Abstract algebra

Groups

Dr. Yee Wei Law ⟨yeewei.law@unisa.edu.au⟩

2023-08-21

The mathematical area of abstract algebra, especially the theory of Galois fields, plays an important role in cryptography.

Contents

1 Introduction

Traditionally, mathematics has been separated into three main areas, namely *algebra*, *geometry* and *analysis* [COFMR19, Preface].

Abstract algebra or modern algebra is the theory of *algebraic structures* [COFMR19, Sec. 1.1].

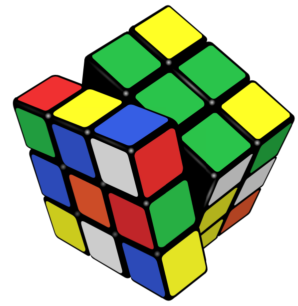
- An algebraic structure is a *set* together with one or more binary *operations* on it satisfying axioms governing the operations.
- The theory of these structures arose from the study of numbers (e.g., integers, rationals, reals) and equations (e.g., polynomial equations).
- There are many algebraic structures, but the most relevant to us (engineers) are *groups*, *rings*, *fields*, *vector space* and *Hilbert space*.
- A *finite field* or *Galois field* is a *field* with a finite number of elements.
- The theory of *finite fields* is a branch of abstract algebra that has come to the fore because of its diverse applications in combinatorics, coding theory, cryptology, and many others [KL21, Preface].

We start our journey in finite fields with *groups*, the most general type of "useful" structure.

- Rings, fields and other "useful" structures are specific types of groups.

2 Groups

A ▶ popular introduction to group theory borrows the appeal of the Rubik's cube, but instead of going on a Rubik's cube adventure, let us start with the textbook definition:



Definition 1: Group [Lov22, Definition 1.2.1]

A pair $(G, \star)$, consisting of set G and binary operation $\star$ on G, that satisfies the three axioms:

Axiom 1 $\star$ is *associative*, i.e., $(a \star b) \star c = a \star (b \star c), \forall a, b, c \in G$.

Axiom 2 There exists an element $e \in G$, called the *identity* of G, such that $a \star e = e \star a = a$, $\forall a \in G$.

Axiom 3 For each $a \in G$, there exists an element $a^{-1} \in G$, called the *inverse* of a, such that $a \star a^{-1} = a^{-1} \star a = e$.
⚠️ a^{-1} ☝️ should be understood as a symbol rather than specifically as a multiplicative inverse.

Notes:

- G is customarily "abused" to denote not only the set but also the group.
- Axiom 2 implies $G \neq \varnothing$. G can have a finite or infinite number of elements.
- The identity is also called the *neutral element* or *unit element* [Coh03, Sec. 2.1].

- A group's *identity is unique*. Proof: Suppose e_1 and e_2 are two different identities, then $e_1 \star e_2 = e_1 = e_2$, contradicting the original supposition.
- Axiom 3 implies $(a \star b)^{-1} = b^{-1} \star a^{-1}$.
- Every element has *exactly one inverse*.
- A group is not necessarily *abelian* or *commutative*. An abelian group satisfies the axiom: $a \star b = b \star a$, $\forall a, b \in G$.

AB=BA is an abelian group.

It is customary to write

- $\star$ as $\cdot$ for *generic* groups, in contexts where $\cdot$ would not be misunderstood as multiplication.
- $\star$ as $+$ for *abelian* groups, in contexts where $+$ would not be misunderstood as addition.

Multiplicative notation

$$a^{-n} = (a^{-1})^n,$$
$$a^n a^m = a^{n+m},$$
$$(a^n)^m = a^{nm}.$$

Additive notation

$$(-n)a = n(-a),$$
$$na + ma = (n+m)a,$$
$$m(na) = (mn)a.$$

Examples of groups (see [Sma16, Sec. A.6], [Gar01, Sec. 17.1]):

Example 1

The pairs $\mathbb{Q}^+ \triangleq (\mathbb{Q}, +)$, $\mathbb{R}^+ \triangleq (\mathbb{R}, +)$ and $\mathbb{C}^+ \triangleq (\mathbb{C}, +)$ are abelian groups.

Example 2

The pairs $\mathbb{Q}^* \triangleq (\mathbb{Q} \setminus \{0\}, \cdot)$, $\mathbb{R}^* \triangleq (\mathbb{R} \setminus \{0\}, \cdot)$ and $\mathbb{C}^* \triangleq (\mathbb{C} \setminus \{0\}, \cdot)$ are abelian groups.

Example 3

The pair $\mathbb{Z}^+ \triangleq (\mathbb{Z}, +)$ is an abelian group.

- The identity is 0.
- The inverse of $a \in \mathbb{Z}$ is $-a \in \mathbb{Z}$.

Example 4

The pair $(\mathbb{Z}, -)$ is *not* a group since $(a - b) - c \neq a - (b - c)$.

The pair $(\mathbb{Z}, \times)$ is *not* a group since only the inverse of 1 exists in $\mathbb{Z}$.

Example 5

When $G = \{0, 1, 2\}$ and $\star$ is addition modulo 3, $(G, \star)$ is an abelian group.

- Associativity and commutativity are straightforward to prove although tedious.
- The identity is 0.
- The inverses are $0, 2, 1$ respectively.

Example 6

When $G = \{1, 2\}$ and $\star$ is multiplication modulo 3, $(G, \star)$ is an abelian group.

- Associativity and commutativity are straightforward to prove although tedious.
- The identity is 1.
- Each element is its own inverse.

The set of integers modulo n has a special place in cryptography.

Definition 2: Congruence [LN94, Definition 1.4]

For $n \in \mathbb{N}$ and arbitrary $a, b \in \mathbb{Z}$, if $a - b$ is a multiple of n, i.e., $a = b + kn$ for some integer k (equivalent, $b = a + ln$ for some integer l), we write

$$a \equiv b \mod n,$$

and say that a is *congruent* to b modulo n.

Congruence modulo n is an *equivalence relation*:

Definition 3: Equivalence relation [LN94, p. 4]

A subset R of $S \times S$ is called an *equivalence relation* on set S if it is

$$\begin{aligned}
&\text{reflexive:} && (s, s) \in R, && \forall s \in S; && (1)\\
&\text{symmetric:} && (s, t) \in R \implies (t, s) \in R, && \forall s, t \in S; && (2)\\
&\text{transitive:} && (s, t), (t, u) \in R \implies (s, u) \in R, && \forall s, t, u \in S. && (3)
\end{aligned}$$

If we collect all the elements of some set S equivalent to some element $s \in S$, then we get the *equivalence class* of s, denoted by [DF99, Gar01]:

$$\bar{s} = \{t \in S | (s, t) \in R\}.$$

⚠ Some texts [LN94] use the notation $[s]$ instead of $\bar{s}$.

If the equivalence relation R is congruence modulo n, then for $a \in \{0, \ldots, n-1\}$, we call the set

$$\bar{a} = \{a + kn | k \in \mathbb{Z}\}$$

the *congruence class* or *residue class* of a.

- Given integer n, $\mathbb{Z}_n^+$ denotes the set $G = \{0, 1, \ldots, n-1\}$ with addition modulo n as the operation.
- $\mathbb{Z}_n^+$ is an additive abelian group [LN94].
- Other notations include $\mathbb{Z}/n^+$ [Gar01] and $(\mathbb{Z}/n\mathbb{Z})^+$ [DF99, Sma16].

- Given integer n, $\mathbb{Z}_n^\times$ denotes the set $G = \{1, \ldots, n-1\}$ with multiplication modulo n as the operation.
- For *prime* n, $\mathbb{Z}_n^\times$ is a multiplicative abelian group.
- Other notations include $\mathbb{Z}/n^\times$ and $(\mathbb{Z}/n\mathbb{Z})^\times$.
- Symbols $\times$ and $*$ are interchangeable.

Example 7

The group $\mathbb{Z}_3^+$ contains three congruence classes, namely $\bar{0}$, $\bar{1}$ and $\bar{2}$. Notice by slight abuse of notation,

$$\bar{a} + 3 = \bar{a}.$$

Since adding 3 to any congruence class cycles back to the congruence class, $\mathbb{Z}_3^+$ is an example of a *cyclic group*.

Definition 4: Cyclic group and generator [LN94, Definition 1.3]

A group G is *cyclic* if there is an element $a \in G$ such that for any $b \in G$, there is some integer j with

- $b = a^j$ if G is multiplicative; or
- $b = ja$ if G is additive.

The element a is a *generator* of G.

Define

$$\langle a \rangle = \begin{cases} \{a^0, a^1, \ldots\} & \text{for multiplicative } G, \\ \{0a, 1a, \ldots\} & \text{for additive } G, \end{cases}$$

then $\langle a \rangle = G$.

Not every element in a cyclic group is necessarily a generator.

Example 8

Any group $\mathbb{Z}_n^+$ is a cyclic group and the congruence class $\bar{1}$ is a generator. This group has n elements and we say the *order* of this group is n.

Definition 5: Order [LN94, Definitions 1.5 and 1.9]

Suppose group G is finite, then the *order* of G, denoted by $|G|$, is the number of elements in G.

The *order* of $g \in G$ (where g not necessarily a generator), denoted by $|g|$, is the smallest integer i with

$$\begin{cases} g^i = 1 & \text{for multiplicative } G, \\ ig = 0 & \text{for additive } G. \end{cases}$$

The above double definition of “order” is motivated by these facts:

- $|g| = n \iff |\langle g \rangle| = n$, where $\langle g \rangle$ is not necessarily G; see [Sma16, Lemma 100.31], [FM19, Lemma 8.26], [Dav21, Corollary 4.27].
- If a is an element of finite group G, then

$$\begin{cases} a^{|G|} = 1 & \text{for multiplicative } G, \\ |G|a = 0 & \text{for additive } G \text{ [Dav21, Corollary 8.16].} \end{cases}$$

  Lagrange’s theorem (see Theorem 3) facilitates a straightforward proof for the above, so our ensuing discussion will lead to the immensely useful theorem.

Example 9

An element of $\mathbb{Z}_n^*$ that has an inverse is called a *unit* (⚠ not to be confused with “unit element”).

An element of $\mathbb{Z}_n^*$ is a unit iff $\gcd(a, n) = 1$ [Dav21, Lemma 4.4].

Proof: For necessity, observe that $aa^{-1} \equiv 1 \mod n$ if a^{-1} is the inverse of a. Therefore, $aa^{-1} - 1 = kn$ for some integer factor k, or equivalently, $aa^{-1} - kn = 1$, which by Bezout’s lemma, implies $\gcd(a, n) = 1$.
For sufficiency, $\gcd(a, n) = 1 \implies as + nt = 1$ for some integer coefficients s and t. The coefficient s satisfies the definition of an inverse for a.

Denote 1️⃣ by U_n the set of units of $\mathbb{Z}_n^*$ and 2️⃣ by $\phi(n)$ — called *Euler’s totient function* — the number of positive integers not exceeding n which are relatively prime to n.

Then, $|U_n| = \phi(n)$ [Dav21, Corollary 4.7].

The order of a group says nothing about the number of generators in the group.

Example 10

The following table is a so-called *Cayley table* for $\mathbb{Z}_6^+$:

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

The group order is 6 and the number of generators is 1.

Notice $\{[0], [2], [4]\}$ is cyclic in terms of congruence modulo 6. More precisely, it is a cyclic *subgroup* of $\mathbb{Z}_6^+$.

Definition 6: Subgroup [LN94, Definition 1.8], [DF99, Sec. 2.1]

A subset H of the group G is a *subgroup* of G if H is itself a group with respect to the operation of G.

Subgroups of G other than the *trivial* subgroups, namely $\{e\}$ and G, are called *nontrivial* subgroups of G. Subgroups of G that are not G itself are *proper* subgroups.

We write

$$\begin{cases} H \leq G & \text{when } H \text{ is a subgroup of } G, \\ H < G & \text{when } H \text{ is a proper subgroup of } G. \end{cases}$$

Theorem 1: [LN94, Theorem 1.15(i)]

Every subgroup of a cylic group is cyclic.

Proof. Given multiplicative cyclic group $G = \langle a \rangle$, let H be a nontrivial subgroup of G. Suppose $a^b \in H$, then $a^{-b} \in H$. This means H contains at least one positive power of a. Let d be the least positive exponent such that $a^d \in H$ (and of course $a^{-d} \in H$). Suppose $c = dq + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < d$, then $a^c \times (a^{-d})^q = a^r$. Since $r < d$ but we assumed d is the least positive exponent, $a^r \notin H \implies a^c \notin H$. Therefore we must have $H = \langle a^d \rangle$, a cyclic subgroup. □

Example 11

Let the operation be multiplication modulo 8, then $G = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ is a cyclic group [FM19, Example 8.23].

- $\langle \bar{1} \rangle = \{\bar{1}\}$ is a trivial cyclic subgroup of G.
- $\langle \bar{3} \rangle = \{\bar{1}, \bar{3}\}$ is a cyclic subgroup of G.
- $\langle \bar{5} \rangle = \{\bar{1}, \bar{5}\}$ is a cyclic subgroup of G.
- $\langle \bar{7} \rangle = \{\bar{1}, \bar{7}\}$ is a cyclic subgroup of G.

Note none of the elements is a generator.

Theorem 2: [LN94, Theorem 1.15(ii)]

In a finite multiplicative cyclic group $\langle g\rangle$ of order n, the element g^m, where $m \in \mathbb{N}$, generates a subgroup of order $n/\gcd(m,n)$.

Proof. By definition of order, n is the least positive integer such that $g^n = 1$, where 1 is the identity element of $\langle g\rangle$. It is straightforward to show that $\langle g^m\rangle \leq \langle g\rangle$. Suppose $|g^m| = k$, then k is the least positive integer such that $g^{mk} = 1$. Furthermore, mk must be the least common multiple of m and n, i.e.,

$$mk = \operatorname{lcm}(m,n) \implies k = \frac{mn}{m\gcd(m,n)} = \frac{n}{\gcd(m,n)}.$$

□

Example 12

Let the operation be multiplication modulo 10, then $G = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$ is a cyclic group [FM19, Example 8.24].

- $\langle\bar{1}\rangle = \{\bar{1}\}$ is a trivial cyclic subgroup of G.
- $\langle\bar{3}\rangle = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$ is a trivial cyclic subgroup of G.
- $\langle\bar{7}\rangle = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$ is a trivial cyclic subgroup of G.
- $\langle\bar{9}\rangle = \{\bar{1}, \bar{9}\}$ is a cyclic subgroup of G.

$\bar{3}$ and $\bar{7}$ are generators of G. As shown above, $\bar{3}^2 = \bar{9}$ does indeed have order $4/\gcd(2,4) = 2$.

Theorem 2 tells us something useful about the orders of *cyclic* subgroups. The next theorem we are going to learn about will tell us something useful about the orders of *finite* subgroups in general — cyclic or not cyclic — but first we need to know what *cosets* are.

Definition 7: Coset [LN94, pp. 6-7], [DF99, p. 78], [Gar01, Secs. 17.3-17.4], [Sma16, Definition 100.37], [Dav21, Sec. 8.1]

Let $(G,\star)$ be a group and $H \leq G$. For any $g \in G$, the *left coset* of H in G (containing g) is defined as

$$g \star H = \{g \star h | h \in H\}.$$

Similarly, the *right coset* of H in G (containing g) is defined as

$$H \star g = \{h \star g | h \in H\}.$$

These alternative terms are equivalent:

- left/right coset of H with respect to g
- left/right translate of H by g
- left/right coset of G modulo H

Any element of a coset is called a *representative* of the coset.

In simpler terms, a coset is the result of taking a subgroup and "shifting" it either on the left or on the right.

- Two different "shifts" can result in the same coset.
- Left and right cosets coincide when the group operation is commutative.
- If H is a finite subgroup of G, then every coset of H in G has the same number of elements as H [LN94, Theorem 1.12].

Figure 1: Things that are not cosets.

- Given $g_1 \neq g_2$, both elements of G, if H is a subgroup of G, then

$$\begin{cases} g_1 \star H = g_2 \star H & \iff \operatorname{inv}(g_1) \star g_2 \in H, \\ g_1 \star H \cap g_2 \star H = \varnothing & \text{otherwise [Dav21, Theorem 8.5].} \end{cases}$$

  The same observation applies to right cosets. These imply cosets form a *partition* of G.
- ⚠ Cosets (coupled with the original group operation) are not necessarily groups. $g \star H$ is a subgroup of $G \iff g \in H$ [Dav21, Theorem 8.5].

Definition 8: Index [LN94, Definition 1.13], [DF99, Sec. 3.2], [Gar01, Sec. 17.4], [Dav21, Sec. 8.4]

If the subgroup H of G only yields finitely many distinct left/right cosets of H in G, then the number of such cosets is called the *index* of H in G, and denoted by $|G : H|$ or $[G : H]$.

Whether index is defined for left or right cosets does not matter because there are as many distinct left cosets as right ones [Dav21, Theorem 8.8].

Example 13

This example is from [LN94, p. 6]. If $G = \mathbb{Z}_{12}^{+}$, then $H = (\{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}, +) \leq G$. The left cosets of H in G are

$$\begin{aligned} \bar{0} + H = \bar{3} + H = \bar{6} + H = \bar{9} + H &= \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}, \\ \bar{1} + H = \bar{4} + H = \bar{7} + H = \overline{10} + H &= \{\bar{1}, \bar{4}, \bar{7}, \overline{10}\}, \\ \bar{2} + H = \bar{5} + H = \bar{8} + H = \overline{11} + H &= \{\bar{2}, \bar{5}, \bar{8}, \overline{11}\}. \end{aligned}$$

The right cosets of H in G are exactly the same as the left cosets.

There are three distinct left/right cosets of H in G, so $|G : H| = 3$. Notice $|G : H| = 3$ multiplied by $|H| = 4$ is exactly $|G| = 12$.

The preceding example paves way for the subsequent very important theorem:

Theorem 3: Lagrange's theorem [LN94, Theorem 1.14], [DF99, Theorem 8], [Sma16, Theorem 100.38]), [FM19, Theorem 8.27], [COFMR19, Theorem 9.4.4], [Dav21, Sec. 8.3]

If H is a subgroup of finite group G, then

$$|G| = |G : H||H|,$$

which implies the order of H divides the order of G.

The utility of Lagrange's theorem is immediately apparent. For example, we can use it to deduce if G is a finite group with identity element e, then $\bar{a}^{|G|} = \bar{e}, \forall a \in G$.

Quick proof: If $|\langle a \rangle| = m$, then $\bar{a}^m = \bar{e}$ and by Lagrange's theorem, $|G| = km$ for some integer k, and thus

$$\bar{a}^{|G|} = (\bar{a}^m)^k = \bar{e}.$$

The next application of Lagrange's theorem is an important theorem:

Theorem 4: Euler's theorem [FM19, Corollaries 8.28–8.29], [Dav21, Corollaries 8.15–8.17]

If positive integers a and n satisfy $\gcd(a, n) = 1$, then

$$a^{\phi(n)} \equiv 1 \mod n,$$

where $\phi(n)$ is Euler's totient function.

Proof. Consider the finite group $\mathbb{Z}_n^*$ and its subgroup U_n consisting of the units of $\mathbb{Z}_n^*$.

By Example 9, if $a \in G$ and $\gcd(a, n) = 1$, then $a \in U_n$ and $|U_n| = \phi(n)$. By Lagrange's theorem,

$$\bar{a}^{|G|} = \bar{1} = \bar{a}^{k|U_n|},$$

for some integer k. Therefore,

$$\bar{a}^{k|U_n|} = (\bar{a}^{\phi(n)})^k = \bar{1}.$$

In order for the preceding equation to be true for any k,

$$\bar{a}^{\phi(n)} = \bar{1} \implies a^{\phi(n)} \equiv 1 \mod n.$$

□

When n is a prime, Euler's theorem leads to *Fermat's little theorem*:

$$a^p \equiv a \mod p, \tag{4}$$

for prime p. Fermat's little theorem forms the basis of the RSA cryptosystem [Opp05, Sec. 14.2.1.3].

Lagrange's theorem also gives rise to the following theorem, which the Diffie-Hellman key exchange protocol depends on:

Theorem 5: [Sma16, Lemma 100.40], [Dav21, Corollary 8.19]

Any group of prime order is cyclic.

Proof. Suppose a is a non-identity element of prime-order group G, then $\langle a \rangle$ is a subgroup of G, and Lagrange's theorem necessitates that $|\langle a \rangle|$ divides $|G|$. Since $|G|$ is prime, $|\langle a \rangle|$ must be either 1 or $|G|$, but by definition of a, $|\langle a \rangle| \neq 1$. Therefore, $|\langle a \rangle| = |G| \implies G = \langle a \rangle$. □

3 References

[COFMR19] C. Carstensen-Opitz, B. Fine, A. Moldenhauer, and G. Rosenberger, *Abstract Algebra: Applications to Galois Theory, Algebraic Geometry, Representation Theory and Cryptography*, De Gruyter, 2019. https://doi.org/10.1515/9783110603996.

[Coh03] P. Cohn, *Basic Algebra: Groups, Rings and Fields*, Springer, 2003.

[Dav21] B. Davvaz, *A first course in group theory*, Springer, 2021. https://doi.org/10.1007/978-981-16-6365-9.

[DF99] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 2nd ed., John Wiley & Sons, Inc., 1999.

[FM19] D. R. Finston and P. J. Morandi, *Abstract Algebra: Structure and Application*, *Springer Undergraduate Texts in Mathematics and Technology*, Springer International Publishing Switzerland, 2019, corrected publication. https://doi.org/10.1007/978-3-319-04498-9.

[Gar01] P. Garrett, *Making, Breaking Codes: Introduction to Cryptology*, Pearson, 2001.

[KL21] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 3rd ed., CRC Press, 2021. Available at https://ebookcentral.proquest.com/lib/unisa/detail.action?docID=6425020.

[LN94] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, revised ed., Cambridge University Press, 1994.

[Lov22] S. Lovett, *Abstract Algebra: A First Course*, 2nd ed., Chapman and Hall/CRC, 2022. https://doi.org/10.1201/9781003299233.

[Opp05] R. Oppliger, *Contemporary Cryptography*, Artech House, Inc., 2005.

[Sma16] N. P. Smart, *Cryptography Made Simple*, *Information Security and Cryptography*, Springer International Publishing Switzerland, 2016. https://doi.org/10.1007/978-3-319-21936-3.