Math 141: Lecture 2

Integers, rationals, reals

Bob Hough

August 31, 2016

Definition of $\mathbb{Z}$

To form the integers $\mathbb{Z}$ from the natural numbers $\mathbb{N}$ the symbol $-$ is introduced. Let

$$-\mathbb{N} = \{-x : x \in \mathbb{N}\}.$$

As a set

$$\mathbb{Z} = (\mathbb{N} \cup -\mathbb{N})/\sim$$

where $\sim$ is an equivalence relation identifying 0 with -0. Formally,

$$x \sim y \Leftrightarrow \begin{cases} x = y & \text{if } x, y \in \mathbb{N} \text{ or } x, y \in -\mathbb{N} \\ x = 0, y = -0 & \text{if } x \in \mathbb{N}, y \in -\mathbb{N} \end{cases}.$$

Operations on $\mathbb{Z}$

The usual conventions extending operations from $\mathbb{N}$ to $\mathbb{Z}$ apply. For instance, we declare, for $n \in \mathbb{Z}$,

$$-(-n) = n.$$

Multiplication is extended by

$$(-m) \times n = m \times (-n) = -(m \times n), \qquad (-m) \times (-n) = m \times n.$$

When $m = np$ and $n \neq 0$, integer division is defined by

$$\frac{-m}{n} = \frac{m}{-n} = -p, \qquad \frac{-m}{-n} = p.$$

Operations on $\mathbb{Z}$

To extend addition from $\mathbb{N}$ to $\mathbb{Z}$, recall the trichotomy principle of $\mathbb{N}$:

Theorem (Trichotomy principle of $\mathbb{N}$)

Let $m, n \in \mathbb{N}$. Exactly one of $m < n, m = n, m > n$ is true. If $m < n$ then $m + 1 \leq n$.

Given $m, n \in \mathbb{N}$, define

$$-m + n = n + -m = \begin{cases} x \text{ s.t. } x + m = n & \text{if } m < n \\ 0 & \text{if } m = n \\ -x \text{ s.t. } x + n = m & \text{if } m > n \end{cases}.$$

Also, $-m + (-n) = -(m + n)$.
Subtraction is defined on $\mathbb{Z}$ by $m - n = m + (-n)$.
Define $m \leq n$ by $n - m \in \mathbb{N}$.

The properties of a commutative ring

Definition

A (commutative) ring is a set R together with two operations $+, \times : R^2 \to R$ which satisfy the following properties:

1. $+, \times$ are commutative: $a + b = b + a$, $a \times b = b \times a$
2. $+, \times$ are associative: $a + (b + c) = (a + b) + c$, $(a \times b) \times c = a \times (b \times c)$
3. Add. and mult. identity: There exist elements $0 \neq 1 \in R$ such that, $\forall a \in R$, $0 + a = 1 \times a = a$.
4. Additive inverse: For each $a \in R$ there exists $-a \in R$ such that $a + (-a) = 0$.
5. $\times$ distributes over $+$: $a \times (b + c) = a \times b + a \times c$.

Only additive inverses are missing from $\mathbb{N}$.

Deducing properties of $\mathbb{Z}$ from those of $\mathbb{N}$

Checking the ring properties of $\mathbb{Z}$ from those of $\mathbb{N}$ when addition is involved is a tedious case-by-case check. We verify the distributive property.

The distributive property

Proof that $\times$ distributes over $+$ in $\mathbb{Z}$.

- $(-a) \times (b + c) = -(a \times (b + c))$ and $(-a) \times b + (-a) \times c = -(a \times b + a \times c)$, so suppose $a \in \mathbb{N}$
- Similarly, replacing both b with $-b$ and c with $-c$ flips the sign of both sides of the equation, so assume $b \in \mathbb{N}$.
- If $c \in \mathbb{N}$, apply the distributive property in $\mathbb{N}$, so assume $c \in -\mathbb{N}$

Write $c = -c'$ with $c' \in \mathbb{N}$. If $b < c'$ write $b + x = c'$. Then $a \times b + a \times x = a \times c'$ follows from the distributive property of $\mathbb{N}$, so

$$a \times (b + c) = a \times (-x) = -a \times x = a \times b + a \times c.$$

The case $b > c'$ is similar. If $b = c'$, reduce to the identity

$$a \times 0 = 0,$$

which may be checked by induction.

$\square$

Examples of rings

The ring $\mathbb{Z}[x]$ of integer polynomials in a single variable x. These are expressions of the form

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0 = \sum_{i=0}^{n} a_i x^i, \qquad n \in \mathbb{N},$$

where the coefficients $a_n, ..., a_0$ are integers. The rules for adding and multiplying polynomials are familiar from high-school algebra.

Examples of rings

The ring $\mathbb{Z}[\epsilon]/\epsilon^2$ of integers with an infinitesimal. This set is given by

$$\mathbb{Z}[\epsilon]/\epsilon^2 = \{a + b\epsilon : a, b \in \mathbb{Z}\}.$$

Addition and multiplication of these expressions is the same as for the ring $\mathbb{Z}[\epsilon]$ of polynomials in ϵ, except all terms involving $\epsilon^2, \epsilon^3, \ldots$ are set to 0. More formally, $\mathbb{Z}[\epsilon]/\epsilon^2$ may be expressed as the set $\mathbb{Z}^2$ with rules

$$(a, b)+(a', b') = (a+a', b+b'), \qquad (a, b)\times(a', b') = (a\times a', a\times b'+a'\times b).$$

We think of this ring as performing computation with one degree of accuracy.

Examples of rings

The ring $\mathbb{Z}[\epsilon]/\epsilon^n$ of integers with a degree n infinitesimal. This behaves like $\mathbb{Z}[\epsilon]/\epsilon^2$, except terms in ϵ^j are kept for $j < n$.

We won't check that the any of the above objects are rings, although I encourage you to convince yourself of this fact (you are not responsible for it on homeworks or exams).

The division algorithm

Theorem (The division algorithm)

For each $x \in \mathbb{Z}$ *and* $n \in \mathbb{N} \setminus \{0\}$ *there exists a unique* $q \in \mathbb{Z}$ *and* $r \in \mathbb{N}$, $0 \leq r < n$ *such that* $x = q \times n + r$*.*

q is called the quotient and r the residue. Warning: on many computer implementations of integers, $\frac{x}{n}$ gives the value q, ignoring r.

Proof.

See HW1 #5. (Note: as we didn't introduce $\mathbb{Z}$ until this lecture, full marks for solutions that treat only $x \in \mathbb{N}$.) $\square$

Modular arithmetic

Let $n \in \mathbb{N}$, $n > 1$, and define an equivalence relation on $\mathbb{Z}$ by $a \sim b$ if and only if $n|(b-a)$. This is equivalent to $a = qn + r$, $b = q'n + r$ for the same residue r, $0 \leq r < n$ in the division algorithm. The set $\mathbb{Z}/\sim$ is denoted

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}.$$

(The bars are usually omitted).

Modular arithmetic

$\mathbb{Z}/n\mathbb{Z}$ is given a ring structure by defining

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} \times \overline{b} = \overline{a \times b}.$$

These are well-defined, since if $a_0 \in \overline{a}$, $b_0 \in \overline{b}$, then $a_0 = a + xn$, $b_0 = b + yn$ for some $x, y \in \mathbb{Z}$, whence

$$a_0 + b_0 = a + b + (x+y)n, \qquad a_0 b_0 = ab + (ay + bx + xyn)n$$

differ from $a + b$, ab by a multiple of n.

The additive identity is $\overline{0}$, mult. ident. is $\overline{1}$, and add. inverse of $\overline{x}$ is $\overline{-x}$.

Euclidean algorithm

Let $m, n \in \mathbb{N}$. The greatest common divisor of m, n, denoted $\mathrm{GCD}(m, n)$ is the largest $d \in \mathbb{N}$ such that $d|m$ and $d|n$.

Theorem (Euclidean algorithm)

Let $m > n \in \mathbb{N}$. Euclid's algorithm

Initialize $(a, b) = (m, n)$. While $b \neq 0$:

1. *Apply the division algorithm to write $a = bq + r$*
2. *Replace (a, b) with (b, r) (so $a := b$, $b := r$)*
3. *Repeat*

produces the pair $(\mathrm{GCD}(m, n), 0)$. Moreover, the algorithm can be used to find $x, y \in \mathbb{Z}$ such $xm + yn = \mathrm{GCD}(m, n)$.

Euclidean algorithm

Proof.

- For all $x \in \mathbb{Z}$ and $d \in \mathbb{N}$, if $d|m$ and $d|n$ then $d|m + nx$. Hence $\text{GCD}(m, n) = \text{GCD}(n, m + nx)$.
- Write $m = nq + r$ and choose $x = -q$ to obtain $\text{GCD}(m, n) = \text{GCD}(n, r)$.
- Let $S = \{a + b : (a, b) \text{ is produced by the algorithm}\}$. By the well-ordering principle, S has a least member $a_0 + b_0$ produced by (a_0, b_0).
- When writing $a = qb + r$, $r < b$, so the sum $a + b$ decreases at each step of the algorithm. Hence $a_0 = \text{GCD}(m, n)$, $b_0 = 0$.
- One checks by induction that if (a, b) is produced by the algorithm, then there exist $x, y, z, w \in \mathbb{Z}$ such that $a = xm + yn$, $b = zm + wn$.

$\square$

Primes

A natural number $p > 1$ is *prime* if the only natural numbers which divide p are 1 and p.

Theorem

Let $a, b \in \mathbb{N}$ and let p be a prime. If $p|ab$ then $p|a$ or $p|b$ (or both).

Proof.

Suppose p does not divide a. Then $\mathrm{GCD}(a, p) = 1$. Apply the Euclidean algorithm to find integer x, y such that $xa + yp = 1$. Multiply both sides by b. Thus $xab + ybp = b$. If $p|ab$ then p divides the left hand side, hence $p|b$. $\square$

Prime factorization

Theorem

Every $n \in \mathbb{N}$, $n > 1$ is divisible by a prime.

For a proof, see HW2. In solving this problem it will be helpful to use a variant of induction called 'strong induction'. Suppose that one wishes to prove a statement $p(n)$ for all integers n. In strong induction, one upgrades $p(n)$ to the statement

$$P(n) = \forall m \leq n, p(n).$$

Evidently $p(n)$ is true for all n if and only if $P(n)$ is true for all n, but in making the inductive step, the inductive assumption in $P(n)$ contains more information.

Prime factorization

Theorem (Prime factorization)

Let $n \geq 2$ be a natural number. Then n has a unique representation as $n = \prod_{i=1}^m p_i^{e_i}$ where $p_1, ..., p_m$ are prime, $p_i < p_j$ if $i < j$ and each $e_i \in \mathbb{N} \setminus \{0\}$.

Proof of existence.

Let $P(n)$ be the statement every $1 < k \leq n$ has a representation of the given type.

- Base case: $n = 0, 1$. True because nothing needs to be proved.
- Inductive step: Assume $P(n)$ for some $n \geq 1$. If $n+1$ is prime, then $n+1$ itself is a representation of this type. Otherwise $n+1 = pk$ where p is prime and $1 < k < n+1$. It follows that k has a representation of the given type, and multiplying by p, $n+1$ does also.

$\square$

Prime factorization

Proof of uniqueness.

To prove the uniqueness, let S denote the set of $n \geq 2$ that have two distinct representations of the given type. If S is non-empty, then it has a least element $n > 1$,

$$n = \prod_{i=1}^{m} p_i^{e_i} = \prod_{j=1}^{k} q_j^{f_j}.$$

Since $p_1 | n$, p_1 divides one of $q_1, ..., q_k$ (this requires a proof by induction, which has been omitted), hence is equal to one of $q_1, ..., q_k$. Cancelling this factor of p_1 from both sides obtains a smaller example $\frac{n}{p_1} \in S$, a contradiction. $\square$

Definition of $\mathbb{Q}$

As a set,

$$\mathbb{Q} = \mathbb{Z} \times (\mathbb{N} \setminus \{0\}) / \sim$$

with pairs (a, b) written $\frac{a}{b}$, and with equivalence given by

$$\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad = bc.$$

The operations are familiar:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}$$

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}, \qquad \text{If } c \neq 0\text{: } \frac{a}{b} \Big/ \frac{c}{d} = \frac{ad}{bc}.$$

These operations respect the equivalence relation, since if a and b are scaled by the same $x \in \mathbb{N} \setminus \{0\}$, the same is true of the numerator and denominator on the right hand side.

Definition of $\mathbb{Q}$

In $\mathbb{Q}$, $0 = \frac{0}{1}$ is the additive identity and $1 = \frac{1}{1}$ is the multiplicative identity. The negative of an element $x = \frac{a}{b}$ is $-x = \frac{-a}{b}$. It now follows from the properties of the integers that $\mathbb{Q}$ satisfies the axioms of ring. We check one of these.

Proof that $+$ is associative in $\mathbb{Q}$.

Note that $\frac{a}{d} + \frac{b}{d} = \frac{a+b}{d}$, after cancelling a factor of d from numerator and denominator. Hence, making a common denominator

$$\left(\frac{p_1}{q_1} + \frac{p_2}{q_2}\right) + \frac{p_3}{q_3} = \frac{p_1 q_2 q_3 + q_1 p_2 q_3 + q_1 q_2 p_3}{q_1 q_2 q_3} = \frac{p_1}{q_1} + \left(\frac{p_2}{q_2} + \frac{p_3}{q_3}\right).$$

$\square$

Definition of $\mathbb{Q}$

We identify $\mathbb{Z} \subset \mathbb{Q}$ with the map $f : \mathbb{Z} \to \mathbb{Q}$, $f(x) = \frac{x}{1}$. Note that f is injective and respects the ring structure, that is, $f(a+b) = f(a) + f(b)$, $f(1) = 1$ and $f(ab) = f(a)f(b)$.

Axioms of a field

Definition

A *field* is a commutative ring R in which every $x \neq 0$ has a multiplicative inverse x^{-1} satisfying $xx^{-1} = 1$.

Let $r = \frac{p}{q} \in \mathbb{Q}$. If $p > 0$ then $r^{-1} = \frac{q}{p}$, while if $p < 0$ then $r^{-1} = \frac{-q}{-p}$. This arrangement makes $\mathbb{Q}$ a field.

The field $\mathbb{Z}/p\mathbb{Z}$

Theorem

Let $p > 1$ be a prime. Then $\mathbb{Z}/p\mathbb{Z}$ is a field.

Proof.

Since $\mathbb{Z}/n\mathbb{Z}$ is a ring for any $n \geq 1$, it suffices to check that for $n = p$ a prime that each $\overline{0} \neq \overline{x} \in \mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse. Choose the representative for the class $\overline{x}$ with $0 < x < p$. Since p does not divide x, $\mathrm{GCD}(x, p) = 1$, and thus, by the Euclidean algorithm, there exists $b, y \in \mathbb{Z}$ such that $xy + bp = 1$. It follows that $\overline{xy} = \overline{1}$ so $\overline{y} = \overline{x}^{-1}$. $\square$

Order axioms of fields

Definition

A field F is said to be *ordered* if there exists a set $F^+ \subset F$ of 'positive' elements, which satisfies the following properties.

1. If $x, y \in F^+$ so are $x + y$ and xy.
2. For each $0 \neq x \in F$, either $x \in F^+$ or $-x \in F^+$ but not both.
3. $0 \notin F^+$.

The order relation $<$ is defined on F by $a < b$ if and only if $b - a \in F^+$.

Note that $<$ automatically satisfies the *trichotomy law*: for any $x, y \in F$, exactly one of $x < y$, $x = y$, $y < x$ holds.
Defining $\mathbb{Q}^+ = \left\{\frac{a}{b} \in \mathbb{Q} : a > 0\right\}$ makes $\mathbb{Q}$ an ordered field.

The inverse function in $\mathbb{Z}/p\mathbb{Z}$

HW2 verifies that in an ordered field F, if $x, y \in F^+$ with $x < y$, then $y^{-1} < x^{-1}$.

The field $\mathbb{Z}/p\mathbb{Z}$ cannot be ordered, as $1 = (-1)^2$ is contained in F^+ for any ordered field, and since any element of $\mathbb{Z}/p\mathbb{Z}$ may be reached by adding 1 several times.

In general, the inverse function in $\mathbb{Z}/p\mathbb{Z}$ may appear quite disordered compared to the usual integer ordering. For instance, in $\mathbb{Z}/11\mathbb{Z}$,

$$(1^{-1}, 2^{-1}, ..., 10^{-1}) = (1, 6, 4, 3, 9, 2, 8, 7, 5, 10).$$

$\sqrt{2} \notin \mathbb{Q}$

$\mathbb{Q}$ permits the solution of linear equations $ax = b$ but is unsatisfactory for the solution of some higher degree polynomial equations.

Theorem

The equation $x^2 = 2$ does not have a rational solution.

Proof.

Consider the set A of all pairs of natural numbers (a, b) for which $a, b > 0$ and $a^2 = 2b^2$. If there is a rational solution to $x^2 = 2$, then A is non-empty, hence, by the well-ordering principle, there is a pair (a_0, b_0) which minimizes $a_0 + b_0$. Then a_0 is even, $a_0 = 2a_1$. It follows that $4a_1^2 = 2b_0^2$, so $2a_1^2 = b_0^2$. The pair (b_0, a_1) has a smaller sum, a contradiction. $\square$

Bounds

Definition

Let F be an ordered field and let $S \subset F$ be a non-empty subset. An element $b \in F$ is an *upper bound* (resp. lower bound) for S if $\forall s \in S, s \leq b$ (resp. $s \geq b$).

The least upper bound and greatest lower bound

Definition

An element $b \in F$ is the *least upper bound* for non-empty set $S \subset F$, written

$$b = \sup S,$$

if b is an upper bound for S, and if, for any b' which is an upper bound for S, $b \leq b'$. An element $b \in F$ is the *greatest lower bound* for S, written

$$b = \inf S,$$

if b is a lower bound for S, and if, for any b' a lower bound for S, $b \geq b'$.

Bounds and the least upper bound

Definition

An ordered field F is said to have the least upper bound (l.u.b.) property if any non-empty subset $S \subset F$ which is bounded above has a least upper bound.

Subfields

Definition

Let F_1, F_2 be fields. We say F_1 is a *subfield* of F_2 if there exists an injective map $f : F_1 \to F_2$ which respects the field structure, that is, $f(a+b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$. In this case we identify $a \in F_1$ with $f(a) \in F_2$.

Theorem

Let F_1, F_2 be fields. An injective map $f : F_1 \to F_2$ which respects the field structure satisfies $f(0) = 0$, $f(1) = 1$, and for all $x \in F_1 \setminus \{0\}$, $f(-x) = -f(x)$, and $f(x^{-1}) = f(x)^{-1}$.

See HW2.

Next lecture we construct $\mathbb{R}$ to be an ordered field which contains $\mathbb{Q}$ as a subfield, and which has the l.u.b. property.

Order property of $\mathbb{Q}$

Theorem

Let F be an ordered field and let $f : \mathbb{Q} \to F$ be an injective map which respects the field structure. For all $q \in \mathbb{Q}^+$, $f(q) \in F^+$.

Proof.

Since $f(1) = 1$ and $(-1)^2 = 1$ it follows that $1 \in F^+$. It may be proved by induction that $f(n) \in F^+$ for all $0 < n \in \mathbb{N}$. Now consider $\frac{p}{q} \in \mathbb{Q}^+$. Then $q \cdot \frac{p}{q} = p \in \mathbb{N}$. It follows that $f(q) \cdot f\left(\frac{p}{q}\right) = f(p) \in F^+$. Since $f(q) \in F^+$, it follows that $f\left(\frac{p}{q}\right) \in F^+$. (A positive times a negative is negative, as follows from the definition of F^+.) $\square$

Consequences of the l.u.b. property

Theorem

For every $x \geq 0$, $x \in \mathbb{R}$ *there exists a unique* $y \geq 0$, $y \in \mathbb{R}$ *such that* $y^2 = x$.

Proof.

Note that, if $0 < s < t$ then $0 < s^2 < st < t^2$. Thus, if a solution exists, it is unique.
Let $S = \{y > 0 : y^2 < x\}$. Since

$$(1+x)^2 = 1 + 2x + x^2 > x,$$

$(1+x)$ is an upper bound for S. Note $\left(\frac{x}{1+x}\right)^2 < x$, so S is non-empty.
Set $s = \sup S$. □

Consequences of the l.u.b. property

Proof.

We show that $s^2 = x$, by ruling out $s^2 < x$ and $s^2 > x$.
Suppose $s^2 < x$ and let $\epsilon = \min(\frac{x-s^2}{4s}, s)$. Then $s' = s + \epsilon$ satisfies

$$(s')^2 = s^2 + \epsilon(2s + \epsilon) \leq s^2 + 3s\epsilon < x$$

so $s' \in S$, but $s' > s$, a contradiction.
Suppose instead that $s^2 > x$. Let $\epsilon = \frac{s^2-x}{2s}$ and $s' = s - \epsilon$. Then

$$(s')^2 = s^2 - 2\epsilon s + \epsilon^2 > s^2 - 2\epsilon s = x.$$

It follows that for any $y \in S$, $y < s'$, so $s' < s$ is a smaller upper bound for S, a contradiction.

$\square$

Consequences of the l.u.b. property

Theorem

The set $\mathbb{N}$ is unbounded above in $\mathbb{R}$.

Proof.

Suppose bounded. Let $s = \sup \mathbb{N}$. Since $s - \frac{1}{2}$ is not an upper bound, there exists $n \in \mathbb{N}$ with $n \geq s - \frac{1}{2}$. It follows that $n + 1 > s$, a contradiction. $\square$

Consequences of the l.u.b. property

Theorem

For every real x there exists $n \in \mathbb{Z}$ with $n > x$. In fact, there exists $n \in \mathbb{Z}$ with $n \leq x < n + 1$.

Proof.

- Assume first that $x > 0$. The set $S = \{n \in \mathbb{N} : n > x\}$ is non-empty, since otherwise x would be an upper bound for $\mathbb{N}$. By the well-ordered property of $\mathbb{N}$, S has a least element m. Then $n = m - 1$ satisfies $n \leq x < n + 1$.
- If $x < 0$, choose $M \in \mathbb{N}$ with $M > -x$. Find m such that $m \leq M + x < m + 1$. Then setting $n = m - M$ one has $n \leq x < n + 1$.

$\square$

Consequences of the l.u.b. property

Theorem

If $x > 0$ and y is an arbitrary real number, then there exists $n \in \mathbb{N}$ such that $nx > y$.

Proof.

Choose any $n > \frac{y}{x}$. $\square$

Food for thought

Write down a field with 4 elements.