$.
- We can also define this using representatives of elements in C_i. Let $g_1 \in C_1$ and $g_2 \in C_2$. Then we want $g_1 g_2 \in C_1 C_2$.

§3.4 Proof of Lagrange's in its generality

Theorem 3.4.1

Let G be a finite group, and H a subgroup. Then $|G|$ is divisible by $|H|$.

Proof. Very simple. Since all the cosets of H have the same cardinality, and form a partition of G (even when H isn't normal). Hence if n is the amount of cosets, $n \cdot |H| = |G|$. □

Remark 3.4.2. $x^{|G|}$ is equal to 1. Consider $H = \langle x \rangle$. This set is $\{1, x, \dots, x^{|H|-1}\}$. This tells us that $x^{|H|} = 1$, so $x^{|G|} = 1$.

Remark 3.4.3. In general, $|G/N| = |G|/|N|$.

§3.5 Eliminating the homomorphism

Proposition 3.5.1

If $\phi : G \to K$ is a homomorphism with kernel $H = \ker \phi$, we have that if $h \in H$, for all $g \in G$, $ghg^{-1} \in H$.

Proof. See that $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(gg^{-1}) = 1_K$. □

Example 3.5.2 (Example of a non-normal subgroup)

Consider D_{12} and look at $H = \{1, s\}$ as a subgroup. Notice that

$$rsr^{-1} = r(sr^{-1}) = r(rs) = r^2 s \notin H.$$

Theorem 3.5.3

A subgroup H of G is normal if and only if for all $h \in H$ and $g \in G$ we have $ghg^{-1} \in H$.

Proof. We have already shown one of the directions, now let's show the other ones. We need to build a homomorphism with kernel H. So we just create G/H as the cosets. We need to verify

Lemma 3.5.4

If $a \equiv a'$ and $b \equiv b'$ then $a'b' \equiv ab$.

Proof. Let $a' = ah_1$ and $b' = bh_2$. Then we need to have that $ah_1bh_2 \equiv ab$. We have that $b^{-1}h_1b$ is some element of H, call it h_3. Thus h_1b is bh_3, and the left hand side becomes $abh_3h_1 \equiv ab$. Since h_3h_1 is an element of H, we are done. □

With that, we can define the multiplication of two cosets as $(g_1H)(g_2H) = (g_1g_2)H$. and the above claim shows that this is well defined, i.e. it doesn't matter what representatives of g_1H and g_2H we choose. So G/H is a group. Moreover, there is an obvious homomorphism $g \mapsto gH$, with kernel H. □

Example 3.5.5 (Modding out in the product group)

Consider the product group $G \times H$. Earlier we identified the subgroup $G' = \{(g, 1) : g \in G\} \cong G$

We can also see that $G' \trianglelefteq G \times H$. (It is the kernel of the homomorphism $G \times H \to H$ with $(g, h) \mapsto h$.) We can also calculate using our new method to get $(a, b)(g, 1)(a^{-1}, b^{-1}) = (aga^{-1}, 1) \in G'$.

Example 3.5.6 (Quotients may not cancel with products)

It's not necessarily true that $(G/H) \times H \cong G$. For example, consider $G = \mathbb{Z}/4\mathbb{Z}$ and the normal subgroup $H = \{0, 2\} \cong \mathbb{Z}/2\mathbb{Z}$.

Example 3.5.7 (Explicit computation)

Let $\phi : D_8 \to \mathbb{Z}/4\mathbb{Z}$ be defined by $s \to \bar{2}$ and $r \to \bar{2}$.

The kernel is $N = \{1, r^2, sr, sr^3\}$ (each of the elements that feature an even number of s and r). We can see that then the odd numbered elements will return 2. So we see that D_8/N is a group of order 2, so it is $\mathbb{Z}/2\mathbb{Z}$. And the image of ϕ is $\{0, 2\} \cong \mathbb{Z}/2\mathbb{Z}$.

Remark 3.5.8. If G is abelian, it obviously follows that each subgroup of G is normal.

Remark 3.5.9. If G is a group with n generators, we can write it as the quotient group F_n/N where N is a kernel. For example suppose you have the relation $x = y$ in your presentation. Then you will force $\phi(x) = \phi(y)$ and so $\phi(xy^{-1}) = 1$. Turn each of these relations into something that should result in 1. Suppose you're left with $R_1, R_2, \ldots, R_n$ where R_i are the things in our relations that should be 1. We just say that $N = \langle R_1, R_2, R_3, \ldots, R_n \rangle$.

§3.6 Problem solutions

3A. Taking arbitrary g and h, we see that $gghh = ghgh \implies gh = hg$. So the group must be abelian. This obviously works for all abelian groups.
3B. Consider the group $G = D_{10}$. Then we have $\phi(r) = 0$ and $\phi(s) = 1$, and we need to verify that $\phi(sr) = \phi(r^4 s) = 1$. So this is a homomorphism and so we have $\langle r \rangle$ is a normal subgroup with $G/N \cong \mathbb{Z}/2\mathbb{Z}$. For the second one, we have $rsr^4 = sr^3 \notin \{1, s\}$.
3C. Is there a normal subgroup of S_4 with an order of 3?

4 Rings and ideals

§4.1 Definition and examples

Definition 4.1.1. A **ring** is a triple $(R, +, \times)$, two operations called addition and multiplication such that

- $(R, +)$ is an abelian group, with identity 0_R or just 0.
- $\times$ is an associative, binary operation on R with an identity 1_R or just 1.
- Multiplication distributes over addition.

Example 4.1.2 (Typical rings)

Here are the typical rings:

- The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all rings with the usual addition and multiplication.
- The integers modulo n are also a ring with the usual addition and multiplication, denoted $\mathbb{Z}/n\mathbb{Z}$.

Definition 4.1.3. The **zero ring** is the ring with a single element, usually denoted 0. A ring is nontrivial if it is not the zero ring.

Remark 4.1.4. A ring is nontrivial iff $0_R \neq 1_R$. If $0 = 1$, $a = 1 \times a = 0 \times a = 0$.

Proposition 4.1.5

For any $r \in R$, $r \times 0 = 0$. $r \times (-1) = -r$.

Example 4.1.6

Given two rings R and S, define the product ring with componentwise addition and multiplication. For example, the chinese remainder theorem says that $\mathbb{Z}/15\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Example 4.1.7

Given a ring R, we can define the **polynomial ring** as follows:

$$R[x] = \left\{ c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 \mid c_0, c_1, \ldots, c_n \in R \right\}.$$

Example 4.1.8

We can adjoin more variables if we want, and we denote this $R[x_1, \ldots, x_n]$.

Example 4.1.9 (Gaussian integers)
With some abuse of notation, we can write the Gaussian integers as

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Example 4.1.10 (Cube root of 2)
We can write, using the same abuse of notation, that

$$\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}.$$

§4.2 Fields

Definition 4.2.1. A **unit** is an element $u \in R$ which is invertible. There exists $x \in R$ with $ux = 1$.

Example 4.2.2
Examples of units follow:

- The units of $\mathbb{Z}$ are ± 1.
- In $\mathbb{Q}$, everything except for 0 is a unit.
- The Gaussian integers $\mathbb{Z}[i]$ have four units, ± 1 and $\pm i$.

Definition 4.2.3. A nontrivial ring is a **field** when all of its nonzero elements are units.

Example 4.2.4
Principal examples of fields follow:

- $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields, since $\frac{1}{c}$ makes sense in them.
- If p is a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field, denoted $\mathbb{F}_p$.

§4.3 Homomorphisms

Definition 4.3.1. Let $R = (R, +, \times)$ and $S = (S, \oplus, \star)$ be rings. A **ring homomorphism** is a map $\phi : R \to S$ such that, if x and y are elements of R:

- $\phi(x + y) = \phi(x) \oplus \phi(y)$
- $\phi(x \times y) = \phi(x) \star \phi(y)$
- $\phi(1_R) = 1_S$

Example 4.3.2

Examples of ring homomorphisms follow:

- The identity map.
- The map $\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$, modding out by 5.
- The map $\mathbb{R}[x] \to \mathbb{R}$ defined by $p(x) \mapsto p(0)$, taking the constant term.
- The trivial ring homomorphism $R \to 0$.

Example 4.3.3

Some maps fail to be homomorphisms

- The map $\mathbb{Z} \to 2\mathbb{Z}$ by taking $x \mapsto 2x$ fails, because it does not preserve multiplication.
- The map $R \to S$ taking $x \mapsto 0$ fails, because $1_R \not\mapsto 1_S$.
- There is no ring homomorphism $\mathbb{Z}/2016\mathbb{Z} \to \mathbb{Z}$.

§4.4 Ideals