

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)

General properties of a ring:

$$-(-x) = x$$

$$(-x)(y) = -xy$$

$$(-x)(-y) = xy.$$

What makes the integers, the integers?

The integers have an ordering: $x > y$ if and only if $x - y$ is positive.

Properties of the positive integers. $x, y \in P$:

- 1 Closed under $+$, closed under \cdot
- 2 x positive if and only if $-x$ negative
- 3 Each integer is either 0, positive, or negative

This tells us quite a bit.

- $x < 0$ and $y > 0 \Rightarrow xy < 0$.

Why?

$$-x > 0 \text{ and } y > 0 \Rightarrow (-x)y > 0 \Rightarrow -(xy) > 0 \Rightarrow xy < 0$$

- $x < 0$ and $y < 0 \Rightarrow xy > 0$.

Why? $-x > 0$, $-y > 0 \Rightarrow (-x)(-y) > 0$. But

$$(-x)(-y) = xy.$$

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 $b = 32$

Idea behind why division algorithm is true Existence of quotient and remainder for $a, b > 0$.

Idea: reduce to a smaller case.

If $0 < a < b$, then $a = b \cdot 0 + a$ works.

Otherwise, suppose we know quotient and remainder for $a - b$; say

$$a - b = b(q') + r.$$

Then $a = b(q' + 1) + r$ gives quotient $q = q' + 1$ and remainder r .

Can make this into a rigorous induction proof—but inductive thinking (i.e. reducing to a previous case is the more important point).

Uniqueness

Suppose $a = bq + r$ and $a = bu + s$ where $0 \leq r, s < b$.

Subtracting gives: $b(q - u) = s - r$.

LHS is multiple of b . RHS lies in $(-b, b)$.

So $s - r = 0$. That is, $s = r$.

Now equate two equations to get $bq = bu$, and hence $q = u$.

Prime numbers

An integer n is prime provided $n > 0$, and n has exactly two positive divisors.

- 1?
- 2?
- 3?
- 4?

importance of primes

Fundamental Theorem of Arithmetic Every positive integer is a product of primes.

Proof. By strong induction.

1 is the product of 0 primes

Suppose true for all integers less than n .

If n is prime, n is the product of a single prime and we are done.

Otherwise, $n = ab$ for some integers a and b with $1 < a, b < n$. Since a is a product of primes and b is a product of primes, so is $n = ab$. ■

Can actually show that up to re-ordering of the primes, there is just one way to write a given positive integer as a product of primes.

Only a finite number of primes are known!

Primes are valuable—they are used in providing secure communication (Cryptography)

Infinitude of primes

There exist an infinite number of primes.

Proof. Suppose not. List them as p_1, p_2, \dots, p_k .

Consider $n = p_1 p_2 \cdots p_k + 1$.

Any prime divisor of n would divide 1 (by the 2 out of 3 rule).
But a prime can't divide 1; so we have a contradiction. ■

Euclid's Lemma

Let p be a prime and a and b be integers. Then $p|ab \Rightarrow p|a$ or $p|b$.

Sketch of proof in case a and b positive.

If $p|a$ done. Otherwise use the Division Algorithm to write $a = pq + r$ for some $0 < r < p$.

$p|ab \Rightarrow pk = ab$ for some integer k

Substitution give $pk = (pq + r)b = pqb + rb$.

By 2-out-of-3 rule, $p|rb$.

We've reduced to a smaller case $r < b$. So $p|b$. ■