

Prelim Review

Hui Sun

July 4, 2024

Contents

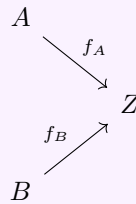
1	Category Theory-Aluffi I.5	3
2	Aluffi II	4
3	Aluffi III: Rings and Modules	10
4	Taylor 1: Complex Calculus	13

Chapter 1

Category Theory-Aluffi I.5

Definition 1.1 (initial, final). Let C be a category. We say $I \in \text{Obj}(C)$ is **initial** if for every $A \in \text{Obj}(C)$, there exists exactly one morphism $f : I \rightarrow A$. (In other words, $\text{Hom}(I, A)$ is a singleton). We say $F \in \text{Obj}(C)$ is **final** if for every $B \in \text{Obj}(C)$, $\text{Hom}(B, F)$ 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 $i_A : A \rightarrow A \amalg B$, $i_B : B \rightarrow A \amalg B$ with the following universal property: for all objects $Z \in \text{Obj}(C)$ and for all morphisms f_A, f_B such that



there exists a unique $\sigma : A \amalg B \rightarrow Z$ 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,

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

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 $|g| \leq |G|$. \square

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 (Dihedral 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 $\gcd(m, n) = 1$. \square

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. \square

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 $G = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \dots$, 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 $\varphi : S_3 \rightarrow \mathbb{Z}/2\mathbb{Z}$ 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 $\varphi : G \rightarrow H$ be a homomorphism, then $\varphi([A, G]) \subset \ker(\varphi)$.

Moreover, one can show that any homomorphism $\varphi : S_3 \rightarrow \mathbb{Z}/2\mathbb{Z}$ should send all elements of order 2 to 0, or all to 1. One can either use the determinant map $\det : S_3 \rightarrow \{\pm 1\}$, 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 $\varphi : \mathbb{Q} \rightarrow \mathbb{Q}$ 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 $\mathbb{Z} \rightarrow \mathbb{Z}$ 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. $\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ is a ring, with the group being under addition of maps. $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ 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 $\varphi : G \rightarrow G'$ determines two subgroups naturally, $\ker(\varphi) \subset G$, $\text{Im}(\varphi) \subset G'$. 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 $\varphi : G \rightarrow H$ 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 $\varphi : G \rightarrow G'$ as a monic morphism means φ is injective. If we consider

$$\ker(\varphi) \xrightarrow[e]{i} G \xrightarrow{\varphi} G'$$

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 $\pi : F(S) \rightarrow G$ 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. \square

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

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

Proof. Let $\tilde{\varphi}([a]) := \varphi(a)$. Then $\text{Im}(\tilde{\varphi})$ 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. \square

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,

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

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

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

Lemma 2.2. For H normal in G , the usual projection $\pi : G \rightarrow G/H$, 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 homomorphism from $G \rightarrow G$, 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 $G/H \rightarrow \text{Aut}(G)$, 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 $G/H \rightarrow \text{Aut}(H)$ is well-defined.

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

1. $\bar{f} : G/H \rightarrow G'$ 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 $\rho : G \times A \rightarrow A$ 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

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

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 any 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. \square

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 $\varphi : G/H \rightarrow A$, where $H = \text{Stab}(a)$ for any $a \in A$, by $\varphi : gH \mapsto g \cdot a$. Then by Lagrange's, we know $|G| = |A| \cdot |H|$. \square

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 $\sigma : G \rightarrow S_p$ 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. \square

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. \square

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. \square

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: $am = 1 \pmod n$, 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. \square

Example 3.4. Let I be an ideal, $\varphi : R \rightarrow S$ 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 $k[x_1, \dots, x_n]$ has dimension n , where $(x_1) \subset (x_1, x_2) \subset \dots \subset (x_1, \dots, x_n)$.

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 $r \in I$. \square

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, $r \in IJ$.

Chapter 4

Taylor 1: Complex Calculus

We will start with the basics.

Definition 4.1 (convergence). $\{z_n\} \subset \mathbb{C}$ converges to z if and only if $|z_n - z| \rightarrow 0$ as $n \rightarrow \infty$. ($z_n = x_n + iy_n$ this is iff $x_n \rightarrow x, y_n \rightarrow y$).

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

Definition 4.2 (absolutely convergent). We say a series is absolutely convergent $\sum_{k=0}^{\infty}$ if

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

Proposition 4.1. If $\sum_{k=0}^{\infty} a_k z_1^k$ 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 . \square