Algebraic Structures: Groups, Rings, and Fields
The RSA Cryptosystem

Rivest, Shamir, and Adelman (1978)

RSA is one of the most used cryptographic protocols on the net. Your browser uses it to establish a secure session with a site.
\[ Z_n = \{0, 1, 2, ..., n-1\} \]
\[ Z_n^* = \{x \in Z_n \mid \text{GCD}(x,n) = 1\} \]

Quick raising to power.

\[ <Z_n, +_n> \]
1. Closed
2. Associative
3. 0 is identity
4. Additive Inverses
   Fast + and -
5. Cancellation
6. Commutative

\[ <Z_n^*, *_n> \]
1. Closed
2. Associative
3. 1 is identity
4. Multiplicative Inverses
   Fast * and /
5. Cancellation
6. Commutative
Fundamental lemma of powers.

Suppose $x \in \mathbb{Z}_n^*$, and $a, b, n$ are naturals.

If $a \equiv \Phi(n) \pmod{\Phi(n)}$ and $b \equiv \Phi(n) \pmod{\Phi(n)}$, then $x^a \equiv x^b \pmod{n}$.

Equivalently,

$x^a \equiv x^a \pmod{n}$.
Euler Phi Function

\[ \Phi(n) = \text{size of } Z_n^* \]

\[ \begin{align*}
p \text{ prime } & \Rightarrow Z_p^* = \{1, 2, 3, \ldots, p-1\} \\
& \Rightarrow \phi(p) = p-1
\end{align*} \]

\[ \phi(pq) = (p-1)(q-1) \]

if \( p, q \) distinct primes
RSA is one of the most used cryptographic protocols on the net. Your browser uses it to establish a secure session with a site.
Pick secret, random large primes: p, q

“Publish”: n = p*q

\[ \phi(n) = \phi(p) \phi(q) = (p-1)*(q-1) \]

Pick random \( e \in \mathbb{Z}^*_{\phi(n)} \)

“Publish”: e

Compute \( d = \text{inverse of } e \text{ in } \mathbb{Z}^*_{\phi(n)} \)

Hence, \( e*d = 1 \pmod{\phi(n)} \)

“Private Key”: d

\[ x^{ed} \pmod{n} = x^{ed \mod{\phi(n)}} \pmod{n} = x \pmod{n} \]
p, q random primes, e random $\in \mathbb{Z}^*_{\phi(n)}$

$n = p^*q$

e*d = 1 [ mod $\phi(n)$ ]

$n,e$ is my public key. Use it to send me a message.
p, q prime, \( n = p \cdot q \), random \( e \in \mathbb{Z}_\phi(n)^* \).

\[ e \cdot d = 1 \mod \phi(n) \]

Suppose you could factor \( n = p \cdot q \).

\[ m = (m^e)^d \equiv m \mod n \]
An even simpler system
Today we are going to study the abstract properties of binary operations.
Rotating a Square in Space

Imagine we can pick up the square, rotate it in any way we want, and then put it back on the white frame.
In how many different ways can we put the square back on the frame?
We will now study these 8 motions, called *symmetries of the square*.
Symmetries of the Square

\[ Y_{\text{SQ}} = \{ R_0, R_{90}, R_{180}, R_{270}, F|, F-, F/, F\backslash \} \]
Composition

Define the operation “•” to mean “first do one symmetry, and then do the next”

For example,

\[ R_{90} \cdot R_{180} \]

means “first rotate 90° clockwise and then 180°”

\[ = R_{270} \]

\[ F_1 \cdot R_{90} \]

means “first flip horizontally and then rotate 90°”

\[ = F_\slant \]

Question: if \( a, b \in Y_{SQ} \), does \( a \cdot b \in Y_{SQ} \)? Yes!
Some Formalism

If $S$ is a set, $S \times S$ is:
the set of all (ordered) pairs of elements of $S$

$S \times S = \{ (a,b) \mid a \in S \text{ and } b \in S \}$

If $S$ has $n$ elements, how many elements
does $S \times S$ have? $n^2$

Formally, $\bullet$ is a function from $Y_{SQ} \times Y_{SQ}$ to $Y_{SQ}$

$\bullet : Y_{SQ} \times Y_{SQ} \to Y_{SQ}$

As shorthand, we write $\bullet(a,b)$ as “$a \bullet b$”
“•” is called a \textit{binary operation} on $Y_{SQ}$

\textbf{Definition:} A binary operation on a set $S$ is a function $\bullet : S \times S \rightarrow S$

\textbf{Example:}

The function $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ defined by

$$f(x, y) = xy + y$$

is a binary operation on $\mathbb{N}$
Associativity

A binary operation ♦ on a set S is associative if:

for all $a, b, c \in S$, \[(a \circ b) \circ c = a \circ (b \circ c)\]

Examples:

Is $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $f(x, y) = xy + y$ associative?

$(ab + b)c + c = a(bc + c) + (bc + c)$? NO!

Is the operation • on the set of symmetries of the square associative? YES!
Commutativity

A binary operation ♦ on a set $S$ is **commutative** if

$$\text{For all } a, b \in S, \quad a \circ b = b \circ a$$

Is the operation $\circ$ on the set of symmetries of the square commutative? **NO!**

$$R_{90} \circ F_1 \neq F_1 \circ R_{90}$$

*Check!*
Identities

$R_0$ is like a null motion

Is this true: $\forall a \in Y_{SQ}, \ a \bullet R_0 = R_0 \bullet a = a$? YES!

$R_0$ is called the identity of $\bullet$ on $Y_{SQ}$

In general, for any binary operation $\diamond$ on a set $S$, an element $e \in S$ such that for all $a \in S$,

$e \diamond a = a \diamond e = a$

is called an identity of $\diamond$ on $S$
Inverses

**Definition:** The inverse of an element \( a \in Y_{SQ} \) is an element \( b \) such that:

\[
a \cdot b = b \cdot a = R_0
\]

**Examples:**

- \( R_{90} \) inverse: \( R_{270} \)
- \( R_{180} \) inverse: \( R_{180} \)
- \( F_\| \) inverse: \( F_\| \)
Every element in $Y_{sq}$ has a unique inverse.
Groups

A group $G$ is a pair $(S, \diamond)$, where $S$ is a set and $\diamond$ is a binary operation on $S$ such that:

1. $\diamond$ is associative \( \forall a,b,c \in S \quad (a \diamond b) \diamond c = a \diamond (b \diamond c) \)

2. (Identity) There exists an element $e \in S$ such that:
   \[ e \diamond a = a \diamond e = a, \quad \text{for all } a \in S \]

3. (Inverses) For every $a \in S$ there is $b \in S$ such that: $a \diamond b = b \diamond a = e$

If $\diamond$ is commutative, then $G$ is called a commutative group \( \text{ (or Abelian group) } \)
Examples

Is $(\mathbb{N}, +)$ a group?

Is $+$ associative on $\mathbb{N}$? YES!

Is there an identity? YES: 0

Does every element have an inverse? NO!

$\exists a \in \mathbb{N}$ s.t. $a + (5) = 0$

$(\mathbb{N}, +)$ is NOT a group
Examples

Is \((\mathbb{Z},+)\) a group?

Is \(+\) associative on \(\mathbb{Z}\)?  YES!
Is there an identity? YES: 0
Does every element have an inverse? YES!

\((\mathbb{Z},+)\) is a group
Examples

Is \((Y_{SQ}, \mathbin{\cdot})\) a group?

Is \(\mathbin{\cdot}\) associative on \(Y_{SQ}\)? YES!

Is there an identity? YES: \(R_0\)

Does every element have an inverse? YES!

\((Y_{SQ}, \mathbin{\cdot})\) is a group
Examples

Is \((\mathbb{Z}_n, +)\) a group?

Is + associative on \(\mathbb{Z}_n\)? \(\text{YES!}\)

Is there an identity? \(\text{YES: 0}\)

Does every element have an inverse? \(\text{YES!}\)

\(a \in \mathbb{Z}_n \implies n - a \in \mathbb{Z}_n\)

\((\mathbb{Z}_n, +)\) is a group
Examples

Is \((\mathbb{Z}_n^*, \cdot)\) a group?

Is \(\cdot\) associative on \(\mathbb{Z}_n^*\)?  \hspace{1cm} \text{YES!}

Is there an identity?  \hspace{1cm} \text{YES: 1 (multiplicative identity)}

Does every element have an inverse?  \hspace{1cm} \text{YES!}

\(a \in \mathbb{Z}_n^*\) does there exist \(b \in \mathbb{Z}_n^*\) \hspace{1cm} \text{s.t.} \ a \cdot b = 1 \ (\text{mod} n) \ ?

\((\mathbb{Z}_n^*, \cdot)\) is a group
Identity Is Unique

**Theorem:** A group has at most one identity element

**Proof:**
Suppose e and f are both identities of G=(S, ♦)

Then f = e ♦ f = e
Theorem: Every element in a group has a unique inverse

Proof:
Suppose \( b \) and \( c \) are both inverses of \( a \)

Then \( b = b \uparrow e = b \uparrow (a \uparrow c) = (b \uparrow a) \uparrow c = c \)
A group $G = (S, \ast)$ is **finite** if $S$ is a finite set. Define $|G| = |S|$ to be the **order** of the group (i.e., the number of elements in the group).

What is the group with the least number of elements? $G = (\{e\}, \ast)$ where $e \ast e = e$

How many groups of order 2 are there?

$(\mathbb{Z}_3, +)$
Generators

A set $T \subseteq S$ is said to generate the group $G = (S, \triangleright)$ if every element of $S$ can be expressed as a finite product of elements in $T$.

Question: Does $\{R_{90}\}$ generate $Y_{SQ}$? NO!

Question: Does $\{S_1, R_{90}\}$ generate $Y_{SQ}$? YES!

A single element $g \in S$ is called a generator of $G=(S, \triangleright)$ if $\{g\}$ generates $G$.

Does $Y_{SQ}$ have a generator? NO!
Generators For \((\mathbb{Z}_n, +)\)

Any \(a \in \mathbb{Z}_n\) such that \(\text{GCD}(a,n) = 1\) generates \(\mathbb{Z}_n\)

**Claim:** If \(\text{GCD}(a,n) = 1\), then the numbers \(a, 2a, \ldots, (n-1)a, na\) are all distinct modulo \(n\)

**Proof (by contradiction):**
Suppose \(xa = ya \pmod{n}\) for \(x, y \in \{1, \ldots, n\}\) and \(x \neq y\)

Then \(n \mid a(x-y)\)

Since \(\text{GCD}(a,n) = 1\), then \(n \mid (x-y)\), which cannot happen
There are exactly 8 distinct multiples of 3 modulo 8.

hit all numbers ⇔ 3 is a generator for $\mathbb{Z}_8$
There are exactly 2 distinct multiples of 4 modulo 8.

4 does not generate $\mathbb{Z}_8$. 
There are exactly
\( \frac{\text{LCM}(n,c)}{c} = \frac{n}{\text{GCD}(c,n)} \)
distinct multiples of \( c \) modulo \( n \)

and hence

elements \( c \) with \( \text{GCD}(c,n) = 1 \)
generate \( \mathbb{Z}_n \)
If $G = (S, \cdot)$, we use $a^n$ denote $(a \cdot a \cdot \ldots \cdot a)$ $n$ times.

**Definition:** The order of an element $a$ of $G$ is the smallest positive integer $n$ such that $a^n = e$ $n > 0$.

**Lemma:** $a$ is a generator of $G$ if order($a$) = $|G|$.
If $G = (S, \diamond)$, we use $a^n$ denote $(a \diamond a \diamond \ldots \diamond a)$ $n$ times.

Definition: The **order** of an element $a$ of $G$ is the smallest positive integer $n$ such that $a^n = e$.

What is the order of $F_1$ in $Y_{SQ}$? 2
What is the order of $R_{90}$ in $Y_{SQ}$? 4

The order of an element can be infinite!
Example: The order of 1 in the group $(Z, +)$ is infinite.
Orders

What if $G$ is a finite group:
is the order of any element of $G$ finite?

Yes: consider $a, a^2, a^3, a^4, a^5, \ldots$
Since $G$ is finite, at some point $a^j = a^k$ for some $j < k$.
Hence $a^{k-j} = \text{identity}$. 

using pigeonhole!
There are exactly
\[ \frac{\text{LCM}(n,c)}{c} = \frac{n}{\text{GCD}(c,n)} \]
distinct multiples of \( c \) modulo \( n \)

and hence

\[ \text{order}_{(\mathbb{Z}_n,+)}(c) = \frac{n}{\text{GCD}(c,n)} \]

\( \text{order} (3) \) in \( \mathbb{Z}_8 \) was 8, \( \text{order} (4) \) in \( \mathbb{Z}_8 \) was 2.

3, 6, 1, 4, 7, 2, 5, 0, 4, 0.
What about \((\mathbb{Z}_n^{\ast}, \ast)\)?

What is order of the group \(\mathbb{Z}_n^{\ast}\)?
\[|\mathbb{Z}_n^{\ast}| = \varphi(n)\]

Does \(\mathbb{Z}_n^{\ast}\) have generators?

What are the orders of elements in \(\mathbb{Z}_n^{\ast}\)?
\( Z_7^* = \{1,2,3,4,5,6\} \)

\[
\begin{align*}
2^0 &= 1; & 2^1 &= 2; & 2^2 &= 4; & 2^3 &= 1 \\
3^0 &= 1; & 3^1 &= 3; & 3^2 &= 2; & 3^3 &= 6; & 3^4 &= 4; \\
& & 3^5 &= 5; & 3^6 &= 1
\end{align*}
\]

2 generates \( \{1, 2, 4\} \) \hspace{1cm} \text{Order 3}

3 generates \( \{1, 2, 3, 4, 5, 6\} \) \hspace{1cm} \text{Order 6}

3 is a generator, but 2 is not.
Theorem (Non-trivial)

**Thm:** There are $\phi(n-1)$ generators of the group $(\mathbb{Z}_n^*, *)$

E.g.,

for $\mathbb{Z}_7^*$, $\phi(7-1) = \phi(2*3) = 2$.

Generators: 3, 5

You can check that:

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

Orders: 1, 3, 6, 3, 6, 2
Orders

Theorem:

Let $x$ be an element of $G$. The order of $x$ divides the order of $G$. 

\[ \text{order}(x) \mid |G| \]

proof coming soon...
Subgroups

Given a group $G = (S, \diamond)$, a subset $S' \subseteq S$ forms a subgroup if $H = (S', \diamond)$ satisfies the group properties.

That is,

- $S'$ is **closed** under the group operation $\diamond$
- The **identity** element of $G$ is also in $S'$.
- The **inverse** of every element in $S'$ is also in $S'$.

$Y_{SQ}$ subgroup $Y_R = \{ R_0, R_{90}, R_{180}, R_{270} \}$
Examples

\[ Y_{\text{rot}} = \{ R_0, R_{90}, R_{180}, R_{270} \} \]

is a subgroup of

\[ Y_{\text{SQ}} = \{ R_0, R_{90}, R_{180}, R_{270}, F|, F-, F\, , F\_ \} \]

**Quick check:**

Closure?
Identity?
Inverses?
**Examples**

\[ \mathbb{Z}_{8, \text{even}} = \{0, 2, 4, 6\} \]

with the + operation is a subgroup of
\[ \mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\} \]

**Quick check:**
- Closure?
- Identity?
- Inverses?
Lagrange’s Theorem

**Theorem:** if $H$ is a subgroup of $G$, then $|H|$ divides $|G|$.

**Fact:** The set generated by any element $x \in G$ is a subgroup of $G$.

$$S' = \{ x, x^2, x^3, \ldots \}$$

$S'$ is a subgroup of $S$.

$$|S'| = \text{order}(x) \left| S \right|$$

**Corollary:** the order of any element $x \in G$ divides $|G|$. 
Proof of Lagrange's Theorem
A ring is a set together with two operations (usually called \(+\) and \(\times\)) modulo multiplication.

For example, in \(\mathbb{Z}_n\), we can do addition and we can define more than one operation on a set of The Rings.
A ring \( R \) is a set together with two binary operations \( + \) and \(*\), satisfying the following properties:

1. \((R,+)\) is a commutative group
2. \( * \) is associative

The distributive laws hold in \( R \):

\[
(a + b) * c = (a * c) + (b * c) \\
a * (b + c) = (a * b) + (a * c)
\]
Examples

Do the integers \( \mathbb{Z} \) form a ring?

\((\mathbb{Z}, +)\) is a commutative group.

* is associative

+ distributes over *...
Fields

Definition:

A field $F$ is a set together with two binary operations $+$ and $\ast$, satisfying the following properties:

1. $(F,+)$ is a commutative group

2. $(F-\{0\},\ast)$ is a commutative group

3. The distributive law holds in $F$:
   
   \[(a + b) \ast c = (a \ast c) + (b \ast c)\]
Examples

Do the integers $\mathbb{Z}$ form a field?

$(\mathbb{Z}, +)$ is a commutative group.

but $(\mathbb{Z}\setminus\{0\}, \ast)$ do not form a group!
there are no multiplicative inverses...
Examples

$\mathbb{Z}_p$ (for prime $p$) is a field.

$(\mathbb{Z}_p, +)$ is a commutative group.

$(\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}, \ast)$ is a commutative group.

The distributive law holds.
Examples

The real numbers $\mathbb{R}$ form a field.

$(\mathbb{R}, +)$ is a commutative group.

$(\mathbb{R} \setminus \{0\}, *)$ is a commutative group.

The distributive law holds.
CRYPTOGRAPHY based on the presumed computational difficulty of a number theoretic problem.

Let $p$ be prime. $g$ be a generator for $(\mathbb{Z}_p^*, *)$

$DH_{p,g}(x) = g^x \mod p$ is fast to compute.

$\text{DISCRETE-LOG}_{p,g}(r) = x$ means that $g^x = r \mod p$.

No one knows a fast algorithm given a random $r$ to compute $x$. 

Let $p$ be prime, $g$ be a generator mod $p$.

**Alice:** Picks random $x \in \mathbb{Z}_{p-1}$
Publishes $g^x \mod p$

**Bob:** Picks random $y \in \mathbb{Z}_{p-1}$
Publishes $g^y \mod p$

Both parties can compute (mod $p$)

$$(g^x)^y = (g^y)^x = g^{xy} \mod p-1$$

Eve sees both published strings. Can she figure out $g^{xy} \mod p$? Does not know $x$ & $y$. 
Diffie-Hellman has an amazing feature.

Two people who have never met and have no prior shared secrets can use the system.

Without this property, commerce on the net would be impossible.

Typical use: Agree on a random string r.

Use r as your secret-key in a more conventional private-key crypto-system.

Use r as your secret-key in a more conventional private-key crypto-system.
In The End...

Why should I care about any of this?

Groups, Rings, and Fields are examples of the principle of abstraction: the particulars of the objects are abstracted into a few simple properties.

All the results carry over to any group.

Ideas central to crypto and other areas!
Symmetries of the Square

Compositions

Groups

Binary Operation

Identity and Inverses

Basic Facts: Inverses Are Unique

Generators

Rings and Fields

Definition

Study Bee