

Why permutations?

- Easy family of functions to study composition, 1-1, onto, inverse, etc with.
- Easy to compute with.
- Exhibits periodic behavior—even before sin's and cos's.
- Illustrates how complex functions can be built up from simpler functions.
- Illustrates how algebra is a tool to model real-life (e.g. perfect shuffles).
- Bridge between concrete and abstract.

A **group** is an algebraic object consisting of a set G and a binary operation \diamond on G such that

- \diamond is associative
- There is an identity for G, \diamond
- Each element of G has an inverse

Examples of groups

- Any permutation group (e.g. S_n , A_n , rigid motions of an object)
- \mathbb{Z} under addition
- \mathbb{R} under addition
- Positive reals under multiplication
- The subsets of X under symmetric difference
- Klein-4

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

Multiplication and Addition are the same!

Lots of different groups are disguised versions of each other.

The positive reals under multiplication is just a disguised version of the reals under addition.

Why? Because there is a dictionary from the positive reals to the reals that translates any product equation into any addition equation.

Map $f : \mathbb{R}^+ \rightarrow \mathbb{R}$ by $f(x) = \log(x)$.

f is a good dictionary, because it is 1 – 1 and onto.

Also the statement $z = x \cdot y$ gets translated to the true statement $\log(z) = \log(x) + \log(y)$.

So (via the logarithm) any multiplication problem becomes an addition problem.

Algebra makes life simpler!

More than one operation

Groups only have one operation.

Familiar objects like the integers, rationals, reals that have both an addition and a multiplication. Often times it is useful to have more than one operation at a time.

Let S be a set and \heartsuit and \diamond be binary operations on S .
We say that \heartsuit is distributive over \diamond on S provided for each $x, y, z \in S$ we have

$$x \heartsuit (y \diamond z) = (x \heartsuit y) \diamond (x \heartsuit z)$$

- Multiplication over addition on \mathbb{R} ?

Addition over multiplication on \mathbb{R} ?

- Union over intersection on subsets of a given set?
- Maximum over addition on \mathbb{R} ?
- Addition over maximum on \mathbb{R} ?
- Intersection over union on subsets of a given set?

Soapbox time

General distributivity principle (for multiplication over addition in the reals): The product of n sums of numbers is the sum of all products whose factors consist of one term from each summand.

Examples

- $(x^3 - 1)(x^2 - 1)(x - 1)$.
- $(x + y)^n$
- $(1 + x + x^2 + x^3 + x^4 + x^5 + x^6)^2$
- How many ways can you roll 4 dice and get a sum of 13?

The integers

Have two operations addition and multiplication

- Addition is associative, commutative, has identity and each element has an additive inverse
- Multiplication is associative, commutative, has identity
- Multiplication distributes over addition (both left and right).

Any algebraic object satisfying this conditions is called a commutative **Ring**.

If we don't insist that the multiplication be commutative, then we have a **Ring**.

Examples of rings

- Integers, rationals, reals using addition and multiplication
- Polynomials over the integers, rationals or reals using polynomial addition and multiplication
- All functions from \mathbb{R} to \mathbb{R} using pointwise addition and multiplication
- The set of all subsets of a given set using symmetric difference as the addition, and intersection as the multiplication
- Etc. (see Field Guide)

What makes the integers, the integers?

The integers have an ordering: $x > y$ if and only if $x - y$ is positive. This ordering has the properties that 0 is not positive and that $x > 0$ and $y > 0 \Rightarrow xy > 0$, and $x + y > 0$.

This tells us quite a bit. If we have a ring $(R, +, \cdot)$ and an ordering > 0 on it such that 0 is not greater than 0, and $x > 0, y > 0 \Rightarrow xy > 0$.

- If $x > 0$, then $-x \not> 0$. (So we can say $y < 0$ provided $-y > 0$.)
- The multiplicative identity must be positive
- If $x > 0$ and $y < 0$, then $xy < 0$.
- If $x < 0$ and $y < 0$, then $xy > 0$

There's no ordering like this for the complexes.

Suppose $\mathbb{C} = P \cup \{0\} \cup N$.

Where could i be?

If $i \in P$, then $i > 0$ and $i > 0 \Rightarrow -1 = (i)^2 > 0$. Impossible.

If $i \notin P$, then $i < 0$ and $i < 0 \Rightarrow -1 = (-i)^2 > 0$. Impossible.

So the complexes don't have an ordering like the integers do.

$<$ is an ordering for the Reals; rationals?

What makes the reals different than the integers?

- Every nonzero element of the reals, rationals has a multiplicative inverse
- The Well-ordering property of the positive integers

An ordered set S has the well ordering property provided each nonempty subset X of S has a least element (i.e. $\exists x \in X$ such that $x \leq y$ for all $y \in X$)

Examples:

- Do integers have well ordering property?
- Do positive integers have well ordering property?
- Do positive rationals have well ordering property?
- Does the set $\{1/2, 1/4, 1/8, 1/16, \dots\}$ have the well ordering property?
- Do the positive even integers have the well ordering property?

So the WOP of the positive integers distinguished the integers from the rationals.

In fact, there is a theorem (Dedekind-Peano) that essentially says the WOP, and the previously listed properties are the defining properties of the integers.

The WOP of the positive integers is what allows induction:

(Principle of Induction) If S is a subset of the positive integers, $1 \in S$ and $j + 1 \in S$ whenever $j \in S$, then $S = \mathbb{P}$.

(Principle of Strong Induction) If S is a subset of positive integers, $1 \in S$ and $j + 1 \in S$ whenever each of $1, 2, \dots, j$ are in S , then $S = \mathbb{P}$.

Divides

Given integers a and b we say a divides b and write $a|b$ provided there exists an integer q such that $aq = b$.

Examples

- Does 3 divide 6?
- Does -3 divide 6?
- Does 7 divide 15?
- Does 5 divide 0?
- Does 0 divide 3?
- Does 0 divide 0?

Note $a|b$ is a statement, a/b is a number.

Properties of divides

- If $a|b$ and $b|a$, then
- $a|a$
- If $a|b$ and $b|c$ then
- If $x = y + z$ and k divides two of x, y , or z , then k divides the third.

The Division Algorithm

Let a and b be integers with $b \neq 0$, then there exist unique integers q and r such that

$$a = bq + r \text{ and } |b| > r \geq 0.$$

Examples:

- $a = 16$ and $b = 3$
- $a = 16$ and $b = 4$
- $a = -16$ and $b = 5$
- $a = 16$ and $b = 32$