CHAPTER 3

Innocent (Commutative) Algebra

> "The introduction of the cipher 0 or the group concept was general nonsense too, and mathematics was more or less stagnating for thousands of years because nobody was around to take such childish steps..."
> - Alexander Grothendieck (in his 1982 letter to Ronald Brown)

> "Taking a new step, uttering a new word, is what people fear most."
> - Fyodor Dostoevsky, Crime and Punishment

3.1. It will not be possible for us to discuss the complete (basic) algebra. We will assume some knowledge and this chapter should be treated to recall some of the basic facts. If one is not comfortable with algebra of rings, fields, vector spaces (and modules), then one may refer to [1, 2]. Even though the chapter is set for algebra, we take some irregular detours to other parts of mathematics.

1. Some Preliminaries

Definition 3.2 (Subset). For two sets S and T we say that S is a *subset* of T if each element of S is also an element of T, i.e. if S $\subseteq$ T $\forall$ $x \in S$ we have $x \in T$.
Simultaneously, we can also say that T contains S which can be written as $T \supseteq S$. If $S \subseteq T$ and $S \neq T$ hold, then we write $S \subset T$ and we say that S is a *proper subset* of T.

Remark 3.3. Two sets are equal iff each is a subset of the other. In symbolic notation: $(A = B) \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$

Definition 3.4 (Cartesian Product). Consider a given family of sets $(S_i)_{i \in I)}$, where I denotes the index set, then the cartesian product denoted as $\prod_i S_i$, of the family of given sets is the set of all functions f from the index set I with f_j in each S_j, for each $j \in I$.

This chapter includes contributions by Purnima Tiwari
This is a part of Prelude of Schemes project available at https://aayushayh.github.io/PtoS.html.
Last Updated: 11 Feb, 2026

For a finite family of sets, we can define the Cartesian Product as:

$$\prod_{i=1}^{i=n} S_i = \{(s_1, s_2, s_3, \cdots, s_n) \ \mid \ s_i \in S_i, \ \forall i \in \{1, 2, 3, \cdots, n\}\}$$

Definition 3.5 (Relation). A relation is a subset of the cartesian product of two sets that helps to establish a connection between the elements of the sets. Given a set X, a relation R over X is a set of ordered pairs of elements from X:

$$\mathbb{R} \subseteq \{(x, y) \mid x, y \in X\} \tag{1}$$

Definition 3.6 (Injection, Surjection and Bijection). A function $f : S \hookrightarrow T$ is *injective* or one-to-one if no element of T (no second coordinate) appears in more than one ordered pair. Such a function is called an **injection**. A function $f : S \twoheadrightarrow T$ is *surjective* or onto if every element of T appears in an ordered pair. Such a function is called a **surjection**.

A function that is both surjective and injective is said to be *bijective*. Bijective functions are called **bijections**.

3.7. One should be careful that all of these definitions are apt for set theoretic foundations only. We would revise most of these definitions in future sections, especially in category theory.

Definition 3.8 (Equivalence Relation). A binary relation[1] $\sim$ on a set is said to be an equivalence relation, iff it is *reflexive, symmetric* and *transitive*. An equivalence class of an element a is defined as:

$$[a] = \{x \in X : \ a \sim x\}. \tag{2}$$

The set of all *equivalence classes* in X with respect to an equivalence relation R is denoted as X/R and is called X modulo R.

3.9. Let us write the axioms[2] for reflexive, irreflexive, symmetric, anti-symmetric, asymmetry and transitive relations.

Reflexive: $\forall a, \ a \sim a$
Symmetric: $\forall a, b, \ a \sim b \implies b \sim a$
Transitive: $\forall a, b, c, \ a \sim b$ and $b \sim c \implies a \sim c$
Asymmetry: $\forall a, b, \ a \sim b \implies \neg \ b \sim a$
Anti-symmetry: $\forall a, b, \ a \sim b, \ b \sim a \implies a = b$
Irreflexive: $\forall a, \ \neg a \sim a$ (for example $(\mathbb{R}, <)$)

[1] In formal logic, a *predicate* or relation is an n-ary symbol and so is an operation. Binary operation is just an example of n-ary operations.

[2] Given any relation, there are some properties that we list down which are called axioms. For instance, axioms of $(\mathbb{R}, \leq)$ consists of reflexivity, anti-symmetry, and transitivity.

Remark 3.10. The symbol '¬' denotes the negation statement.

Definition 3.11 (Congruence Relation). If a and b have the same remainder when they are divided by a non-zero integer m, then we say that *a is congruent to b mod m*, represented as:

$$a \equiv b(mod\ m) \tag{3}$$

Congruence modulo m is an equivalence relation which is compatible with the operations of addition, subtraction, and multiplication.

Definition 3.12 (Residue Class). The residue class of a mod m is denoted as $[a]$, where $[a]$ represents the set of all integers that are congruent to a modulo m.

Definition 3.13 (Partial Order and Total Order). The reflexive, antisymmetric and transitive relation $\mathcal{R}$ is called a partial order relation and $\mathcal{R}$ is said to define a partial ordering of $\mathcal{S}$. The addition of the trichotomy law to the set of axioms of the partial order, defines the total order.

Hence, for a set $\mathcal{S}$ to be totally(/partially) ordered, it must have a relation $\mathcal{R}$ on it with the total(/partial) order.

Example 3.14. $(\mathbb{R}, <)$ is an example of strict linear order which is total ordered and $(\mathbb{R}, \leq)$ is an example of linear order which is partially ordered.

Lemma 3.15 (Kuratowski-Zorn Lemma a.k.a. Zorn's Lemma). If every totally ordered subset of a poset $\mathcal{S}$ has an upper bound, then $\mathcal{S}$ contains a maximal element.

2. Algebraic Structures

Definition 3.16 (Algebraic Structure). An algebraic structure is defined as a non-empty set that forms the closure with at least one operation, denoted as $(S, \star)$, where S denotes the non-empty set and $\star$ defines the operation.

In accordance with the above definition, any non-empty set with an operation will form an algebraic structure and with the duality principle, will also possess a geometrical interpretation.

Definition 3.17 (Semigroup and Monoid). A *semigroup* is an algebraic structure equipped with a binary operation and satisfying associativity.

A *monoid* is a semigroup fulfilling the existence of a unique identity. For example, $(\mathbb{R}, +, 0)$.

3.18. A group can be seen as a set of *symmetries* of any objects. And symmetries, on the other hand, will be defined as mapping an entity to itself, while preserving the structure.

Definition 3.19 (Group). A group is a set G with a binary operation $G \times G \to G$, usually written as

$$(a, b) \Rightarrow a + b, a \times b, ab, \text{ or } a \cdot b, \tag{4}$$

and must follow the following *axioms*:

(1) $\exists$ a unique identity $(e, 1, \text{ or } 0)$ such that $ea = a = ae$
(2) $\exists$ a 2-sided inverse, for every element a^{-1} such that $a^{-1}a = aa^{-1} = e$
(3) $\exists$ associativity amongst the elements such that $(ab)c = a(bc)$

3.20. Alternatively, we can also see a group as a monoid, consisting of a 2-sided inverse of all the elements in the underlying set.

Definition 3.21 (Commutative Group). Let $(G, \star)$ be a group, then G is said to be a commutative group if $a \star b = b \star a, \ \forall \ a, b \in G$.

3.22. We say that a group structure $(G, \star)$ is **Abelian** if it is commutative. That is, in an Abelian Group, the order of applying the group operation on the elements becomes irrelevant. Hence, the elements have become invariant under the order of application of the group operation.

Example 3.23 (finite Abelian group). A group G defined as $(G = \{e, a, b, c\}, \star)$ [3] , where $\star : G \times G \longrightarrow G$, such that each element is self inverse and when two different elements other than identity are multiplied, then the 3rd element, other than the identity is the result.

Definition 3.24 (Order of an Element). For a group G and $x \in G$, the order of x is defined as the smallest positive integer n such that $x^n = e$, where e is the identity of G. It is denoted as $o(x)$.

If no positive power of x is the identity, the order of x is defined to be infinity and x is said to be of infinite order.

3.25. An element of a group has order 1 iff it is the identity.

Definition 3.26 (Order of a Group). For a discrete group G, the **order** of the group is the cardinality of the underlying set. Hence, for a finite group G, its order $|G|$ is a natural number.

Theorem 3.27 (Fundamental theorem of order). Let G be a group and $g \in G$ be an element then,

(1) If $|g| = \infty$, then $g^n = g^m$ iff $n = m$.
(2) If $|g| = k$ is finite, then $g^n = g^m$ iff $k|(n - m)$.

[3] Klein four-group

Definition 3.28 (Group Generator). A group generator is a subset of a group, such that every element of the group can be expressed as a finite combination of elements and their inverses. This can be expressed notationally as:

$$G = \langle S \rangle \tag{5}$$

and we say that *G is generated by S* or *S generates G*.

Definition 3.29 (Relations). Any equations in a general group G that the generators satisfy are called relations in G.

Definition 3.30 (Subgroup). Consider a group G, and a subset H of G. H is a subgroup of G, iff H also froms a group under the same operations as in G.

Definition 3.31 (Normalizer). Given a subset S of the underlying set of a group G, its normalizer consists of all the elements from G such that the left and the right action by those elements on S, results in the same subsets.

$$N(S) = N_G(S) = \{n \in G : Sn = nS\}$$

A normalizer forms a subgroup of G.

Definition 3.32 (Centralizer). Consider a group G, and a subset S of G, i.e., a subset of it's underlying set, then the centralizer subgroup of S in G is the subgroup of all the elements c in G which commute with all the elements of S.

$$C_G(S) = \{c \in G : cs = sc\}$$

Theorem 3.33. Given a subset $S \subset G$ of a group G, then the centralizer subgroup of S is a subgroup of the normalizer subgroup such that,

$$C_G(S) \subset N_G(S)$$

Definition 3.34 (Stabilizer). Consider a group G an let us define an action by the group G on a set X for every element $x \in X$ such that,

$$G \times X \to X$$

Now, a stabilizer subgroup, also known as the **isotropy subgroup** of x is defined as the set of all the elements in G that leave x fixed. In other words, the action *stabilizes* every element of X, in other words.

Hence, a stabilizer subgroup of X consists of a set of elements under which all the elements of X are conjugation invariant. It is represented as:

$$Stab_G(x) = \{g \in G : g \cdot x = x\}$$

Now, if all the stabilizer groups are trivial, then the action is called a **free action**.

THEOREM 3.35. Let $a \in G$, and $(G, \cdot)$ be a finite group, then the set generated by the power of a defined as: $S = \{a^n : n \in \mathbb{Z}, a \in G\}$ is finite.

PROOF. Let $a \in G$. Then, $\cdots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, \cdots \in G$ where, $n \in \mathbb{Z}$. By closure property, the above holds. Now, $(G, \cdot)$ is a finite group, hence all the elements are not distinct. Let, $r < s : a^r = a^s$, then left action by a^{-r} gives us:

$$a^{-r} \cdot a^r = a^{-r} \cdot a^s \tag{6}$$

$$e = a^{-r} \cdot a^s = a^{s-r} \tag{7}$$

$$\therefore \ o(a) \leq (s - r) \tag{8}$$

The integral powers of a will result into non-distinct values. Hence, S is a finite set. □

THEOREM 3.36 (Cauchy's Theorem). Let G be a finite group with order $|G| \in \mathbb{N}$. If a prime number p divides $|G|$, then equivalently,

(1) G has an element of order p.
(2) G has a subgroup of order p.

Bibliography

[1] Bourbaki, *Algèbre*. Springer, 2007.

[2] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*. CRC Press, 2018.

[3] R. Bott and L. W. Tu, *Differential forms in algebraic topology*, vol. 82. Springer Science & Business Media, 2013.

[4] D. A. Buchsbaum, "Exact categories and duality," *Transactions of the American Mathematical Society* **80** no. 1, (1955) 1–34.

[5] A. Grothendieck, "Sur quelques points d'algèbre homologique," *Tohoku Mathematical Journal, Second Series* **9** no. 2, (1957) 119–183. English translation available at https://www.math.mcgill.ca/barr/papers/gk.pdf.

[6] F. Peter, "Abelian Categories: An Introduction to the Theory of Functors,".

[7] J.-L. Verdier, "Catégories dérivées Quelques résultats (état 0)," in *Cohomologie Etale: Séminaire de Géométrie Algébrique du Bois-Marie SGA 4 1/2*, pp. 262–311. Springer, 1977.

[8] C. A. Weibel, *An introduction to homological algebra*. No. 38. Cambridge university press, 1994.

[9] D. Happel, *Triangulated categories in the representation theory of finite dimensional algebras*, vol. 119. Cambridge University Press, 1988.

[10] S. MacLane, "Henri Cartan and Samuel Eilenberg, Homological Algebra,".

[11] T. Stacks project authors, "The Stacks project." https://stacks.math.columbia.edu, 2025.

[12] C. A. Weibel, *The K-book: An Introduction to Algebraic K-theory*, vol. 145. American Mathematical Soc., 2013.

[13] M. Atiyah, *K-theory*. CRC press, 2018.

[14] H. Miller, "Leray in Oflag XVIIA: The origins of sheaf theory, sheaf cohomology, and spectral sequences,".

[15] J.-P. Serre, "Faisceaux algébriques cohérents," *Annals of Mathematics* **61** no. 2, (1955) 197–278.

[16] A. Grothendieck, "Éléments de géométrie algébrique: I. Le langage des schémas," *Publications Mathématiques de l'IHÉS* **4** (1960) 5–228.

[17] A. Verma, "Local aspects of topological quantization and the Wu-Yang Monopoles," *arXiv:2406.18799* (2024) .

[18] T. Y. Chow, "You could have invented spectral sequences," *Notices of the AMS* **53** (2006) 15–19.

[19] A. HATCHER, "Algebraic Topology," *http://www. math. cornell. edu/˜ hatcher/AT/ATpage. html* (2002) .

[20] J. McCleary, *A user's guide to spectral sequences*. No. 58. Cambridge University Press, 2001.

[21] M. Dubois-Violette, "The Weil-BRS algebra of a Lie algebra and the anomalous terms in gauge theory," *Journal of Geometry and Physics* **3** no. 4, (1986) 525–565.

[22] R. Vakil, "The rising sea: Foundations of algebraic geometry,". available at https://math.stanford.edu/~vakil/216blog/FOAGjul2724public.pdf.

[23] W. Browder, "Torsion in H-spaces," *Annals of Mathematics* **74** no. 1, (1961) 24–51.

[24] D. Mumford, *The red book of varieties and schemes: includes the Michigan lectures (1974) on curves and their Jacobians*, vol. 1358. Springer, 2004.

[25] R. Hartshorne, *Algebraic geometry*, vol. 52. Springer Science & Business Media, 2013.