Prelim Review

Hui Sun

June 12, 2024

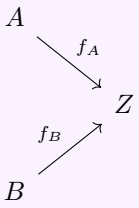
Contents

Chapter 1

Category Theory-Aluffi I.5

Definition 1.1 (initial, final)**.** Let C be a category. We say $I \in Obj(C)$ is **initial** if for every $A \in Obj(C)$, there exists exactly one morphism $f : I \to A$. (In other words, $Hom(I, A)$ is a singleton). We say $F \in Obj(C)$ is **final** if for every $B \in Obj(C)$, $Hom(B, F)$ is a singleton.

Definition 1.2 (coproduct)**.** Let A, B be objects of a category C, then the coproduct $A \amalg B$ is an object of C with two morphisms $i_A : A \to A \amalg B$, $i_b : B \to A \amalg B$ with the following universal property: for all objects $Z \in Obj(C)$ and for all morphisms f_A, f_B such that



there exists a unique $\sigma : A \amalg B \to Z$ such that the following diagram commutes:

Chapter 2

Aluffi II

Proposition 2.1. Let $|g|$ be the order of an element $g \in G$, then $|g| \leq |G|$.

Proof. It's trivial if $|G| = \infty$. For $|G| < \infty$, consider the following $|G| + 1$ terms,

$$g^0, g, g^2, \ldots, g^{|G|}$$

Note all can be distinct, hence there exists $i < j$ such that $g^i = g^j$, i.e., $g^{j-i} = e$. This implies that $|g| \leq |G|$. □

Example 2.1. There exists g, h with finite orders each, and gh has infinite order. For example, the group generated by relations:

$$\langle r, s : r^2 = s^2 = e \rangle$$

The term rs has infinite order. Note there exists geometric examples with matrix groups.

Proposition 2.2. The following is a list of statements/propositions that you should know.

1. If $g^N = e$, then $|g|$ divides N.
2. If $g^m = N$, then $|g| = \frac{lcm(|g|,m)}{m}$
3. If $gh = hg$, then $|gh|$ divides $lcm(|g|, |h|)$
4. We have $|g^m| = \frac{|g|}{\gcd(m,|g|)}$

Definition 2.1 (Dihedrayl group)**.** The group D_{2n} is the group of rotations and reflections of n-polygons. (There are $2n$ elements in this group).

We note that D_6 and S_3 are isomorphic. They are both generated by x, y such that $x^2 = e, y^3 = e$.
We first note that $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group of order n,and $[1]$ is a generator.

Proposition 2.3. $[m]$ is a generator of $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(m, n) = 1$.

Proof. $[m]$ is a generator if and only if $[m]$ has order n, which by the above proposition 4, we have $[m] = m[1]$, hence $\gcd(m, n) = 1$. □

Proposition 2.4. $(\mathbb{Z}/n\mathbb{Z})^* = \{[m] : \gcd(m,n) = 1\}$ is a group under the multiplication defined as

$$[m] \cdot [n] = [mn]$$

Proof. We will only check the existence of inverse. For each $[m]$, we know $\gcd(m,n) = 1$, hence $[m]$ is a generator of the additive group $\mathbb{Z}/n\mathbb{Z}$, hence we know there exists some integer q such that $q[m] = [1]$, this implies that $[q][m] = [1]$, hence inverse. □

Example 2.2. $G \cong H \times G$ does not mean that H is the trivial group. For example, consider G as the infinite product $G = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \ldots$, and take $H = \mathbb{Z}$.

Note that if we take $G = \mathbb{Z}$, then H is the trivial group. Proof: consider where $\varphi(1)$ gets sent to. No matter where it is sent to, there are elements not mapped by φ.

Example 2.3. Let $\varphi : S_3 \to \mathbb{Z}/2\mathbb{Z}$ be a homomorphism, then φ sends elements of order 3 to 0. One can define the commutator subgroup. Let G be a group, then the commutator subgroup $[A, G]$ is generated by

$$\langle ghg^{-1}h^{1-}, g, h \in G \rangle$$

then

Proposition 2.5. Let $\varphi : G \to H$ be a homomorphism, then $\varphi([A, G]) \subset \ker(\varphi)$.

Moreover, one can show that any homomorphism $\varphi : S_3 \to \mathbb{Z}/2\mathbb{Z}$ should send all elements of order 2 to 0, or all to 1. One can either use the determinant map $\det : S_3 \to \{\pm 1\}$, or consider that

$$\varphi((12)(23)(12)) = \varphi(13) = \varphi(12)\varphi(23)\varphi(12)$$

then $\varphi(13) = \varphi(23)$.

Example 2.4. Any homomorphism $\varphi : \mathbb{Q} \to \mathbb{Q}$ is linear, i.e., $\varphi(p) = qp$ for some $q \in \mathbb{Q}$. We note that $\varphi(p) = p\varphi(1)$, and $\varphi\left(\frac{1}{p}\right) = \frac{1}{q}\varphi(1)$. Hence we have $\varphi\left(\frac{p}{q}\right) = \frac{p}{q}\varphi(1)$. By the same argument, any homomorphism from $\mathbb{Z} \to \mathbb{Z}$ is also linear.

We note that isomorphisms preserve the following things:

Proposition 2.6. If G, H are isomorphic, then

1. If G is abelian, then H is abelian.
2. The order of g=the order of $\varphi(g)$

If it's just a homomorphism, then the order of $\varphi(g)$ divides the order of g. For example, there is no nontrivial homomorphism from $\mathbb{Z}/4\mathbb{Z}$ to $\mathbb{Z}/7\mathbb{Z}$, because $\varphi(g)$'s order would have to divide 4 and 7.

Example 2.5. $(\mathbb{R}, \cdot)$ and $(\mathbb{C}, \cdot)$ are not isomorphic. There are no finite order elements in $\mathbb{R}$, but i has order 4 in $\mathbb{C}$.

Example 2.6. $Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ is a ring, with the gruop being under addition of maps. $Aut(\mathbb{Z}/n\mathbb{Z})$ is a group under composition of maps.

Proposition 2.7. Let H be a subset of a group G, then H is a subgroup if for all $a, b \in H$, $ab^{-1} \in H$.

Every homomorphism $\varphi : G \to G'$ determines two subgroups naturally, $\ker(G) \subset G, Im(G) \subset G'$. This is because if H' is a subgroup of G', then $\varphi^{-1}(H')$ is a subgroup of G. In fact, the image of any subgroup of G is also a subgroup of G'.

Definition 2.2 (cyclic group). A group is cyclic if it is either $\cong \mathbb{Z}$ or $\cong \mathbb{Z}/n\mathbb{Z}$.

Let's now classify all the subgroups of cyclic groups.

Proposition 2.8. If $H \subset \mathbb{Z}$ is a subgroup, then $H = d\mathbb{Z}$ for some $d \geq 0$. (Proof: let d be the smallest positive integer in H).

If $G \subset \mathbb{Z}/n\mathbb{Z}$ is a subgroup, then $G = \langle [d]_n \rangle$ for some d that divides n. Moreover, this exists a bijection between the subgroups of $\mathbb{Z}/n\mathbb{Z}$ with the divisors of n.

Idea 2.1. This means that all subgroups of cyclic groups are cyclic.

Example 2.7. Show that $\mathbb{Z}/12\mathbb{Z}$ has 6 subgroups. Proof: 12 has 6 divisors: 1,2,3,4,6,12.

Proposition 2.9. Let $\varphi : G \to H$ be a surjective homomorphism, then if G is cyclic, H is also cyclic.

This gives the result that the projection π_n allows us to go from a cyclic subgroup of $\mathbb{Z}$ to a cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$.

To understand $\varphi : G \to G'$ as a monic morphism means φ is injective. If we consider

$$\ker(\varphi) \underset{e}{\overset{i}{\rightrightarrows}} G \xrightarrow{\varphi} G'$$

Then $\varphi \circ i = \varphi \circ e$, where e is the trivial map and i is the inclusion map, this means that $\ker(\varphi) = \{e\}$.

Proposition 2.10. Let $S \subset G$ be a subset, S generates G if and only if $\pi : F(S) \to G$ is surjective.

Proof. Assume π is surjective, then for any $g \in G$, we have $\pi(w) = g$ for some $s \in F(S)$, and $w = s_1^{n_1} \dots s_n^{n_k}$, hence every g corresponds to that. □

Theorem 2.2. Let $\varphi : G \to G'$ be a homomorphism, then there exists a bijection $\tilde{\varphi}$

$$\tilde{\varphi} : G/\ker(\varphi) \to Im(\varphi)$$

Proof. Let $\tilde{\varphi}([a]) := \varphi(a)$. Then $Im(\tilde{\varphi})$ is a subgroup of G'. We just need to show that $\tilde{\varphi}$ is injective.

$$\tilde{\varphi}([a]) = \tilde{\varphi}([b]) \Rightarrow \varphi(a) = \varphi(b) \Rightarrow \varphi(ab^{-1}) = e \Rightarrow ab^{-1} \in \ker(\varphi) \Rightarrow [a] = [b]$$

Note that the last argument is by $H = \ker(\varphi)$ is normal, hence we want to show $Ha = Hb$, and $ab^{-1} \in H$ means $Hab^{-1} \subset H$, i.e., $Ha \subset Hb$, and vice versa. □

Example 2.8. The commutator subgroup of a group G is defined roughly to capture the group that is "not commutative with other elements." In other words, they should, in some sense, be complimentary to the center. The commutator subgroup $[G, G]$ of G is the subgroup **generated by**

$$\langle ghg^{-1}h^{-1}, g, h \in G \rangle$$

Proposition 2.11. The $G/[G, G]$ is abelian. In other words, the quotient group by the commutator subgroup is abelian. (This intuitively makes sense because if we view the "noncommutative elements" as the same, then the rest should just be abelian).

Proof. We would like to show that $g[G, G]h[G, G] = gh[G, G] = hg[G, G]$. In other words,

$$g^{-1}h^{-1}gh \in [G, G] \Rightarrow g^{-1}h^{-1}gh \subset [G, G] \Rightarrow g^{-1}h^{-1}gh \in [G, G] = [G, G]$$

This is because that any coset contained in one coset is equal to the entire coset. □

Lemma 2.1. we claim that for any subgroup H,

$$gH \subset H \Rightarrow gH = H$$

For any $h \in H$, we know that $g^{-1}gH \in H$, and because $gh \in H$, we have that $g^{-1} \in H$, hence we have that $h \in gH$ as well.

Warning 2.3. This fact should be memorized, i.e., if any coset gH is contained in an other coset $g'H$, then they are the same.

Chapter 3

Set Theory

We will review some definitions that we might forget.

Definition 3.1 (order relation or simple order)**.** An ordered relation C is one such that

1. For every $x, y \in A$, either xCy or yCx.
2. xCx is not true for all x.
3. If xCy, yCz, then xCz.

Definition 3.2 (well-ordered set)**.** A set A with an order relation $<$ is called well-ordered if every set has a smallest element.

If A is a well-ordered set, then any subset of A with restricted order is a well-ordered set. And if A, B are well-ordered sets, then the directionary product of $A \times B$ is well-ordered.

Theorem 3.1. Let A by any set, then there exists a order relation on A such that A is well-ordered.

Definition 3.3 (strict partial order, partial order)**.** Given a set A, a relation $\prec$ is called a stric partial order if

1. There is no $x \in A$, such that $x \prec x$.
2. For $x \prec y, y \prec z$, we have $x \prec z$.

A partial order $\leq$ is such that

1. $x \leq x$ for all x
2. If $x \leq y, y \leq x$, then $x = y$.
3. If $x \leq y, y \leq z$, then we have $x \leq z$.

Note that a strict partial order is a order relation without the comparability.

Proposition 3.1. Let A be a strictly partially ordered set, then there exists a maximal simply ordered subset B of A.

Lemma 3.1 (Zorn's lemma)**.** Let A be a strictly partially ordered set. If every simply ordered subset of A has an upper bound in A, then there exists a maximal element in A.

Chapter 4

Topology

4.1 12, 13, 14, 15, 16

Definition 4.1 (topology). A topology on a set X is a collection $\mathcal{T}$ of subsets of X such that

1. $X, \varnothing \in \mathcal{T}$.
2. $\bigcup_{\alpha \in A} U_\alpha$ is in $\mathcal{T}$.
3. For any finite intersection $\bigcap_{i=1}^{N} U_i \in \mathcal{T}$.

Any set belonging to $\mathcal{T}$ is called an open set.

If X is any set, with $\mathcal{T}$ all subsets of X, then $\mathcal{T}$ is called the discrete topology. If $\mathcal{T}$ only contains $X, \varnothing$, then it is the indiscrete topology. One can check that the topology defined by

$$\mathcal{T} = \{U \subset X : U^c \text{ is countable or is all of } X\}$$

is a topology on X. Moreover, if $\mathcal{T}, \mathcal{T}'$ are two topologies on X, and $\mathcal{T} \subset \mathcal{T}'$, then $\mathcal{T}'$ is called finer than $\mathcal{T}$. Now we recall the basis for topologies.

Definition 4.2 (basis). A basis is a collection $\mathcal{B}$ of subsets of X, such that

1. For each $x \in X$, there exists a $B \in \mathcal{B}$ such that $x \in B$.
2. If x belongs to the intersection of two basis elements B_1, B_2, then there exists $B_3 \in \mathcal{B}$ such that $x \in B_3 \in B_1 \cap B_2$.

The topology generated by $\mathcal{B}$ is defined such that: U is an open set if for every $x \in U$, there exists $B \in \mathcal{B}$ such that $x \in B \subset U$.

An equivalent condition for 1 is such that $\bigcup B = X$, and an equivalent condition for 2 is such that $B_1 \cap B_2 = \bigcup_\alpha B_\alpha$, with $B_\alpha \in \mathcal{B}$. And it is easy to show that the toplogy $\mathcal{T}$ generated by $\mathcal{B}$ is indeed a basis. There is an equivalent way to get a topolgy using the basis: $\mathcal{T}$ generated by a basis $\mathcal{B}$ can also be defined by taking all arbitrary unions of the basis elements, and it is easy to show that these definitions are equivalent. Next we remember how to go from a topology to a basis.

Lemma 4.1. Let $(X, \mathcal{T})$ be a topological space, and $\mathcal{C}$ is a collection of open sets X such that for each open set U, with $x \in U$, there exists $C \in \mathcal{C}$ such that $x \in C \subset U$. Then $\mathcal{C}$ is a basis.

Proof. It is easy to show that C is a basis. Note that we also have to show that the topology $\mathcal{T}'$ generated by $\mathcal{C}$ is the same as $\mathcal{T}$. Let $U \in \mathcal{T}$, then for all $x \in U$, there exists C such that $x \in C \subset U$, which is in $\mathcal{T}'$ by

definition. Let's assume $O \in \mathcal{T}'$, then $O = \bigcup_\alpha C_\alpha$, note that each $C_\alpha \in \mathcal{T}$, hence O is an open set in $\mathcal{T}$ as well. □

Now we state a lemma to check whether one toplogy is finer than the other using basis.

Lemma 4.2. Let $\mathcal{B}, \mathcal{B}'$ are bases for topologies $\mathcal{T}, \mathcal{T}'$, then the following are equivalent.

1. $\mathcal{T}'$ is finer than $\mathcal{T}$.
2. For each $x \in X$, and each $B \in \mathcal{B}$ such that $x \in B$, there exists $B' \in \mathcal{B}'$ such that $x \in B \subset B'$.

Now one can see that in $\mathbb{R}^2$, the toplogy generated by open balls and open rectangles are the same. The **standard** topology on $\mathbb{R}$ is defined by

$$U = \{x : a < x < b, a, b \in \mathbb{R}\}$$

and there are other topologies such as the lower-limit topology for $\mathbb{R}$ defined by $\{x : a \leq x < b\}$, or the K-topology

$$\{x : a < x < b\} - \left\{\frac{1}{n} : n \in \mathbb{Z}_+\right\}$$

One can show that lower limit topology and the K-topology are strictly finer than the standard topology. Now we define a subbasis.

Definition 4.3 (subbasis). A subbasis $\mathcal{S}$ for a topology on X is a collection of $U_\alpha \in \mathcal{T}$, such that $\bigcup_\alpha U_\alpha = X$. The topology generated by the subbasis is the union of all finite intersections of U_α's.

Note that to show that the topology generated by a subbasis is indeed a topology, it suffices to show that the set of finite intersections of $B \in \mathcal{S}$ is indeed a basis. There are some important consequences.

1. Let $\{\mathcal{T}_\alpha\}$ be an arbitrary collection of topologies, then $\bigcap_\alpha \mathcal{T}_\alpha$ is also a topology, but $\bigcup_\alpha \mathcal{T}_\alpha$ is not necessarily a topology.
2. et $\{\mathcal{T}_\alpha\}$ be an arbitrary collection of topologies, then there exists a unique smallest topology that contains $\bigcup_\alpha T_\alpha$.
3. The topology generated by a basis $\mathcal{B}$ is equal to the topology of all topologies containing $\mathcal{B}$

insert notes

Problem 4.1. Show that the directionary order topology on $\mathbb{R} \times \mathbb{R}$ is the same as the product topology $\mathbb{R}_d \times \mathbb{R}$, where $\mathbb{R}_d$ is the discrete topology.

Proof. The directionary order topology on $\mathbb{R} \times \mathbb{R}$ is generated by the basis $\mathcal{B}$,

$$\mathcal{B} = \{a \times (b, c) : a, b, c \in \mathbb{R}, b < c\}$$

And the basis $\mathcal{B}'$ for the product topology $\mathbb{R}_d \times \mathbb{R}$ is

$$\mathcal{B}' = \{(U, V) : U \text{ is open in } \mathbb{R}_d \, , V \text{ is open in } \mathbb{R} \}$$

We note that every basis element in $\mathcal{B}$ is also a basis element in $\mathcal{B}'$. Conversely, note that all basis elements $\mathcal{B}'$ are arbitrary unions of elements in $\mathcal{B}$, hence all the basis elements in $\mathcal{B}'$ belong to the order topology on $\mathbb{R} \times \mathbb{R}$. Because the order topology on $\mathbb{R} \times \mathbb{R}$, and it is contained in $\mathbb{R}_d \times \mathbb{R}$, because there exists a unique smallest topology containing the basis, we have the two topologies are equal. □

insert notes here

Definition 4.4 (T_1 space)**.** A topological space is said to be T_1, if for all x, y distinct, there exists open sets U, V such that $x \in U, y \in V$.

Lemma 4.3. A space is T_1 if and only if setes of finite points $\{x_1, \ldots, x_n\}$ are closed.

Proof. Assume that sets of finite points are closed, then for any x, y distinct, $\{x\}, \{y\}$ are both closed. Hence $X \setminus \{x\}, X \setminus \{y\}$ are both open, and they do not contain the other points. Hence the space is T_1 by definition. Conversely, assume that a space is T_1, then it suffices to show that $\{x\}$ is closed for arbitrary x, i.e., it contains all of its limit points. If y is distinct from x, then there exists an open set that doesn't intersect $\{x\}$ by the space being T_1, hence y is not a limit point of $\{x\}$. □

The next lemma illustrates why we care about Hausdorff spaces.

Lemma 4.4. A sequence in a Hausdorff space, if converges, converges to a unique limit point.

Problem 4.2. Let A, B be subsets of X, then $\overline{A} \cup \overline{B} = \overline{A \cup B}$.

Proof. For any closed set containing A and a closed set containing B, their union also contains $A \cup B$, hence $\overline{A \cup B} \subset \overline{A} \cup \overline{B}$. The other side is checked by different cases, and definition of a limit point. □

Problem 4.3. We have $\bigcup_\alpha \overline{A_\alpha} \subset \overline{\bigcup_\alpha A_\alpha}$, and this is a strict inclusion.

Proof. The inclusion can be shown using the same argument. Consider the sets

$$A_n = \left\{ x : \frac{1}{n} < x \leq 1, n \in \mathbb{N} \right\}$$

Hence we have sets that look like $\left(\frac{1}{n}, 1\right]$, and

$$\bigcup_n \overline{A_n} = (0, 1] \ , \overline{\bigcup_n A_n} = [0, 1]$$

□

Problem 4.4. Let $A = (0, 1), B = (1, 2)$, then $\overline{A \cap B} = \varnothing$, and $\overline{A} \cap \overline{B} = 1$. So I think $\overline{A \cap B} \subset \overline{A} \cap \overline{B}$.

Proof. For any closed set that contains A, and intersected with □

Problem 4.5. X is Hausdorff if and only if the diagnoal $\Delta = \{x \times x \in X \times X\}$ is closed in $X \times X$.

Proof. X is Hausdorff iff for all x, y distinct, you can find U, V open such that $x \in U, y \in V$, such that $U \cap V = \varnothing$. Then for all $(y, z) \notin \Delta$, $(y, z) \in U \times V$, and $U \times V \cap \Delta = \varnothing$. (Assume there exists $(y, z) \in U \times V \cap \Delta$, then $(y, z) = (y, y)$, and $y \in U, y \in V$, but this is impossible since $U \cap V = \varnothing$.) Hence by definition, (y, z) is not a limit point of Δ, this is if and only if Δ is closed. □

Problem 4.6. For the finite complement topology on $\mathbb{R}$, the sequence $\left\{\frac{1}{n} : n \in \mathbb{N}\right\}$ converges to every single point in $\mathbb{R}$.

Proof. □

Problem 4.7. If U is open, then is it true that $U = Int(\overline{U})$?

Proof. No, consider $U = (0, 1) \cup (1, 2)$ □

Chapter 5

Algebra

5.1 Group Theory

Example 5.1. Give an example of an element that has a right inverse but not a left inverse.

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

We note that the permutations (bijective maps from T to T) of a set T form a group, under composition of maps. Now we remind the definition of symmetric groups.

Definition 5.1 (Symmetric group)**.** Let the group of permutations of the set of indices $\{1, 2, \ldots, n\}$ is called the symmetric group, denoted by S_n. And if n is finite, then $|S_n| = n!$.

There is only one group of order 2, because every group can be shown to have the form $\{1, g\}$, which is S_2. For S_3, it is the smallest group that the law of composition isn't commutative.

Proposition 5.1. Any subgroup of the additive integers is of the form

$$\{a\mathbb{Z} : a \in \mathbb{Z}\}$$

Proposition 5.2. For $a, b \in \mathbb{Z}$ such that d is the greatest common divisor of a, b, i.e., $d = gcd(a, b)$, then

$$\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b$$

This is because for $d = gcd(a, b)$, there exists integers s, t such that $d = sa + tb$. This implies that if a, b are coprime, then the subgroup of $\mathbb{Z}$ that contains both a, b is $\mathbb{Z}$ itself.

Example 5.2. $\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$ has infinite order in GL_2.

Example 5.3. The simplest group that is not cyclic. The Klein four group consisting of 4 elements:

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

Problem 5.1. Suppose $a, b \in G$, then ab and ba have the same order.

This can be done by expanding out the terms.

Problem 5.2. A cyclic group of order n contains $\phi(n)$ of generators, where $\phi(n)$ is the positive integers that are relatively prime to n, less than n.

Problem 5.3. The product of two elements of finite order could be an element of infinite order.

Proof.

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{bmatrix}$$

Their product is $\begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 2 \end{bmatrix}$. □

Definition 5.2 (subgroup)**.** H is a subgroup of G if and only if for any $a, b \in H$, $ab^{-1} \in H$.

Proposition 5.3. If 1 is the identity of a subgroup H of G, then 1 is the identity of G as well.

This can be used to show that if $\phi : G \to G'$ is a homomorphism, then $\phi(1_G) = 1_{G'}$. One can show that $1_{G'}$ is the identity of the subgroup $Im(\phi)$.

Definition 5.3. The kernel of a homomorphism ϕ is

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

Definition 5.4. The alternating group A_n is the group of even permutations, i.e., having an even number of two-element swaps. Alternatively, it is the kernel of the sign homomorphism $S_n \to \{-1, 1\}$ (it only has positive 1 determinant).

Definition 5.5. A subgroup N is normal if for every $a \in N$, and every $g \in G$, $gag^{-1} \in N$.

Proposition 5.4. The kernel of the map from $G \to Aut(G)$

$$g \mapsto f_g(h) = ghg^{-1}$$

The kernel of this map is all the elements g such that $gh = hg$, which is called the center Z of G. It is a normal subgroup.

Proposition 5.5. The conjugate map $\varphi : G \to G$ is an automorphism, i.e., it is an isomorphism onto itself.

$$\varphi(x) = gxg^{-1}$$

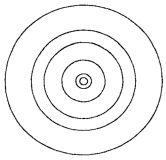
for some $g \in G$.

Proof. The inverse map is given by conjuation by g^{-1}, hence is bijective. Homomorphism is easy to check. □

We note that two elements a, b commute if and only if $aba^{-1} = b$.

Definition 5.6 (fibers)**.** Let $f : S \to T$ be bijective, then define the preimage of a particular element as the fibers of f.

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



Some Fibres of the Absolute Value Map $\mathbb{C}^\times \to \mathbb{R}^\times$.

The fibers define an equivalence relation. In other words, two elements a, b are equivalent, $a \sim b$ if and only if $f(a) = f(b)$.

Let $\varphi : G \to G'$ be a homomorphism, then the fibers are given by the cosets aK, where K is the kernel of φ.

Proposition 5.6. The order of an element $a \in G$ divides the order of the group G.

Proof. The order of an element a is the same as the number of elements of $\langle a \rangle$, which is the cyclic group generated by a. By Lagrange's theorem, the order of the subgroup divides the order of the group. □

Proposition 5.7. Let $\varphi : G \to G'$ be a homomorphism for a finite group, then

$$|G| = |ker(\varphi)| \cdot |Im(\varphi)|$$

Proof. This follows by cosets partition G and Lagrange's theorem. □