Prelim Review

Hui Sun

October 25, 2024

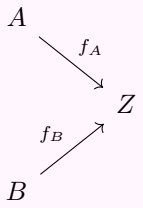
Contents

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.

Example 2.9. Let H be a normal subgroup of G, and K be a subgroup of G, then $HK = \{hk : h \in H, k \in K\}$ is a normal subgroup.

To show that it is a subgroup, we note that

$$HK = \pi^{-1}(\pi(K))$$

where $\pi : G \to G/H$. In other words, $\pi^{-1}(gH) = gH$.

Lemma 2.2. For H normal in G, the usual projeciton $\pi : G \to G/H$, we have $\pi^{-1}(gH) = gH$.

Example 2.10. Cosets are disjoint. Let $g \in g_1H \cap g_2H$, then $g_1h_1 = g_2h_2$, then $g_1 = g_2h_2h_1^{-1}$, hence $g_1H \subset g_2H$.

Example 2.11 (8.13). Let $|G|$ be odd, show that every element is a square.

Method 1: it'd be nice if we can show that $f(g) = g^2$ is an injective homomrophism from $G \to G$, but this is not the case. It need not to be a homomorphism. In fact, it is a homomorphism only when G is abelian. Now consider $\langle g \rangle$, it is an abelian group, so we can restrict f to all the $\langle g \rangle$, then we can show that it is injective, hence surjective.

Method 2: observe that $g^{|G|} = 1, g^{|G|+1} = g$, then $(g^{|G|+1})^2 = g$.

Example 2.12 (8.25). An interesting homomorphism from $G/H \to Aut(G)$, when H is abelian and normal.

We know that if H is normal, then $f : g \mapsto \gamma_g$ satisfies $\gamma_g(H) \subset H$, and hence an homomorphism would be $g \mapsto \gamma_g|_H$. Now if H is abelian, we see that $H \subset \ker(f)$, i.e. there is the homomorphism from $G/H \to Aut(H)$ is well-defined.

Lemma 2.3. Let $f : G \to G'$, then the following are equivalent:

1. $\overline{f} : G/H \to G'$ is well-defined, i.e., $gH \mapsto f(g)$.
2. $H \subset \ker(f)$.

Definition 2.3 (action on a set). An action ρ of G on a set A is a function $\rho : G \times A \to A$ such that

$$\rho(e, a) = a, \forall a, \rho(gh, a) = \rho(g, \rho(h, a)), \forall g, h, a$$

We call an action is transitive if for all $a, b \in A$, there exists g such that

$$b = \rho(g, a)$$

We know that left multiplications are faithful and also transitive.

Theorem 2.4 (Cayley's theorem). Every group acts faithfully on some set.

Proof: Every group acts faithfully on itself by left multiplication.

Definition 2.4 (orbit, stabilizer). The orbit of an element $a \in A$ under the action of G is the set

$$O(a) = \{\rho(g, a) : g \in G\}$$

The stabilizer subgroup of G of $a \in A$ is

$$Stab(a) = \{g \in G : \rho(g, a) = a\}$$

Proposition 2.12. Orbits partition the set A.

Proof. We can show this directly: if $\rho(g_1, a) = \rho(g_2, b)$, then $\rho(g', a) \in O(b)$ for ant g'.

Alternatively, we can show that if $c = \rho(g, a) \in O(a)$, then $O(c) \subset O(a)$; then we can show if $c \in O(a)$, then $a \in O(c)$, so $O(a) \subset O(c)$, hence $O(a) = O(c)$, hence any overlap implies equality. □

From this we see that orbits partition A, and the induced action on each orbit is transitive. Hence it suffices to consider transitive actions if we want to understand any group actions on a set.

Proposition 2.13. If G acts transitively on a set A, then $|A|$ divides $|G|$.

Proof. One can define a bijection between $\varphi : G/H \to A$, where $H = Stab(a)$ for any $a \in A$, by $\varphi : gH \mapsto g{\cdot}a$. Then by Lagrange's, we know $|G| = |A| \cdot |H|$. □

Example 2.13 (9.11). Let G be a finite group, and p be the smallest prime such that it divides $|G|$. Let H be a subgroup of G of index p, then H is normal.

The proof relies on showing $\ker(\sigma) = H$, where $\sigma : G \to S_p$ corresponds to an action of G on G/H.

Example 2.14. Any group of order p^2 is abelian.

Chapter 3

Aluffi III: Rings and Modules

Definition 3.1. An integral domain is nonzero commutative ring R such that for all $a, b \in R$

$$ab = 0 \Rightarrow a = 0 \text{ or } b = 0$$

Equivalently, left and right multiplication by every nonzero element $u \in R$ is injective.

In other words, if we define a left zero divisor as $a \in R$ such that for some $b \neq 0$ we have $ab = 0$, then the integral domain requires NO nonzero zero divisors (0 is always going to be a zero divisor).

Proposition 3.1. Multiplication cancellation holds in integral domains, i.e., if $ab = ac$, then $b = c$, for $a \neq 0$.

Proof. We will know it holds if multiplication by a is an injective function, this is true if and only if a is not a zero divisor. □

Example 3.1. $\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Q}$ are integral domains, and $\mathbb{Z}/n\mathbb{Z}$ is not, for some n. However, $\mathbb{Z}/p\mathbb{Z}$ is a integral domain.

Definition 3.2. A left unit in R is u such that there exists v and $uv = 1$. In other words, a left unit has a right inverse.

We note that two-sided units have unique inverses, and if we call the two-sided units just units, the units of a ring form a group!

One warning: if u only has a right inverse, and no left inverse, then this u may have many right inverses.

Definition 3.3 (field)**.** A field is a commutative ring such that every nonzero element is a unit. (And of course, fields are integral domains, integral domains are not always fields, for example, $\mathbb{Z}$).

Proposition 3.2. In a field, left (and right) multiplication by any $u \neq 0$ is injective and surjective.

Proof. This uses the fact that $u \neq 0$ is a two-sided unit. □

Proposition 3.3. A finite integral domain is a field. (In other words, a finite commutative ring is a field if and only if it is an integral domain).

Proof. It suffices to show that the left and right multiplications by an element in this integral domain is surjective (this would imply this element is a unit). We know the multiplication is injective, and an injective map from a finite set to itself is also surjective. □

Example 3.2. $\mathbb{Z}/p\mathbb{Z}$ is a field, hence an integral domain. This is because the group of units in $\mathbb{Z}/n\mathbb{Z}$ is those m such that $\gcd(m,n)=1$.

If m is a unit in $\mathbb{Z}/n\mathbb{Z}$, then $1 \equiv am$ for some m, then m is a generator of $\mathbb{Z}/n\mathbb{Z}$, hence $\gcd(m,n)=1$. Proof: $am = 1 \mod n$, hence there exists some b such that $am+bn=1$, hence $\gcd(m,n)=1$.

Proposition 3.4. A polynomial ring $R[x]$ is an integral domain if R is an integral domain.

Example 3.3. A commutative ring R is a field if and only if the only ideals are R and $\{0\}$.

Proof. If $a \neq 0$, then $aR = R$, then the left multiplication by a is surjective, hence a is a unit. □

Example 3.4. Let I be an ideal, $\varphi : R \to S$ be a ring homomorphism, $\varphi(I)$ need not to be an ideal.

Take $R=\mathbb{Z}, I=2\mathbb{Z}, S=\mathbb{Q}$.

Example 3.5. $\mathbb{Z}[x]$ is not a PID. We can take the ideal generated by $(2,x)$, it is the polynomials with even constant terms, but cannot be generated by a single element of $\mathbb{Z}[x]$.

Alternatively, $(x) \subset (2,x)$, where (x) is a prime ideal, but clearly (x) is not maximal. But in a PID, nonzero prime ideal $\iff$ maximal ideal.

However, $k[X]$ is a PID, for k field.

Example 3.6. A finite commutative ring R, and an ideal I in R, R/I is a field if and only if R/I is an integral domain. **Hence**, for a commutative ring R, if R/I is finite, an ideal is maximal if and only if it is prime.

Example 3.7. A prime ideal in $\mathbb{Z}$ is exactly (p), where p is prime.

Proposition 3.5. Here are several conditions where the prime ideal I is equivalent to maximal ideals.

1. R/I is commutative and finite.
2. R is a commutative PID.

Example 3.8. $k[x]$ is a PID, just like $\mathbb{Z}$ is a PID.

You choose a monic polynomial with the smallest degree and use the division algorithm to show that everything in $k[x]$ is divisible by this polynomial. Hence every prime ideal in $k[x]$ is also maximal.

Definition 3.4 (dimension of rings)**.** The Krull dimension of a commutative ring R is the length of the longest chain of prime ideals in R.

For example, for $k[x]$, where k is field, $k[x]$ is a PID, and all prime ideals are maximal, so the Krull dimension of a PID is 1. Likewise, $\mathbb{Z}$ also has dimension 1. However, take $\mathbb{Z}[x]$, the length of prime ideals $(2, x)$ is 2, hence it has dimension 2. And $k[x_1, \ldots, x_n]$ has dimension n, where $(x_1) \subset (x_1, x_2) \subset \ldots \subset (x_1, \ldots, x_n)$.

Proposition 3.6. If R/I is reduced (no nilpotent elements), then the ideal I is radical. In other words, for $r^n \in I$, for some n, we have $r \in I$.

Proof. $(r + I)^n = I$ implies that $r^n \in I$, by R/I being reduced, we know $r \in I$. Hence R/I is reduced means that if $r^n \in I$, then $r \in I$. □

Example 3.9. Assume R/IJ is reduced, then $I \cap J \subset IJ$.
We show that if $r \in I \cap J$, then $r^2 \in IJ$, and by the previous proposition, $r \in IJ$.

3.1 Modules

Definition 3.5 (R-module)**.** A R-module is an abelian group M endowed with an action from R, i.e. endowed with a function $\cdot : R \times M \to M$ (such that it satisfies with a few properties).

Proposition 3.7. Every abelian group M is a $\mathbb{Z}$-module. In other words, abelian groups and $\mathbb{Z}$-modules are the same notion.

Proof. This is because one knows that $\mathbb{Z}$ is initial in Ring, hence there exists a unique homomorphism from $\mathbb{Z} \to \text{End}(M, M)$. □

Definition 3.6 (homomorphism between modules)**.** Let M, N be R-modules, then $\varphi : M \to N$ is a homomorphism if it is a homomorphism wrt the abelian structure, and respects the ring actions.

1. $\varphi(m + n) = \varphi(m) + \varphi(n)$
2. $\varphi(r \cdot m) = r\varphi(m)$

Note that the R-modules along with the homomorphisms form a category "R-Mod." Moreover, if k is a field, then a k-module is called a k-vector space, and the morphisms are linear maps.

Definition 3.7 (Noetherian)**.** A ring R is said to be Noetherian if every ideal $I \subset R$ is finitely generated. An R-module M is Noetherian if every submodule is finitely generated.
An example where a ring/module is not Noetherian: $\mathbb{Z}[x_1, \ldots]$, and the ideal/submodule generated by $(x_1, x_2, \ldots)$.

Chapter 4

Groups II

Theorem 4.1 (p-group, fixed point theorem)**.** Let G be a p-group acting on a fintie set A (a finite group with a power of p elements), let $Z = \{a \in A : ga = a \text{for all} g\}$, then we have

$$|A| \equiv |Z| \mod p$$

For example, one could apply this to the conjugacy action, giving the class formula.

Theorem 4.2 (Class formula)**.** Let G be a finite set, and $Z(G)$ be its center, then we have

$$|G| = |Z(G)| + \sum_{a \in A} |O_a|$$

where A is a set that contains one representative for every nontrivial conjugacy class in G.

With the class formula, we can do a lot of things. For example, we know every group of prime order is cyclic, by consider $\langle g \rangle, g \neq 0$ and applying Lagrange. Hence it's commutative. Now we also know that every group of order p^2 is commutative.

Proposition 4.1. Every group of order p^2 is commutative.

Proof. G is a p-group, hence has no trivial center $Z(G)$, hence $|Z(G)| = p$ or p^2. If $|Z(G)| = p$, then we know that $|G/Z(G)| = p$, hence it is cyclic, then G is commutative (can check this). If $|Z(G)| = p^2$, then it is commutative anyways.

More general statement: let $|G| = pq$, where p, q are primes, then either G is commutative or G has trivial center. □

Example 4.1. S_3 cannot have a normal subgroup H of order 2.

This is because S_3 has trivial center, and any normal subgroup is a union of conjugacy classes, hence H must have one other conjugacy class containing of one element. However, a conjugacy class with one element lives in the center. This is a contradiction.

Example 4.2. 1. If there is only 1 cyclic subgroup of order p, then this subgroup must be normal.

Theorem 4.3. Fix p, all p-Sylow subgroups are conjugate to each other.

Example 4.3. Every simple p-groups are cyclic. (Hint: they must have order p).

Slogan: size of the conjugacy class $[a]$ is equal to the index of the centralizer $[G : Z(a)]$.

4.1 IV.4 Conjugacy classes in S_n

Definition 4.1 (type)**.** The type of $\sigma \in S_n$ is the length of disjoint cycles(orbits) it makes. For example, if σ acts on $\{1, \dots, 8\}$ as $(12346)(78)$, then the type is $[5, 2, 1]$.

Please note that the cycles used in a type are disjoint, since they are orbits.

Proposition 4.2. Let $\tau \in S_n$, and $(a_1, \dots, a_n)$ be a cycle, then

$$\tau^{-1}(a_1, \dots, a_n)\tau = (\tau^{-1}(a_1), \dots, \tau^{-1}(a_n))$$

Theorem 4.4. σ_1, σ_2 are conjugates of each other if and only if they have the same type.

In other words, one type of $\sigma \in S_n$ corresponds to one conjugacy class.

Proof. Disjoint cycles are still disjoint under conjugation (since it's a bijection). And if they have the same type, one can define $\tau(a_i) = a_i'$ to establish conjugation between the two elements in S_n. □

Theorem 4.5 (Conjugacy in S_n)**.** The number of conjugacy classes in S_n is the number of partitions of n.

Theorem 4.6. There are 5 conjugacy classes $[\sigma]_{S_n}$ of even permutations in S_n, but there are 6 conjugacy classes $[\sigma]_{A_n}$, as the type $[5]$ splits due to prop 4.15.

4.2 IV.5 Short exact sequences

Definition 4.2 (short exact sequence)**.** Let N, H be groups, and α, β be homomorphisms, then an exact short sequence is the following:

$$1 \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1$$

where α is injective and β is surjective, and $\ker(\beta) = Im(\alpha)$.

A short exact sequence is said to split if H can be realized as a subgroup of G, and $H \cap N = \{e\}$.

Chapter 5

Irreducibility and Factorization in ID

Theorem 5.1 (Hilbert basis theorem). Let R be a Noetherian ring, then $R[x]$ is also a Noetherian ring.

This implies that if I is an ideal of $R[x]$, then $R[x]/I$ is also Noetherian (the ideals of $R[x]/I$ can be identified with ideals of $R[x]$ containing I.)

5.1 Prime and irredubile elements

Let R be a commutative ring for everything below.

Definition 5.1. Let $a, b, c \in R$, we say $a|b$ if there exists c such that $a = bc$, i.e. $a \in (b)$. Moreover, a, b are associates if $(a) = (b)$, i.e., if $a|b, or b|a$.

Proposition 5.1. In an integral domain R, a, b are associates if and only if $a = bc$ for some unit c.

Definition 5.2 (prime, irreducible elements). Let R be an integral domain. An element $a \in R$ is prime if and only if (a) is prime. In other words, if a is not a unit and $a|bc$, then $a|b$, or $a|c$.

An element a is irreducible if and only if a is not a unit and $a = bc$, then either b or c is a unit.

Proposition 5.2. In a PID, prime ideals are maximal ideals.

Proof. You can proceed directly. Alternatively, let (a) be a prime ideal, then a is irreducible, if $(a) \subset (b)$, then $b|a$, hence $a = be$ for some e. a is irreducible implies that either b or e is a unit.

Alternatively, (a) prime, a is irreducible, then (a) is maximal in principal ideals, i.e., in all ideals (in a PID), then (a) is maximal. □

Proposition 5.3.

1. $\mathbb{Z}[x]$ is a UFD, but no PID.
2. In a PID, the greatest common divisor of a, b can be rewritten as a linear combination of them.

Theorem 5.2 (Simple facts you should know). Let $a, b \in R$,

1. if $a = br$, for some $r \in R$, then $(a) \subset (b)$
2. if $a = be$ for some unit e, then $(a) = (b)$.

Theorem 5.3 (Gauss's lemma). Let $f, g \in R[x]$, then $cont(fg) = cont(f)cont(g)$.

5.2 Exercises

Exercise 5.1 (1.12). Let R be an integral domain, then a is irreducible if and only if (a) is maximal among the proper principal ideals.

Proof. a is irreducible if and only if $a = bc$ implies either b or c is a unit. Let $(a) = (b)$, if b is a unit, then $(b) = (1)$; if (c) is a unit, then $(a) = (b)$ (by Lem 1.5, where $(a) = (b)$ if and only if $a = bc$ for some unit c). □

Exercise 5.2 (1.13). Showing that in $\mathbb{Z}$, a is irreducible if and only if a is nonzero and prime.

Proof. In integral domains, nonzero prime elements are always irreducible. Now assume a is irreducible, then (a) is maximal since $\mathbb{Z}$ is a PID, and maximal ideals are always prime, hence (a) is prime. □

Example 5.1. Show that $x^2 + y^2 - 1$ is not irreducible in $\mathbb{C}[x, y]$.

We can view $\mathbb{C}[x, y] = \mathbb{C}[x][y]$, then $(x - 1)$ is prime in $\mathbb{C}[x]$, and it follows the Eisenstein's criterion that the polynomial is indeed irreducible.

Chapter 6

Definition and Theorem List

6.0.1 groups

Proposition 6.1. Cancellation holds in groups, i.e., if $g_1 a = g_2 a$, then $g_1 = g_2$.

Definition 6.1 (order)**.** An order of an element g is the smallest positive integer n such that $g^n = e$, denoted $|g|$, and $|g| = \infty$ if it does not have finite order.

Proposition 6.2. If $g^k = e$ for some k, then $|g|$ divides k.

Proposition 6.3. Let $g \in G$ have finite order, then g^m also has finite order, and

$$|g^m| = \frac{|g|}{\gcd(m, |g|)}$$

The next one concerns with the order of commuting elements.

Proposition 6.4. If $gh = hg$, then $|gh|$ divides $lcm(|g|, |h|)$.

Definition 6.2 (symmetric group)**.** The symmetric group S_n is the group $\mathrm{Aut}\{1, \ldots, n\}$, i.e., the group of permutations of $\{1, \ldots, n\}$.

Definition 6.3 (Dihedral group)**.** The dihedral group D_{2n} is the group of rotations and reflections of a n-polygon. There are n rotations and n reflections, hence $2n$ elements.

Warning 6.1. Symmetries in D_{2n} corresponds to permutations in S_n, and you can view D_{2n} acting faithfully on the set $\{1, \ldots, n\}$.

Definition 6.4 (modulo)**.** An equivalence relation defined on $\mathbb{Z}$ with modulo:

$$a \equiv b \mod n \iff n \mid (b - a)$$

Proposition 6.5. If $a \equiv a' \mod n$ and $b \equiv b' \mod n$, then $a + b = a' + b' \mod n$. In other words, the cosets addition is well-defined.

Proposition 6.6. The order of $m \in \mathbb{Z}/n\mathbb{Z}$ is 1 if $n \mid m$, and

$$|m| = \frac{n}{\gcd(m, n)}$$

Then we have the next quite important statement.

Theorem 6.2. $m \in \mathbb{Z}/n\mathbb{Z}$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(m, n)$.

Warning 6.3. This means that every element in $\mathbb{Z}/p\mathbb{Z}$ generates it.

Definition 6.5 (multiplicative group)**.** Let $(\mathbb{Z}/n\mathbb{Z})* := \{m \in \mathbb{Z}/n\mathbb{Z} : \gcd(m, n) = 1\}$, this is a group with the multiplication operation $(a \mod n) \cdot (b \mod n) = ab \mod n$.

Proposition 6.7. Let $\varphi : G \to H$ be a group homomorphism, then $\varphi(e_G) = e_H$, and $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Proposition 6.8. The trivial group is both initial and final in Grp. (recall initial is there exists only one homomorphism from $\{e\}$ to any group, and final is there exists only one homomorphism from any group to $\{e\}$).

Now we see how homomorphisms work with order.

Proposition 6.9. Let $\varphi : G \to H$ be a group homomorphism, and let $g \in G$ be an element of finite order, then $|\varphi(g)|$ divides $|g|$.

Definition 6.6 (cyclic)**.** A group is cyclic if it is isomorphic to $\mathbb{Z}$ or to $\mathbb{Z}/n\mathbb{Z}$.

Proposition 6.10. Let $\varphi : G \to H$ be an isomorphism, then for all $g \in G$, $|\varphi(g)| = |g|$. And G is commutative if and only if H is commutative.

Theorem 6.4. Two *commutative* finite groups are isomorphic if and only if they have the same number of elements of any given order.

Example 6.1. S_3 and $\mathbb{Z}/6\mathbb{Z}$ are not isomorphic, since one is abelian, one isn't.

Definition 6.7 (group of homomorphisms)**.** Let H be commutative, then $\hom(G, H)$ is a commutative group for all group G.

6.0.2 Subgroups

Proposition 6.11. If $\{H_\alpha\}_{\alpha\in A}$ is any family of subgroups a group G, then $H = \bigcap_\alpha H_\alpha$ is a subgroup of G.

Definition 6.8 (finitely generated). A group G is finitely generated if there exists a finite subset

$$\{a_1, \dots, a_n\} \subset G$$

such that $G = \langle a_1, \dots, a_n \rangle$.

Proposition 6.12. Subgroups of cyclic groups are cyclic.

Proposition 6.13. Let $G \subset \mathbb{Z}$ be a subgroup, then $G = d\mathbb{Z}$ for some $d \geq 0$. And every subgroup of $\mathbb{Z}$ is isomorphic to $\mathbb{Z}$.

Proposition 6.14. Let $n > 0$ be an integer and let $G \subset \mathbb{Z}/n\mathbb{Z}$ be a subgroup, then G is a cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by some $d \in \mathbb{Z}/n\mathbb{Z}$, and $d \mid n$.

Proposition 6.15. Let $\varphi : G \to H$ be a homomorphism, then the following are equivalent:

1. φ is monic
2. $\ker \varphi = \{e_G\}$.
3. $\varphi; G \to G'$ is injective as a set function.

monic means that for any group G', and two homomorphisms $f, g : G' \to G$, if $\varphi \circ f = \varphi \circ g$, then $f = g$.

6.0.3 Quotient groups

Definition 6.9 (normal subgroup). A subgroup $N \subset G$ is normal if for all $g \in G$,

$$gNg^{-1} \in N$$

Definition 6.10 (quotient group). Let H be a normal subgroup of a group G, then the quotient group G/H is the group obtained by cosets, group operation defined by

$$(aH)(bH) := (ab)H$$

Theorem 6.5 (first homomorphism theorem). Let H be a normal subgroup, then for every group homomorphism $\varphi : G \to G'$ such that $H \subset \ker \varphi$, there exists a unique homomorphism $\tilde{\varphi} : G/H \to G'$ such that

$$\varphi = \tilde{\varphi} \circ \pi$$

where $\tilde{\varphi}(aH) = \varphi(a)$.

Corollary 6.1. Let $\varphi : G \to G'$ be a surjective homomorphism, then

$$G/\ker\varphi \cong G'$$

Proposition 6.16. Let H be a normal subgroup, and K is any subgroup containing H, then there is a bijection between K and a subgroup of G/H, defined by $u(K) = K/H$. In other words, a subgroup of K containing H is a collection of cosets in G/H.

Theorem 6.6 (fraction holds)**.** Let H, N to be normal subgroups of G, then

$$\frac{G/H}{N/H} \cong G/N$$

Theorem 6.7 (second homomorphism theorem)**.** Let H, K be subgroups and H is normal, then

1. HK is a subgroup of G, and H is normal in HK.
2. $H \cap K$ is normal in K, and
$$\frac{HK}{H} \cong \frac{K}{H \cap K}$$

6.0.4 Lagrange's theorem

Definition 6.11 (index)**.** Let H be a normal subgroup, the index is the number of cosets of H in G, i.e., the number of elements in the quotient group G/H.

Proposition 6.17. Let H be a subgroup of a group G. then for all $g \in G$, the functions

$$H \to gH, h \mapsto gh$$

is a bijection.

Theorem 6.8 (Lagrange's theorem)**.** If G is a finite group, and H is a subgroup, then $|G| = [G : H] \cdot |H|$. In particular, $|H|$ divides $|G|$.

Corollary 6.2. The order of any element $|g|$ divides the order of the group.

Example 6.2. Let G be any group of order p, then the group is cyclic and abelian. In other words, the group is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Proof. Let $g \in G$ be any element that is not e, then $G \cong \langle g \rangle$, hence is cyclic of order p. □

Theorem 6.9 (Fermat's last theorem)**.** Let p be any prime integer, and let a be any integer, then

$$a^p \equiv a \mod p$$

6.0.5 group actions

Definition 6.12 (action). An action of a group G on a set A is a set-function $\rho : G \times A \to A$ such that $e \cdot a = a$, and for all $g, h \in G$, and $a \in A$, associativity holds

$$gh \cdot a = g \cdot (h \cdot a)$$

Example 6.3. G acts by left-multiplication on the set G/H of left-cosets, sending aH to gaH.

Definition 6.13 (transitive action). An action of a group G on a set A is transitive if for all $a, b \in A$, there exists $g \in G$, such that

$$b = g \cdot a$$

In other words, every element can be expressed as another element under an action.

Definition 6.14 (orbit). The orbit of $a \in A$ under an action of a group G is the set

$$O(a) = \{g \cdot a : g \in G\}$$

Definition 6.15 (stabilizer). Let G act on a set A, and let $a \in A$, the stabilizer is the subroup of G which fix a.

$$\text{Stab}(a) = \{g \in G : g \cdot a = a\}$$

Proposition 6.18. Orbits form a partition of the set A. The action of G acts transitively on any orbit.

Proposition 6.19. Every transitive left-action of G on a nonempty set A is isomorphic to the left-multiplication of G on G/H, H = the stabilizer of any $a \in A$. More precisely, if G acts transitively on A, then $|A|$ divides $|G|$.

For example, let G' be a group, and G acts on G', then

$$G/Stab(a) \cong O(a)$$

where $a \in G'$, and $O(a)$ is the orbit of a. The isomorphism map is defined by $\varphi(gStab(a)) = g \cdot a$.

Theorem 6.10. If $O(a)$ is an orbit of a finite group G, then $|O(a)|$ divides $|G|$. In other words,

$$|O(a)| \cdot |Stab(a)| = |G|$$

Example 6.4. There are no transitive actions of S_3 on a set of 5 elements. This is because transitive actions induce an isomorphism, and 5 does not divide 6.

Proposition 6.20. Suppose a group G acts on a set A, and let $a \in A, g \in G$. Let $b = g \cdot a$, then

$$Stab(b) = gStab(a)g^{-1}$$

Now if $Stab(a)$ is normal, then stabilizers for all g is the same.

6.1 Chapter III: Rings and Modules

In a ring, we have $0 \times r = 0$.

Definition 6.16 (integral domain). A nonzero commutative ring R is an integral domain if for all $a, b \in R$, such that $ab = 0$, we have either $a = 0$ or $b = 0$.

Warning 6.11. $\mathbb{Z}$ is an integral domain, a UFD, a PID, even an Euclidean domain.

Definition 6.17 (zero divisor). a is a zero divisor if there exists nonzero v such that $av = 0$.

Proposition 6.21. In a commutative ring, a is not a zero divisor if and only if multiplication by a is injective from $R \to R$.

Proposition 6.22. Let R be a commutative ring, then u is a unit if and only if multiplication by u is surjective from R to R, if and only if it is injective, i.e. u is not a zero divisor.

Definition 6.18 (field). A field is a nonzero commutative ring R in which every nonzero element is a unit.

Theorem 6.12. Finite integral domains are fields.

Definition 6.19 (polynomial rings). Let R be a ring, a polynomial ring $R[x]$ is a collection of polynomials with operations: $f(x) = \sum a_i x^i$, and $g(x) = \sum b_i x^i$ as

$$f(x) + g(x) = \sum (a_i + b_i) x^i$$

$$f(x) \cdot g(x) = \sum_k \sum_{i+j=k} a_i b_j x^{i+j}$$

Definition 6.20 (ring homomorphism). Let $\varphi : R \to S$ be a ring homomorphism, then for all $a, b \in R$,

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = \varphi(a)\varphi(b)$$

and $\varphi(1_R) = 1_S$.

Proposition 6.23.

$$End(\mathbb{Z}) \cong \mathbb{Z}$$

defined by $\varphi(f) = f(1)$.

Proposition 6.24. Let R be a ring, then the function $r \mapsto \lambda_r$ is an injective ring homomorphism $R \to End(R)$, where $\lambda_r(a) = ra$.

6.1.1 Ideals and quotient rings

Definition 6.21 (ideal). Let R be a commutative ring, a subgroup I (under addition) is an ideal of R if for all $r \in R$, and $rI \subset I$.

Remark: the only ideal of a ring R containing 1 is R itself.

Definition 6.22 (kernel of a ring homomorphism). Let $\varphi : R \to S$ be a ring homomorphism, then $\ker \varphi = \{r \in R : \varphi(r) = 0\}$. Note that $\ker \varphi$ is an ideal of R.

Definition 6.23 (quotient ring). Let I be an ideal, hence a normal subgroup of R under addition, and R/I is a ring, with the following operations:

$$(a + I) + (b + I) = (a + b) + I$$

$$(a + I)(b + I) = (ab) + I$$

For a ring R, let $f : \mathbb{Z} \to R$ be the unique ring homomorphism, defined by $a \mapsto a \cdot 1_R$. Then $\ker f = n\mathbb{Z}$.

Definition 6.24 (characteristic). The characteristic of a ring R is the smallest n such that $1 \cdot n = 0$. In other words, $char(R)$ is the order of 1.

Alternatively, the characteristic of R is the above n.

Theorem 6.13 (first homomorphism theorem). Let I be an ideal of a commutative ring R, then for every ring homomorphism $\varphi : R \to S$ such that $I \subset \ker \varphi$, there exists a unique homomorphism $\tilde{\varphi}$ such that

$$\varphi = \tilde{\varphi} \circ \pi$$

where $\tilde{\varphi}$ is defined by $\tilde{\varphi}(r + I) = \varphi(r)$.

Just like the group homomorphism, then subgroups J of R containing I can be identified with subgroups of R/I, defined by $u(J) = J/I$.

Theorem 6.14 (fraction holds). Let I be an ideal of a ring R, and J be an ideal containing I, then J/I is an ideal of R/I, and

$$\frac{R/I}{J/I} \cong R/J$$

Definition 6.25 (principal ideal). A principal ideal is an ideal of R such that it is generated by one element aR, denoted by (a).

Proposition 6.25. The sum of ideals is an ideal. (the sum can be arbitrary). If $I_1, \ldots, I_n$ are ideals, then $\sum_i I_j$ is also an ideal. (like how sum of subspaces of a vector space is a subspace).

In particular, the sum of principal ideals is also an ideal, $I = \sum_i (a_i)$, where elements of this ideal are of the form $r_1 a_1 + \cdots + r_n a_n$.

Definition 6.26 (finitely generated). If a ring can be written as

$$R = \sum_{i=1}^{n} (a_i)$$

then we say this ring is finitely generated.

Definition 6.27 (Noetherian). A ring R is Noetherian if every ideal I of R is finitely generated.

Definition 6.28 (PID). An integral domain R is a PID if every ideal of R is principal.

Example 6.5. $\mathbb{Z}, k[x]$ for field k are PID. $\mathbb{Z}[x]$ is not a PID, since $(2, x)$ is not a principal ideal.

Chapter 7

Fields and Galois theory

Definition 7.1.

Chapter 8

Taylor 1: Complex Calculus

We will start with the basics.

Definition 8.1 (convergence). $\{z_n\} \subset \mathbb{C}$ converges to z if and only if $|z_n - z| \to 0$ as $n \to \infty$. ($z_n = x_n + iy_n$ this is iff $x_n \to x, y_n \to y$).

We note that every complex Cauchy sequence converges because every real Cauchy sequence converges.

Definition 8.2 (absolutely convergent). We say a series is absolutely convergent $\sum_{k=0}^{\infty}$ if

$$\sum_{k=0}^{\infty} |a_k| < \infty$$

Proposition 8.1. If $\sum_{k=0}^{\infty} a_k z^k$ converges at $z_1 \neq 0$, then either this series converges absolutely for all $z \in \mathbb{C}$, or there exists R such that it is absolutely convergent for all $|z| < R$, and divergent for $|z| > R$ (R is called the radius of convergence).

Proof. We know $\sum a_k z_1^k$ converges hence $|a_k z_1^k| \leq C$ for all k. Then for $|z| \leq r|z_1|$ for some $r < 1$, we have $\sum |a_k z^k| \leq C \sum r^k < \infty$. This shows that the series converges absolutely for $|z| < R$ for some R. □

Example 8.1. $f(z) = z^2$ is maps the upper half plane $\mathbb{H}$ surjectively onto $\mathbb{C} \setminus \mathbb{R}^-$, where $\mathbb{R} = (-\infty, 0]$).

Theorem 8.1 (Cauchy's integral theorem). Let $f \in C^1(\overline{\Omega})$ be holomorphic on Ω, then

$$\int_{\partial\Omega} f(z)dz = 0$$

Proof. This follows from Green's theorem.

$$\int_{\partial\Omega} f dz = \int_{\partial\Omega} f dx + if dy = \int\int i\frac{\partial f}{\partial x} - \frac{\partial f}{\partial y} dxdy = 0$$

the RHS is 0 by Cauchy-Riemann equations for f being holomorhpic. □

Theorem 8.2 (Cauchy's integral formula)**.** Let $f \in C^1(\overline{\Omega})$, then for $z \in \Omega$, then

$$f(z) = \frac{1}{2\pi i} \int_{\partial\Omega} \frac{f(\zeta)}{(\zeta - z)} d\zeta$$

Proof. This follows from shrinking $\int_{\partial\Omega}$ to $\int_{\partial D_r}$ with D_r centered at z, then parametrizing. □

Proposition 8.2 (Mean value property)**.** Let $z_0 \in \Omega$, then

$$f(z_0) = \frac{1}{2\pi} \int_0^{2\pi} f(z_0 + re^{i\theta}) d\theta$$

whenever the closure of $D_r \subset \Omega$.

Note that one can keep differentiate the Cauchy integral formula, we get

$$f'(z) = \frac{1}{2\pi i} \int_{\partial\Omega} \frac{f(\zeta)}{(\zeta - z)^2} d\zeta$$

Moreover, we have

$$f^{(n)}(z) = \frac{n!}{2\pi i} \int_{\partial\Omega} \frac{f(\zeta)}{(\zeta - z)^{n+1}} d\zeta$$

Now we reach a strong conclusion where every holomorphic f can be written as a power series about any point $z \in \Omega$.

Proposition 8.3. If $f \in C^1(\overline{\Omega})$ is holomorhpic, then $z \in D_r(z_0) \subset \Omega$, then $f(z)$ has a convergent power series

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n = \sum_{n=0}^{\infty} \frac{f^{(n)}(z_0)}{n!} (z - z_0)^n$$

Chapter 9

Stein 1: preliminaries to complex analysis

We start with simple formulas for complex numbers.

$$Re(z) = \frac{z+\overline{z}}{2}, Im(z) = \frac{z-\overline{z}}{2i}, |z|^2 = z\overline{z}, |z^n| = |z|^n$$

Moreover,

$$e^{i\theta} = \cos(\theta) + i\sin(\theta)$$

We also know that $\mathbb{C}$ is complete and a set $\Omega \subset \mathbb{C}$ is compact if and only if it it closed and bounded. In $\mathbb{C}$, a set is compact if and only if for any open covering of Ω, there exists a finite subcover.

Definition 9.1 (connected). A set Ω is connected if there doesn't exist open sets U, V such that $\Omega = U \bigcup V$.(A connected open set in $\mathbb{C}$ is called a region.)

Equivalently, Ω is connected if for any $p, q \in \Omega$, there exists a path γ connecting p, q such that $\gamma \subset \Omega$.

Next we discuss holomorphic functions.

Proposition 9.1 (Cauchy-Riemann Equations). Let f be holomorphic in Ω, then for $z \in \Omega$, we have

$$\frac{\partial f}{\partial x} + i\frac{\partial f}{\partial y} = 0$$

Equivalently, we have

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}$$

If we further define differentiate with respect to z in terms of x, y, we have

Definition 9.2 (derivative wrt z). We define the operators as follows:

$$\frac{\partial f}{\partial z} = \frac{1}{2}\left(\frac{\partial f}{\partial x} + \frac{1}{i}\frac{\partial f}{\partial y}\right)$$

$$\frac{\partial f}{\partial \overline{z}} = \frac{1}{2}\left(\frac{\partial f}{\partial x} - \frac{1}{i}\frac{\partial f}{\partial y}\right)$$

Then we immediately have the following:

Proposition 9.2. Let f be holomorphic on Ω, then we have for $z \in \Omega$,

$$\frac{\partial f}{\partial \overline{z}} = 0, \frac{\partial f}{\partial z}(z) = 2\frac{\partial u}{\partial z}(z)$$

So it's clear that holomorphic implies Cauchy-Riemann equations, but it doesn't go exactly conversely. In fact, if f satisfies the CR equations and if u, v are continuously differentiable, then f is holomorphic.

Definition 9.3 (radius of convergence)**.** For a power series $\sum_{n=0}^{\infty} a_n z^n$, the radius of convergence R is as follows:

$$1/R = \limsup_{n\to\infty} |a_n|^{1/n}$$

We note that $R = \infty$ for e^z, and $R = 1$ for geometric functions.

Proposition 9.3. Let $f(z) = \sum_{n=0}^{\infty} a_n z^n$, then $f'(z) = \sum_{n=1}^{\infty} n a_n z^{n-1}$, f' has the same radius of convergence as f.

Chapter 10

Stein 2: Cauchy's integral theorem and applications

We state Goursat's theorem.

Theorem 10.1 (Goursat)**.** If Ω is a region in $\mathbb{C}$, and $T \subset \Omega$ a triangle whose interior is also contained in Ω, if f is holomorphic, then

$$\int_T f(z)dz = 0$$

This implies for any rectangle R, if f is holomorphic, then $\int_R f(z)dz = 0$. Before we state the Cauchy's integral theorem, we state the following.

Theorem 10.2 (primitive exists)**.** Let f be holomorphic on an open disk D, then f has a primitive on this disk.

Proof. You define the primitive as $F(z) = \int_\gamma f(w)dw$, where γ is the line connecting the origin and z. □

This give Cauchy's theorem.

Theorem 10.3 (Cauchy's theorem)**.** If f is holomorphic in a disk, then for any $\gamma \subset D$, we have

$$\int_\gamma f(z)dz = 0$$

Chapter 11

Stein III: Meromorphic functions

Definition 11.1 (meromorphic function). f is meromorphic if there exists a set of points $\{z_1, z_2, \ldots\}$ that has no limit point in Ω such that f is holomorphic in the punctured disk and has poles at these points $\{z_1, z_2, \ldots\}$.

Chapter 12

Folland

Theorem 12.1 (monotone convergence theorem). For a sequence of f_n nonnegative such that $f_1 \leq f_2 \leq \ldots$, such that $\lim_{n\to\infty} f_n = f$, for some f. Then we have

$$\lim_{n\to\infty} \int f_n d\mu = \int f d\mu$$

Definition 12.1 (σ-algebra). A σ-algebra is a family of set that is closed under countable unions and complements.

Definition 12.2 (measure). A measure on a sigma algebra $\mathcal{M}$ if a function $\mu : \mathcal{M} \to [0, \infty]$ such that

1. $\mu(\varnothing) = 0$
2. $\{E_j\}_1^\infty$ is a sequence of disjoint sets in $\mathcal{M}$, then

$$\mu\left(\bigcup_1^\infty E_j\right) = \sum_1^\infty \mu(E_j)$$

(gives emptyset measure 0 and is countably additive, note that it requires disjointness).

Definition 12.3 (σ-finte). A measure space $(X, \mathcal{M})$ is called σ-finite if $X = \bigcup_{j=1}^\infty E_j$, and for each j, $\mu(E_j) < \infty$.

Proposition 12.1 (measure). Let $(X, \mathcal{M}, \mu)$ be a measure space, then

1. (monotonicity) if $E, F \in \mathcal{M}$, and $E \subset F$, then $\mu(E) < \mu(F)$.
2. (non-disjoint sets) for $\{E_j\}_1^\infty$, we have $\mu(\bigcup_j E_j) \leq \sum_1^\infty \mu(E_j)$.
3. (continuity) If $E_1 \subset E_2 \subset \ldots$, then $\mu(\bigcup_j E_j) = \lim_{j\to\infty} \mu(E_j)$
4. (continuity) If $E_1 \supset E_2 \ldots$, and $\mu(E_1) < \infty$, then

$$\mu(\cap_j E_j) = \lim_{j\to\infty} \mu(E_j)$$

Definition 12.4 (complete measure space). A measure space $\mathcal{M}$ is complete if $\mathcal{M}$ contains all subsets of null sets, i.e. if for E, we have $\mu(E) = 0$, then $F \subset E$, we have $F \in \mathcal{M}$ as well.