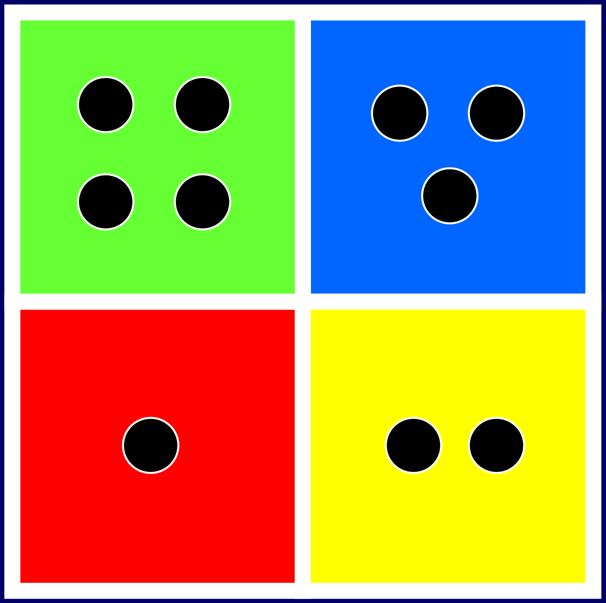
Algebraic Structures: Groups, Rings, and Fields



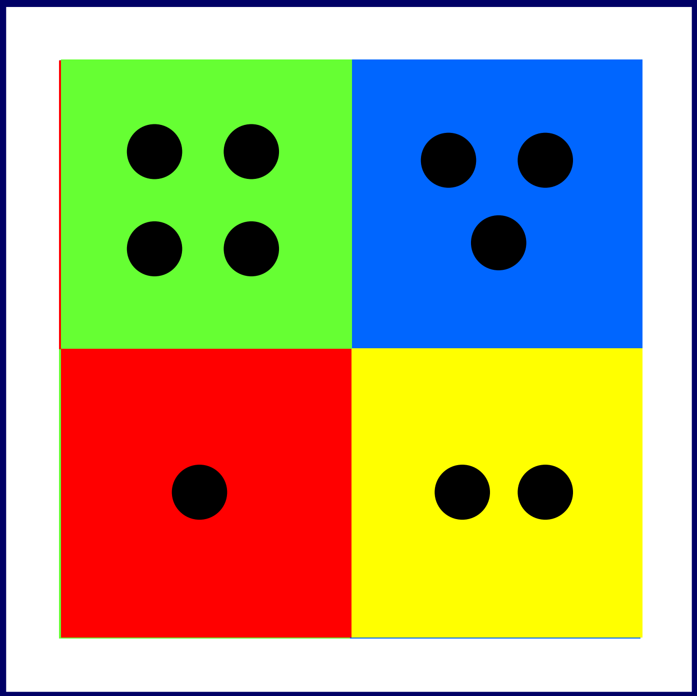
The RSA Cryptosystem

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.

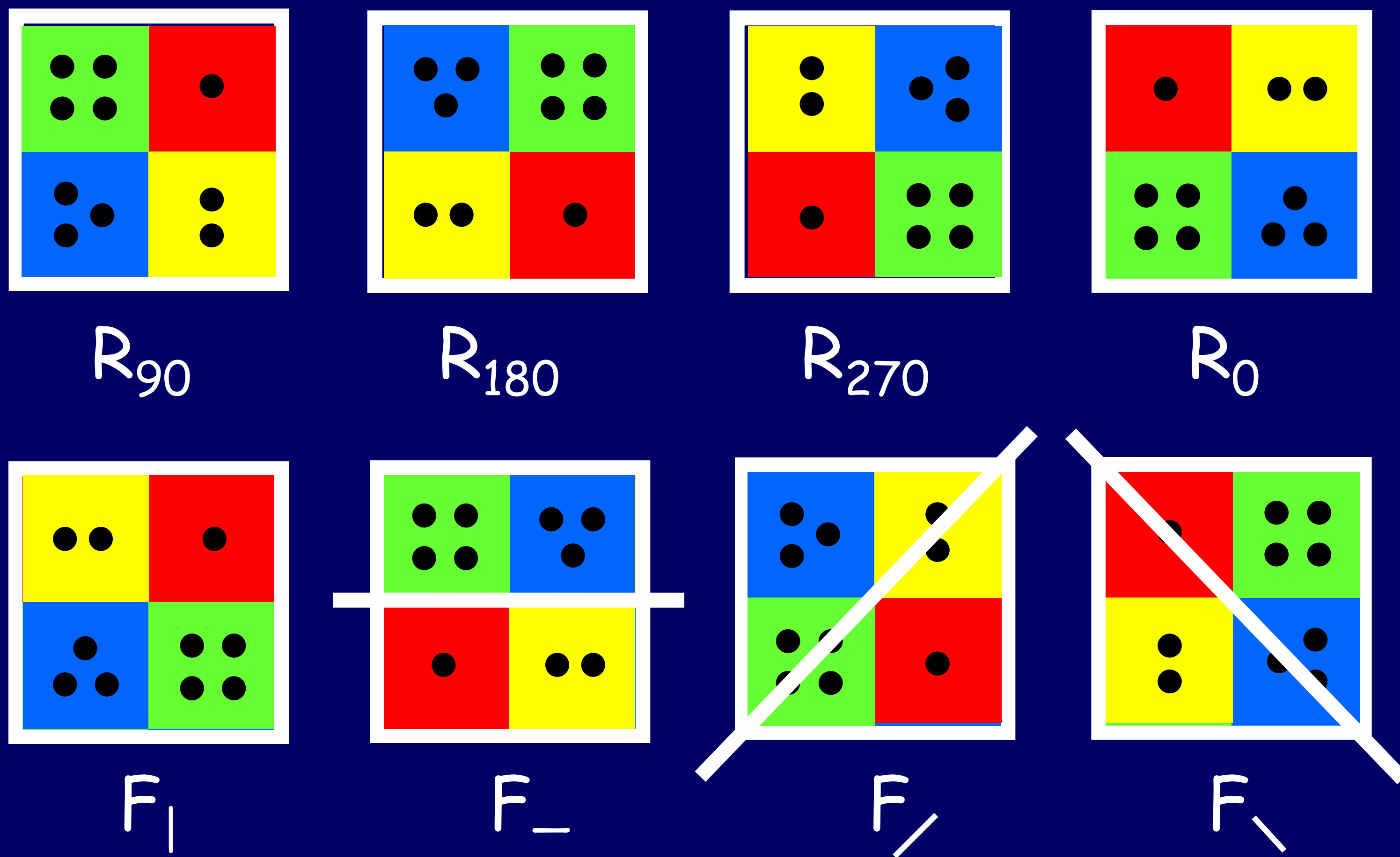
Today we are going to study the abstract properties of binary operations

Rotating a Square in Space

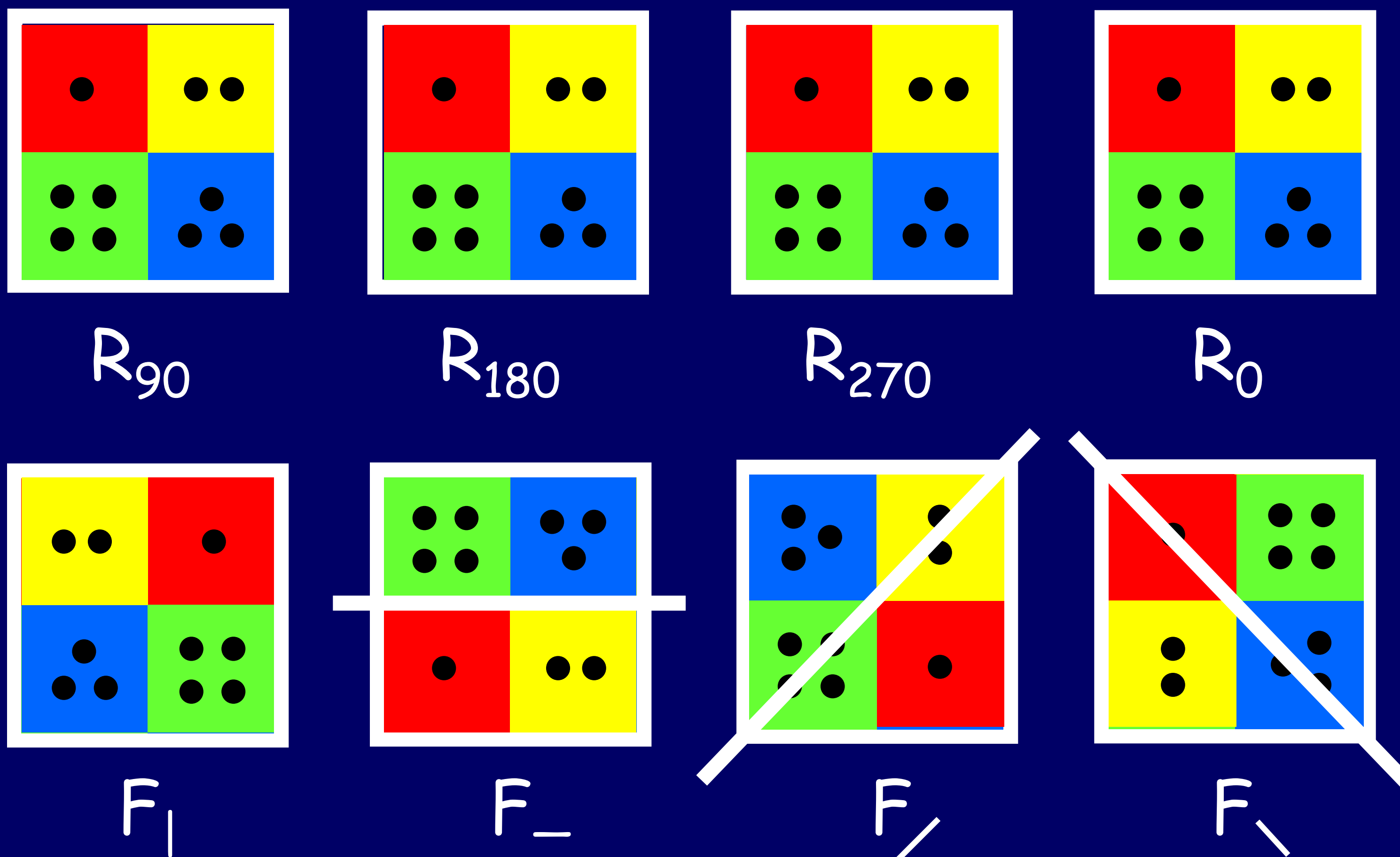


Imagine we can pick up the square, rotate it in any way we want, and then put it back on the white frame

In how many different ways can we put the square back on the frame?



In how many different ways can we put the square back on the frame?



Symmetries of the Square

$Y_{SQ} = \{ R_0, R_{90}, R_{180}, R_{270}, F_{|}, F_{-}, F_{/}, F_{\backslash} \}$

Composition

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

For example,

$R_{90} \bullet R_{180}$ means "first rotate 90° clockwise and then 180°"

$= R_{270}$

$F_{|} \bullet R_{90}$ means "first flip horizontally and then rotate 90°"

$= F_{/}$

Question: if $a,b \in Y_{SQ}$, does $a \bullet b \in Y_{SQ}$? Yes!

	R_{0}	R_{90}	R_{180}	R_{270}	$F_{\vert}$	F_{-}	$F_{/}$	$F_{\backslash}$
R_{0}	R_{0}	R_{90}	R_{180}	R_{270}	$F_{\vert}$	F_{-}	$F_{/}$	$F_{\backslash}$
R_{90}	R_{90}	R_{180}	R_{270}	R_{0}	$F_{\backslash}$	$F_{/}$	$F_{\vert}$	F_{-}
R_{180}	R_{180}	R_{270}	R_{0}	R_{90}	F_{-}	$F_{\vert}$	$F_{\backslash}$	$F_{/}$
R_{270}	R_{270}	R_{0}	R_{90}	R_{180}	$F_{/}$	$F_{\backslash}$	F_{-}	$F_{\vert}$
$F_{\vert}$	$F_{\vert}$	$F_{/}$	F_{-}	$F_{\backslash}$	R_{0}	R_{180}	R_{90}	R_{270}
F_{-}	F_{-}	$F_{\backslash}$	$F_{\vert}$	$F_{/}$	R_{180}	R_{0}	R_{270}	R_{90}
$F_{/}$	$F_{/}$	F_{-}	$F_{\backslash}$	$F_{\vert}$	R_{270}	R_{90}	R_{0}	R_{180}
$F_{\backslash}$	$F_{\backslash}$	$F_{\vert}$	$F_{/}$	F_{-}	R_{90}	R_{270}	R_{180}	R_{0}

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}

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

As shorthand, we write $\bullet(a,b)$ as "$a \bullet b$"

Called the short hand notation

Binary Operations

"•" is called a binary operation on Y_{SQ}

Definition: A binary operation on a set S is a function $\blacklozenge : S \times S \to S$

Example:

The function f: $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 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:

$$\text{for all } a,b,c \in S, \quad (a \blacklozenge b) \blacklozenge c = a \blacklozenge (b \blacklozenge c)$$

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

In associativity, the order is not important, but to have commutativity, the order must be there.

A binary operation ♦ on a set S is commutative if

For all $a,b \in S$, $a \blacklozenge b = b \blacklozenge a$

Is the operation • on the set of symmetries of the square commutative? NO!

$$R_{90} \bullet F_{|} \neq F_{|} \bullet R_{90}$$

Note that R0 is not fixed, it can be changed, means identity can be changed.

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 $\blacklozenge$ on a set S, an element $e \in S$ such that for all $a \in S$,

$$e \blacklozenge a = a \blacklozenge e = a$$

is called an identity of $\blacklozenge$ on S

Inverses

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

$$a \bullet b = b \bullet a = R_0$$

Examples:

R_{90} inverse: R_{270}

R_{180} inverse: R_{180}

$F_{|}$ inverse: $F_{|}$

Every element in Y_{SQ} has a unique inverse

Every row and column have only and only one R0 and hence unique inverse will be present.

	R_{0}	R_{90}	R_{180}	R_{270}	$F_{\mid}$	F_{-}	$F_{/}$	$F_{\backslash}$
R_{0}	R_{0}	R_{90}	R_{180}	R_{270}	$F_{\mid}$	F_{-}	$F_{/}$	$F_{\backslash}$
R_{90}	R_{90}	R_{180}	R_{270}	R_{0}	$F_{\backslash}$	$F_{/}$	$F_{\mid}$	F_{-}
R_{180}	R_{180}	R_{270}	R_{0}	R_{90}	F_{-}	$F_{\mid}$	$F_{\backslash}$	$F_{/}$
R_{270}	R_{270}	R_{0}	R_{90}	R_{180}	$F_{/}$	$F_{\backslash}$	F_{-}	$F_{\mid}$
$F_{\mid}$	$F_{\mid}$	$F_{/}$	F_{-}	$F_{\backslash}$	R_{0}	R_{180}	R_{90}	R_{270}
F_{-}	F_{-}	$F_{\backslash}$	$F_{\mid}$	$F_{/}$	R_{180}	R_{0}	R_{270}	R_{90}
$F_{/}$	$F_{/}$	F_{-}	$F_{\backslash}$	$F_{\mid}$	R_{270}	R_{90}	R_{0}	R_{180}
$F_{\backslash}$	$F_{\backslash}$	$F_{\mid}$	$F_{/}$	F_{-}	R_{90}	R_{270}	R_{180}	R_{0}

Groups

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

1. $\blacklozenge$ is associative

2. (Identity) There exists an element $e \in S$ such that:

   $$e \blacklozenge a = a \blacklozenge e = a, \qquad \text{for all } a \in S$$

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

If $\blacklozenge$ is commutative, then G is called a commutative group Called 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!

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

Examples

Take care of additive and multiplicative inverse.

Is (Z,+) a group?

Is + associative on Z? YES!

Is there an identity? YES: 0

Does every element have an inverse? YES!

(Z,+) is a group

Examples

Is $(Y_{SQ}, \bullet)$ a group?

Is $\bullet$ associative on Y_{SQ}? YES!

Is there an identity? YES: R_0

Does every element have an inverse? YES!

$(Y_{SQ}, \bullet)$ is a group

Any number from Z can be converted to Z7 many to one mapping exists.

Examples

Note that Zn is a cyclic group, which contains only integers from 0 to (n-1) both inclusive.
It is like a mod operator, which repeats its values.
Z7 = K mod 7, = Remainder obtained when K is divided by 7.
Example: if n=7: then both 0 and 7 are in the group, with value a s zero. Hnece -1 will also be in the group with value as 6.

0, 1, 2, ...(n-1), these are like equivalence classes.

Is $(Z_n,+)$ a group?

Is + associative on Z_n? YES!

Is there an identity? YES: 0

Does every element have an inverse? YES!

$(Z_n, +)$ is a group

Examples

Zn* : the set of all numbers from 0 to (n-1) which are co-prime with n.
The concept is again same like the Zn.

Note that 0 will not be included in Zn*

Is $(Z_n^*, *)$ a group?

Is * associative on Z_n^*? YES!

Is there an identity? YES: 1

Does every element have an inverse? YES!

Inverse of 3 is 5, as 15 mod 7 is 1. Note that final output of multiplying any number with its inverse should be the identity.

$(Z_n^*, *)$ is a group

Identity Is Unique

Theorem: A group has at most one identity element

Proof:

Suppose e and f are both identities of $G=(S,\blacklozenge)$

Then $f = e \blacklozenge f = e$

Inverses Are Unique

Theorem: Every element in a group has a unique inverse

Proof:

Suppose b and c are both inverses of a

Then $b = b \blacklozenge e = b \blacklozenge (a \blacklozenge c) = (b \blacklozenge a) \blacklozenge c = c$

A group $G=(S,\blacklozenge)$ 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?

$G = (\{e\},\blacklozenge)$ where $e \blacklozenge e = e$

Generators

A set $T \subseteq S$ is said to generate the group $G = (S, \blacklozenge)$ 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 $\{S_{|}, R_{90}\}$ generate Y_{SQ}? YES!

Single element should be there, to be called the generator.

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

Does Y_{SQ} have a generator? NO!

Generators For $(Z_{n,}+)$

Any $a \in Z_n$ such that GCD(a,n) = 1 generates Z_n

Claim: If GCD(a,n) =1, then the numbers
a, 2a, …, (n-1)a, na are all distinct modulo n

If we multiply every element of Zn by a number co-prime with n, then the set will not change. There will be one to one mapping between the exixting set and the newly created set.

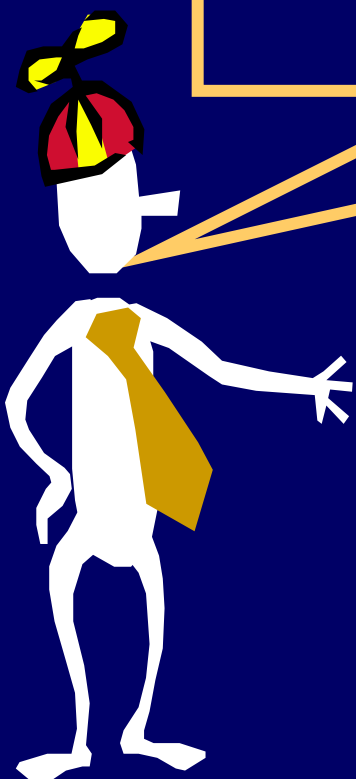
Proof (by contradiction):

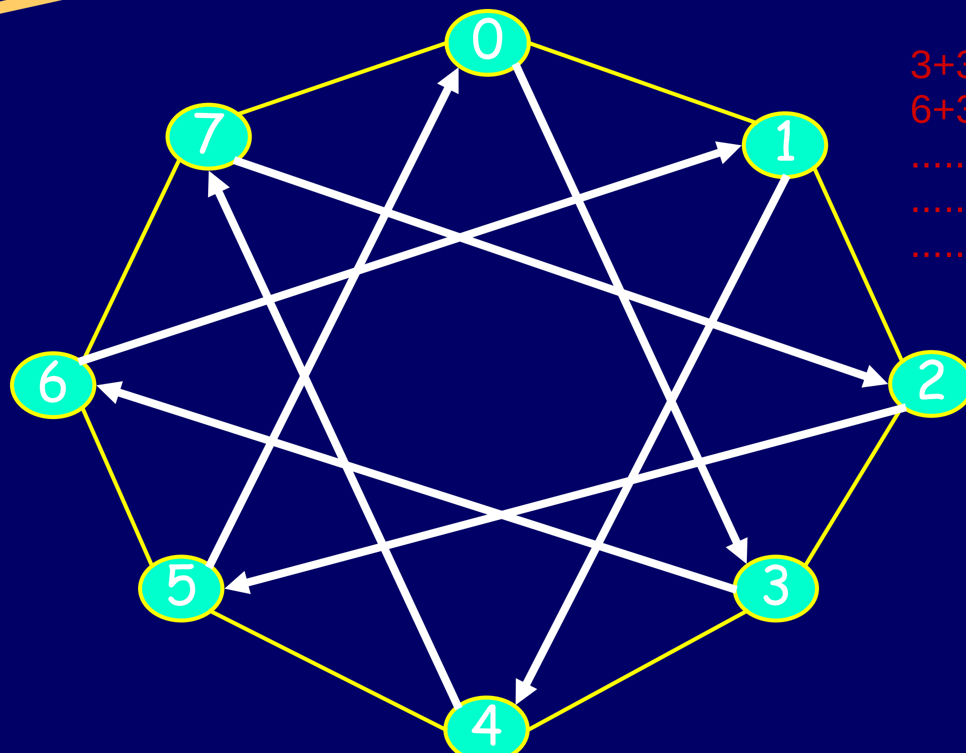
Suppose xa = ya (mod n) for $x,y \in \{1,\ldots,n\}$ and $x \neq y$

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

Since GCD(a,n) = 1, then $n \mid (x-y)$, which cannot happen

There are exactly 8 distinct multiples of 3 modulo 8.

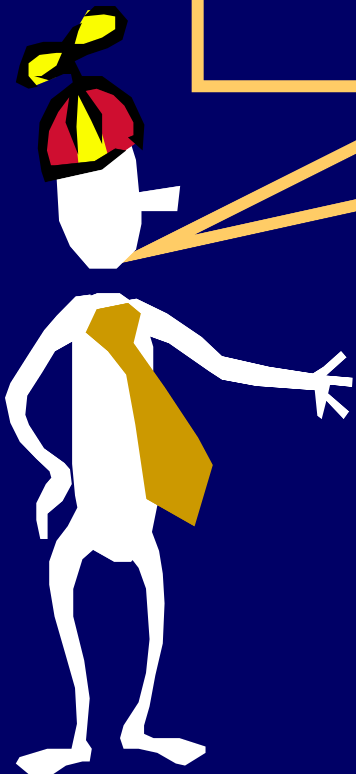


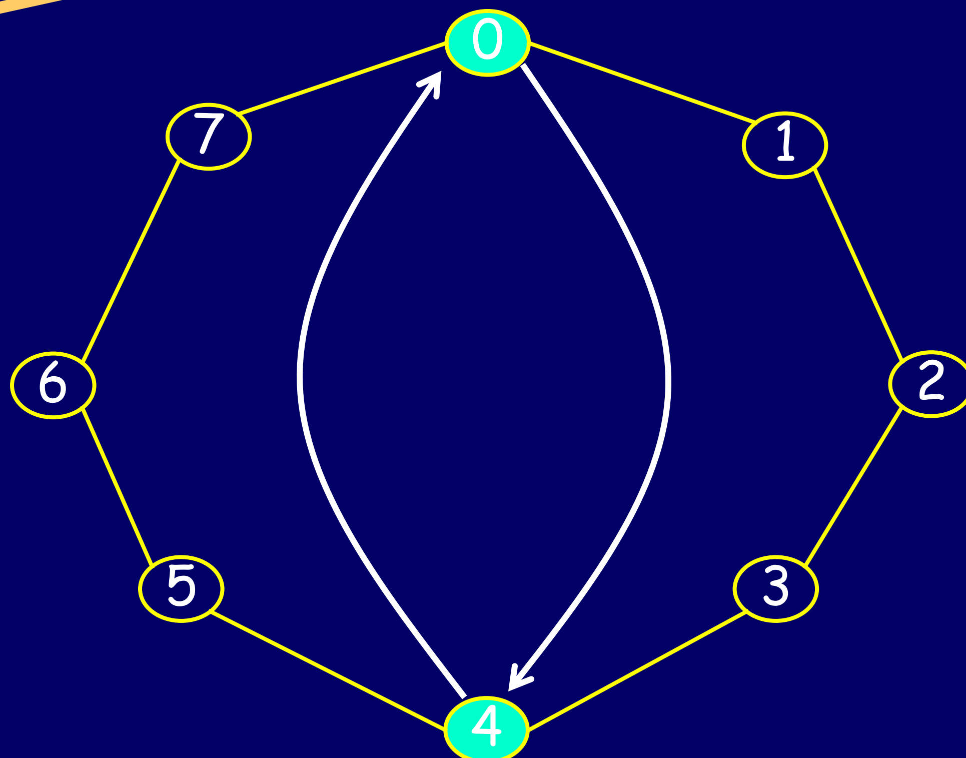


3+3=6
6+3=9 => 1.
……………………………………
……………………………………
…………

hit all numbers $\Leftrightarrow$ 3 is a generator for Z_8

There are exactly 2 distinct multiples of 4 modulo 8





4 does not generate Z_8

Order of an element

If $G = (S, \blacklozenge)$, we use a^n denote $\underbrace{(a \blacklozenge a \blacklozenge \ldots \blacklozenge a)}_{\text{n times}}$

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

Lemma: a is a generator of G if $\text{order}(a) = |G|$

If $G = (S, \blacklozenge)$, we use a^n denote $\underbrace{(a \blacklozenge a \blacklozenge \ldots \blacklozenge a)}_{\text{n times}}$

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 $F_|$ in Y_{SQ}? 2

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

The order of an element can be infinite!

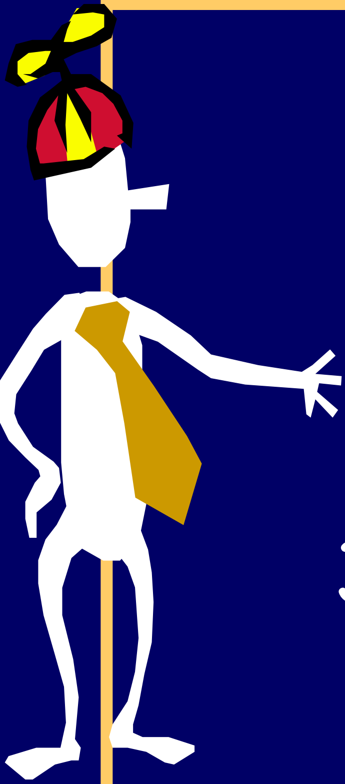
Example: The order of 1 in the group (Z,+) is infinite

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} = identity.

a^j (e-a^(k-j))=0; As a^j!=0 then a^(k-j)=e, and hence the order is k-j.



$Z_7^* = \{1,2,3,4,5,6\}$

$2^0 = 1;\ 2^1 = 2;\ 2^2 = 4;\ 2^3 = 1$

$3^0=1;\ 3^1 = 3;\ 3^2 = 2;\ 3^3 = 6;\ 3^4 = 4;$
$3^5 = 5;\ 3^6 = 1$

2 generates $\{1, 2, 4\}$ Order 3
3 generates $\{1,2,3,4,5,6\}$ Order 6

3 is a generator, but 2 is not.

Subgroups

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

That is,

S' is closed under the group operation $\blacklozenge$

The identity element of G is also in S'.

The inverse of every element in S' is also in S'.

Examples

$Y_{rot} = \{ R_0, R_{90}, R_{180}, R_{270} \}$

is a subgroup of

$Y_{SQ} = \{ R_0, R_{90}, R_{180}, R_{270}, F_|, F_-, F_/, F_\backslash \}$

<u>Quick check:</u>

Closure?

Identity?

Inverses?

Examples

$Z_{8,even} = \{0, 2, 4, 6\}$

with the + operation is a subgroup of

$Z_8 = \{0,1,2,3,4,5,6,7\}$

<u>Quick check:</u>

Closure?

Identity?

Inverses?

Rings

We can define more than one operation on a set

For example, in Z_n we can do addition and multiplication modulo n

A ring is a set together with two operations (usually called + and *)

Definition:

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

3. 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 *, satisfying the following properties:

1. (F,+) is a commutative group

2. (F-{0},*) is a commutative group

   Here, 0 is the identity in + operation, that's why, remove it.

3. The distributive law holds in F:

$$(a + b) * c = (a * c) + (b * c)$$

Examples

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

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

but $(\mathbb{Z}\backslash\{0\}, *)$ do not form a group!

there are no multiplicative inverses…

Examples

Z_p (for prime p) is a field.

$(Z_p, +)$ is a commutative group.

$(Z_p^* = Z_p \setminus \{0\},\ *)$ is a commutative group.

The distributive law holds.

Examples

The real numbers P form a field.

(P, +) is a commutative group.

(P\{0}, *) is a commutative group.

The distributive law holds.