The Objects in Higher Mathematics

a dictionary of higher maths

Jay Zhao

Contents

§1. Fundamentals

§1. 1. Binary Operation

A binary operation $\bullet$ is a rule for combining two elements from a set to produce another element in the set. It can be defined as a function $\bullet : S \times S \to S$.

Common properties of binary operations:
- **Associativity** $a \bullet b = b \bullet a$ for all a and b.
- **Closure** $a, b \in S \Rightarrow a \bullet b \in S$.
- **Commutativity** $a \bullet b = b \bullet a$ for all a and b.
- **Identity** an identity element e is an element where $e \bullet x$ is x. for all x
- **Inverse** an inverse element of a is an element such that $a \bullet a^{-1} = e$

§1. 2. Binary Relationships

A binary relationship $\rightarrowtail$ over a set A to a set B is a subset of the cartesian product

$$(\rightarrowtail) \subseteq A \times B$$

If $(a, b) \in R$, we write $a \rightarrowtail b$, meaning "a is related to b".

Common properties of binary relationships:
- **Reflexivity** $a \rightarrowtail a$ for all a
- **Symmetric** $a \rightarrowtail b \Rightarrow b \rightarrowtail a$
- **Antisymmetric** $a \rightarrowtail b$ and $b \rightarrowtail a$ only if $a = b$
- **Transitive** $a \rightarrowtail b$ and $b \rightarrowtail c \Rightarrow a \rightarrowtail c$

Special types of binary relationship:
- **Partial Ordering** a partial ordering is a binary relationship that is:
  1. Reflexive
  2. Transitive
  3. Antisymmetric
- **Total Ordering** a total ordering is a partial ordering where for for every pair of elements a, b either $(a, b) \in (\rightarrowtail)$ or $(b, a) \in (\rightarrowtail)$.
- **Equivalence Relationships** an equivalence relationship is a binary relationship that is:
  1. Reflexive
  2. Symmetric
  3. Transitive

§1. 3. Functions

- The **pre-image** $f^{-1}(T)$ is the set of all $x \in X$ such that $f(x) \in T$.
- The **image** $f(S)$ is the set $\{f(x) \mid x \in S\}$

§2. Groups

§2. 1. Groups and Subgroups

Groups A set G is considered to be a group under the binary operation $\bullet$, denoted $(G, \bullet)$ if together the following *four* conditions are met:

1. **Closure** $a, b \in G \Rightarrow a \bullet b \in G$.
2. **Associativity** $a \times (b \bullet c) = (a \bullet b) \bullet c$. *So the order of evaluation doesn't matter.*
3. **Identity** There is an element $e \in G$ such that $\forall x \in G, e \bullet g = g = g \bullet e$.
4. **Inverse** For every element $x \in G$ there is another element x^{-1} such that $x \bullet x^{-1} = e$.

Remark: A group is a monoid each of whose elements is invertible

We love groups because this is just enough information to represent any closed set of permutations. This is formalized by ☂ Theorem 2.3.1.

Order The order of a finite group G is the total number of elements in G. The order of an element $g \in G$ is the smallest positive integer n such that $g^g = e$.

Subgroup a subgroup is a subset of $(G, \bullet)$ which is also a group under $\bullet$.

> ☂ **Theorem 2.1.1** (Lagrange's Theorem): if G is a finite group and $H \subseteq G$ then the order of H divides the order of G

Index The index of a subgroup written $[G : H]$ is the number of left co-sets of H in G.

Abelian Group A group $(G, \bullet)$ is abelian if $\bullet$ is commutative, a group is non abelian otherwise. This is actually very interesting see: ☂ Theorem 2.5.1

§2. 2. Subgroup Structures: Center, Centralizer, Normalizer

Orbits The orbit of an element $g \in G$ is the set $\{g, g^2, g^3, \ldots\}$.

Conjugate Elements Two elements a and b are conjugates of one another if $xax^{-1} = b$ for some x. a and b are said to be in the same conjugacy class.

Center The center $Z(G)$ of a group G, is the set of elements $z \in Z(G)$ such that for all $g \in G$ we have that $gz = zg$. This center is always a normal subgroup of G. A group is a abelian if $Z(G) = G$. The conjugacy class of every element of $Z(G)$ is itself only.

Centralizer For a subset S of G, the centralizer of S in G, denoted $C_G(S)$, is the subgroup of G defined by $\{g \in G \mid gs = sg \text{ for all } s \in G\}$. It is the largest subgroup where S is a center.

Normalizer The normalizer $N_G(S)$ of a subgroup S of G is the set $\{g \in G \mid gS = Sg\}$. It is the largest subgroup of G where S is normal.

§2. 3. Homomorphisms and Isomorphisms

Homomorphism Given two groups $(G, \bullet)$ and $(H, \cdot)$, a homomorphism from G to G is a function $h : G \to H$ where $h(a \bullet b) = h(a) \cdot h(b)$ for all a and b in G.

Kernel The kernel of a group homomorphism is the preimage of the identity in the codomain of the group homomorphism.

Isomorphism An isomorphism is a bijective homomorphism.

Automorphism An automorphism of a group is an isomorphism of the group to itself.

☂ **Theorem 2.3.1** (Cayley's Theorem): Every finite group, is isomorphic to a subset of S_n

§2. 4. Normal Subgroups and Quotient Groups

Normal Subgroups A normal subgroup N is the kernel of a group homomorphism and it's also a subgroup N where $gN = Ng$ for all elements $g \in N$. If this is the case we write

$$N \trianglelefteq G$$

Quotient Group Given a group G and a normal subgroup G/N, the quotient group is the group of left cosets of N with $aN \bullet bN = (abN)$. This is where $\mathbb{Z}/n\mathbb{Z}$ comes from.

§2. 5. Direct Products

External Direct Product the external direct product of groups $(G, \bullet)$ and $(H, \cdot)$ is $S = H \times G$ with the binary operation $(h_1, g_1) * (h_2, g_2) = (h_1 \cdot h_2, g \bullet g_2)$. We have that the order of $|h, g| = \operatorname{lcm}(|h|, |g|)$. Written as $G \oplus H$, or just $G \times H$.

☂ **Theorem 2.5.1** (Fundamental Theorem of Abelian Groups): hi

Internal Direct Product If we have two subsets of H and K satisfying:

1. $G = \{hk \mid h \in H, k \in K\}$
2. $H \cap K = \{e\}$
3. $hk = kh$ for all $k \in K$ and $h \in H$

Then G is the internal direct product of H and K.

§2. 6. Group Actions

Remember that groups sort of describe permutations, and they sort of describe symmetries. This is very useful. But to utilize this power we have to map our abstract nonsense to some slightly less abstract nonsense.

Group Action $\alpha : G \times X \to X$ is a group action of G acting on X. Which satisfies:

1. $\alpha(e, x) = x$
2. $\alpha(b, \alpha(a, x)) = \alpha(ba, x)$

Explained in words this is:

1. Applying no action does nothing
2. Applying an action and then another action, is the same as the action of doing one after the other.

Remark: A good conceptual example for the set X is the set of colourings of a necklace or some other object.

Orbits The orbit of $x \in X$ is the set of all configurations equivalent to x by some group action. $\mathrm{Orb}(x) = \{\alpha(g, x) \mid g \in G\}$

Stabilizer The stabilizers of $x \in X$ i the set of all permutations which fix x is the set $\{g \in G \mid \alpha(g, x) = x\}$. This is a subgroup of g.

☂ **Theorem 2.6.1** (Orbit Stabilizer Theorem):

$$|\mathrm{Orb}(x)| \times |\mathrm{Stab}(x)| = |G|$$

We can use this fact to count the number of orbits

$$\text{number of orbits} = \sum \frac{1}{|\mathrm{Orb}(x)|} = \frac{1}{|G|} \sum |\mathrm{Stab(x)}| = \frac{1}{|G|} \sum |\mathrm{Inv}(g)|$$

where $\mathrm{Inv}(g) = \{x \in X \mid \alpha(g, x) = x\}$.

🧡 **Corollary 2.6.1.1** (Burnside's Lemma):

$$|\mathrm{Classes}| = \frac{1}{|G|} \sum |I(g)|$$

§2. 7. Sylow Theorems

Theorem 2.7.1 (The Sylow Theorems): Let G be a group of order $p^n m$ where $(p, m) = 1$. A **Sylow p-group** is a subgroup of order p^n. Let n_p be the number of Sylow p-subgroups of G. Then

1. $n_p \equiv (1 \bmod p)$.
2. $n_p \mid m$
3. Any two Sylow p-subgroups are conjugate subgroups and isomorphic.

§2. 8. The PID structure Theorem

An abelian group G is **finitely generated** if it is finitely generated as a $\mathbb{Z}$-module. So

$$G = \{a_1 g_1 + a_2 g_2 + \ldots + a_n g_n \mid a_i \in \mathbb{Z}, g_i \in G\}$$

Theorem 2.8.1 (Fundamental Theorem of finitely generated abelian groups): Let G be a finitely generated abelian group. Then there exists an integer r, prime powers $q_1, \ldots q_m$ (not necessarily distinct) such that

$$G \cong \mathbb{Z}^{\oplus r} \oplus Z/q_1\mathbb{Z} \oplus \cdot \oplus \mathbb{Z}/q_m\mathbb{Z}$$

§3. Rings

Rings A set R is considered to be a ring under the binary operations $+$ and $\times$, written as $(R, +, \times)$. If the following conditions are met:

1. $(R, +)$ is an abelian group with identity 0.
2. $\times$ is an associative operation with identity 1 (no inverse necessarily).
3. Multiplication distributes over addition.

A ring $(R, +, \times)$ is said to be commutative if $\times$ is commutative.

Product Rings The product ring of two rings R and S is is the set of elements $R \times S$ and where the multiplication and addition operations are done pairwise.

Polynomial Ring Given any ring we can form a polynomial ring as the set of polynomials with coefficients in R.

$$R[x] = \{a_n x^n + \ldots + a_0\}$$

This is pronounced R "adjoin" x

Multivariable Polynomial Rings We can consider polynomials in n variables with coefficients in R denoted $R[x_1, x_2, \ldots, x_n]$

Unit A unit of a ring is an element of a ring with an inverse.

§3. 1. Homomorphisms

Homomorphism Let R and S be rings, a homomorphism is a map $\phi : R \to S$ where

1. $\phi(x + y) = \phi(x) + \phi(y)$
2. $\phi(x \times y) = \phi(x) \times \phi(y)$
3. $\varphi(1) = 1$

Isomorphism A ring isomorphism is a bijective ring homomorphism.

§3. 2. Ideals

The ideal is the equivalent of the normal subgroup for rings.

Kernel The kernel of a ring homomorphism is the set of $r \in R$ such that $\phi(r) = 0$.

Ideal A ideal is a sub-group of the rings additive group with the following properties:

1. if $a, b \in I$ then $a + b \in I$
2. if $x \in I$ and $r \in R$ then $x \times r \in I$

Every kernel of a ring homomorphism is a ideal.

Remark: Ideals aren't necessarily sub-rings

Quotient Ring Given an ideal I the quotient ring

$$R/I = \{r + I \mid r \in R\}$$

it's the same idea as the cosets in groups. R/I forms a ring. Pronounces R mod I.

This again is where we get $\mathbb{Z}/n\mathbb{Z}$. It also lets us write the set of gaussian integers as $\mathbb{Z}[i]/\mathbb{Z}[i^2 + 1]$.

§3. 3. Generating Ideals

If an ideal contains a unit, it must contain 1 and then it must be R. So we say a **proper ideal** is a ideal **without any units**.

I actually know what a module is, so I can just say that: An ideal is an R-module. The ideal $(x_1, \ldots, x_n)$ is the submodule spanned by $x_1, \ldots, x_n$.

You can think of (x) as all the multiples of (x). In an ideal we can also just straight up write (this is super powerful).

$$x \equiv y \pmod{I}$$

to mean that $x - y \in I$. Everything we know about modular arithmetic carries over!

§3. 4. Principal Ideal and Principal Ideal Rings

Principal Ideal A principal ideal is an ideal generated by a single element.

A principal ideal ring is a ring where every ideal is a principal idea. This means we can write $(x, y) = (g)$ and where the shorthand notation for gcd comes from.

§3. 5. Fields

A field is a ring where every non-zero element is a unit. Meaning that every element has an inverse. This also means that there are no ideals besides the two trivial ones.

§3. 6. Integral Domains

An integral domain is a ring with no **zero** divisors.

zero divisors a is a zero divisor of the ring R if $ab = 0$ where a and b are both non-zero.

In an integral domain we have that $ac = bc$ implies that $(a - b)c = 0$ and thus either $a = b$ or $c = 0$

PID an integral domain where all ideals are principal is called a **principal ideal domain**

§3. 7. Prime Ideals

In a prime ideal if $xy \in I$ then either $x \in I$ or $y \in I$

☂ **Theorem 3.7.1**: An ideal I is prime if and only if R/I is an integral domain.

This is by definition, think about $xy \equiv 0 \bmod p$.

§3. 8. Maximal Ideals

A proper ideal I is maximal if it is not contained in any other proper ideal.

☂ **Theorem 3.8.1**: An ideal I is maximal if and only if R/I is a field.

Notice maximal ideals are prime, this is because R/I is a field and hence is an integral domain. (I still like saying there are no zero-divisors).

§3. 9. Field of Fractions

Given an integral domain R, we define the **field of fractions** or **fraction field** $\mathrm{Frac}(R)$ as follows: It consists of elements a/b with the usual rules of addition and multiplication.

Notice that we need it to be an integral domain because otherwise we might end up with 0 in the denominator.

This is why we call it a integral domain. Because we can do fractions which are pretty important.

§3. 10. Unique Factorization Domains

A non zero non-unit of an integral domain R is said to be **irreducible** if it cannot be written as the product of two non-units.

An integral domain R is a **unique factorization domain** if every non-zero non-unit of R can be written as the product of irreducible elements, which is unique up to multiplication by units.

☂ **Theorem 3.10.1**: Let R be a PID, then R is a UFD

What this means is that if every ideal of R is principal (we can take the gcd) and it is an integral domain meaning there are no zero-divisors. Then it is also a unique factorization domain. 😞😞😞😞.

§4. Vector Spaces

An R-module over a commutative rings is any structure where we can add any two numbers together and scale them by an element of R.

A **vector space** is a module where the ring is actually a field.

§4. 1. Direct Sums

If A and B are subsets of M which are themselves R-modules. Then M is the direct sum of A and B if every element can be written uniquely as the sum of elements from A and B. This means then that A and B shouldn't have any overlap.

If M and N are R modules we define $M \oplus N$ to be the set of elements (m, n) with and scaling being term wise.

§4. 2. Linearity Independence, Span and Basis

Linear Combination A sum of the form $r_1 v_1 + r_2 v_2 + \ldots + r_n v_n$

Linear Independence A set of elements is linearly independent if no non-trivial linear combination is equal to 0

Generating Set / Spanning A subset of a module is called a generating if it generates every element of a module, and is called spanning in the context of a vector space.

Basis a set is a basis if it is both a generating set and every element can be written as a linear combination uniquely, meaning that it that the set is also linearly-independent.

☂ **Theorem 4.2.1** (Maximality and minimality of basis): Let V be a vector space over some field k and take $e_1, \ldots, e_n \in V$. The following are equivalent.
1. e_i for a basis
2. e_i is spanning but not proper subset is spanning
3. e_i is independent but no superset is independent

Remark: for modules (1) implies (2) and (3) but we can't go backwards

☂ **Theorem 4.2.2** (Dimension Theorem): Every basis of a vector space V has the same number of elements.

The proof is to show that spanning sets are never smaller than independent sets.

The theorem is generally true even if the basis is not finite by considering the cardinality of the basis.

Dimension The dimension of a vector space is the size of any finite basis which is unique by ☂ Theorem 4.2.2.

If $\dim(V) = n$ then we can write $V = e_1 k \oplus e_2 k + \ldots + \oplus e_n k$.

Rank We say that the rank of a linear map is the dimension of it's image. This is the same as the number of linearly independent columns.

§4. 3. Linear Maps

Linear Map A linear map $V \to W$ which is linear meaning that $f(a + b) = f(a) + f(b)$.

A linear map is unique defined by what it does to the basis vectors.

§4. 4. Subspaces and picking convenient Bases

Let M be a left R module. A sub-module N of M is a module N such that every element is also an element of M. If M is a vector space than N is a subspace.

Null Space / Kernel The kernel of a map $T : V \to W$ is the preimage of 0. It's a subspace of V.

Nullity Dimension of the Null Space.

Spans Let V be a vector space and $v_1, v_2, \ldots, v_m$ be any vector of V. The span of these vectors is the set

$$\{a_1 v_1 + a_2 v_2 + \ldots + a_m v_m\}$$

Column Space the image of a linear transformation

☂ **Theorem 4.4.1** (Rank Nullity Theorem):

$$\dim V = \dim \ker T + \dim \operatorname{im} T$$

$$\dim V = \operatorname{rank} + \operatorname{nullity}$$

§4. 5. Eigen-things

Eigenvector Let $T : V \to V$ and $v \in V$ be a non-zero vector. We say that v is an eigenvector if $T(v) = \lambda v$ for some λ.

Eigenvector The value of λ above is called an eigenvalue of T. And that v is a λ-eigenvector.

Notice that the set of λ-eigenvectors forms a subspace with the addition of 0.

We have actually that

$$\det(M - \lambda) = 0$$

§4. 6. Dual space and trace

Tensor product The tensor product $V \otimes V$of V and W is the set of elements $v \otimes w$. Now the tensor product of two vectors is bi-linear. This means that:

1. $(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$
2. $v \otimes (w_1 + w_2) = v \otimes (w_1) + v \otimes (w_2)$
3. $(c \cdot v) \otimes w = v \otimes (c \cdot w)$

If $e_1, e_2, ..., e_n$ is a basis of V and $f_1, f_2, ..., f_n$ is a basis of W then $e_j \otimes f_j$ forms a basis for $V \otimes W$.

Dual Space the dual space $V^\vee$ of V (a k-space) is the space of linear maps from V to k. Addition and multiplication is done pointwise.

The basis for the dual space of $e_i^\vee$ is defined by $e_i^\vee$ mapping e^i to 1 and everything else to 0.

$V^\vee \oplus W$ represents the set of linear maps $V \to W$. There is a natural bijection between the two.

So we have that $V^\vee \otimes V \cong V \to V$. Consider also the evaluation map $\mathrm{ev} : V^\vee \times V$ which collapses each pure tensor $f \otimes v \mapsto f(v)$. This is a linear map as well.

We can now perform the following map:

$$(V \to V) \longrightarrow V^\vee \otimes V \longrightarrow k$$

This is why changes in basis keeps the trace the same.

§4. 7. Determinant

Wedge Product The wedge product looks like the tensor product but with: $v \wedge v = 0$ and hence $v \wedge w = -w \wedge v$.

The determinant arises when we take a bunch of wedge products.

§4. 8. Inner Product Spaces

Inner Form For real numbers the inner product is defined as a bilinear form written as $\langle \bullet, \bullet \rangle$ which is: symmetric and positive definite. i.e. $\langle a, b \rangle = \langle b, a \rangle$ and $\langle a, b \rangle \geq 0$.

Inner Form For complex numbers: instead we have conjugate symmetry meaning that $\langle a, b \rangle = \overline{\langle b, a \rangle}$ and sesquilineariarity meaning linear in the first argument and anti-linear in the second argument. The form is still positive definite.

An inner product space is either a real vector space equipped with a real inner form, or a complex vector space equipped with a complex inner form.

Norm The norm $\|v\|$ is defined as $\sqrt{\langle v, v \rangle}$ this is why we needed it to be positive definite.

🟪 **Lemma 4.8.1** (Cauchy Schwartz):

$$\langle v, w \rangle \leq \|v\| \; \|w\|$$

with equality only when w and v are dependent.

☂ **Theorem 4.8.2** (Triangle Inequality):

$$\|v\| + \|w\| \geq \|v + w\|$$

§4. 9. Orthogonality

Orthogonal Two non-zero vectors are orthogonal in an inner product space if if their inner product is 0.

An orthonormal basis is a set of basis vectors which are all orthogonal to one another and which are all normal, meaning that their norm is 1.

The applications of this are very very lovely, see Fourier Transform notes.

§4. 10. Duals, Adjoint, and Transpose

Dual of a Map Let V and W be vector spaces. Suppose $T : V \to W$ is a linear map. Then we actually get a map $T^\vee : W^\vee \to V^\vee$.

$$f \mapsto f \circ T$$

This is called the dual map.

It converts a map taking in W to a map taking in V by first mapping V to W. Shockingly this is the transpose of a matrix?

This comes about by analysis on the basis vectors and where they get mapped to.

☂ **Theorem 4.10.1**: Let V be a finite-dimensional *real* inner product space and $V^\vee$ its dual. Then the map $V \to V^\vee$ by

$$v \mapsto \langle \bullet, v \rangle \in V^\vee$$

is an isomorphism of real vector spaces.

Adjoint / Conjugate Transpose Let V and W be finite dimensional inner product spaces, and let $T : V \to W$. The adjoint of T, denoted $T^\dagger : W \to V$, is defined as follows: for every vector $w \in W$, we let $T^\dagger \in V$ be the unique vector with

$$\langle v, T^\dagger(w)\rangle = \langle T(v), w\rangle$$

We have that $T^\dagger$ is well defined because $\langle \bullet, w\rangle$ is some element $f \in W^\vee$ So $\langle T(\bullet), w\rangle = f(T(\bullet)) = T^\vee(f) \in A^\vee$. So this that not only would $T^\dagger$ exist but there is only one possible $T^\dagger$.

Now we want to see if $T^\dagger$ is a linear map. We can see pretty clearly that scaling w does exactly what we want it to do, this is very good.

We also have that

$$\begin{aligned}\langle v, T^\dagger(a+b)\rangle &= \langle T(v), a+b\rangle \\ &= \langle T(v), a\rangle + \langle T(v), b\rangle \\ &= \langle v, T^\dagger(a)\rangle + \langle v, T^\dagger(b)\rangle \\ &= \langle v, T^\dagger(a) + T^\dagger(b)\rangle\end{aligned}$$

and since there is only one value of $T_\dagger(a+b)$ is must be linear.

☂ **Theorem 4.10.2** (Adjoints are conjugate transposes): Fix a *orthonormal* basis of a finite-dimensional inner product space V. Let $T : V \to V$ be a linear map. If we write T as a matrix in this basis then matrix $T^\dagger$ in the same basis is the conjugate transpose of the matrix T; that is we transpose the matrix and take the complex conjugate.

§4. 11. Normal Maps

Normal we say that a linear map T is normal if $TT^\dagger = T^\dagger T$.

We say that T is **Hermitian** if $T = T^\dagger$. This is also called symmetric.

☂ **Theorem 4.11.1**: $T : V \to V$ is normal if and only if one can pick an orthonormal basis of eigenvectors

☂ **Theorem 4.11.2**: A hermitian matrix is normal and has all real eigenvalues.