MATH 340 review notes

jryzkns

1 Axiomatic Approach to $\mathbb{N}$

Definition: $\mathbb{N}$ is a set with 3 axioms (sometimes referred to as the "Peano Axioms"):

1. $1 \in \mathbb{N}$
2. For every $a \in \mathbb{N}$, there is an element called the *successor* of a, written as $succ(a) = a + 1 \in \mathbb{N}$
3. Every element $a \in \mathbb{N}$ arises in this manner:

$$\mathbb{N} = \{succ^k(1) \mid k \geq 0\}$$

2 Mathematical Induction

Principle of Mathematical Induction:
Suppose $X \subseteq \mathbb{N}$ and:

1. $1 \in X$
2. $a \in X \Rightarrow a + 1 \in X$

Then $X = \mathbb{N}$.
This is taken as an axiom and cannot be proven from the 3 axioms presented in section 1.
Strong Induction:
Suppose $X \subseteq \mathbb{N}$ satusfies the properties

1. $1 \in X$
2. $\forall i \in [1, n] \;\; i \in X \Rightarrow n + 1 \in X$

This variant of induction is logically equivalent to the simple form of induction, but in a proof it may be desirable to refer to more than 1 case that is taken to be true, in which case a strong induction is preferred.
The Well-Ordering Principle (WP):
Every non-empty subset $Y \subseteq \mathbb{N}$ has a minimal element.
We can use WP to prove the Principle of Induction:
Suppose $X \subseteq \mathbb{N}$ has the properties $1 \in X$ and $k \in X \Rightarrow k + 1 \in X$, WTS $X \in \mathbb{N}$. Suppose $Y = \{n \in \mathbb{N} \mid n \notin X\}$, then $X = \mathbb{N} \Leftrightarrow Y = \varnothing$
We proceed to show that $Y = \varnothing$ by contradiction, assuming $Y \neq \varnothing$. By WP, Y has a minimum element $n^* \in Y$. As $1 \notin Y$ (because $1 \in X$), $n^* > 1$ so $n^* - 1 \in \mathbb{N}$ and $n^* - 1 \notin Y$ because n^* is the minimal element of Y. Therfore $n^* - 1 \in X$, but then $succ(n^* - 1) = n^* - 1 + 1 = n^* \in X$ by the inductive hypothesis. As $n^* \in Y$, we have come to a contradiction, and therefore $Y = \varnothing$ and $X = \mathbb{N}$.
Note: WP is false for other sets of numbers. For example, there is no minimal element in $\mathbb{R}^+$ as $\forall x \in \mathbb{R}^+ \;\; \frac{1}{2}x < x$.

3 Operations on $\mathbb{N}, \mathbb{Z}$

Multiplication on $\mathbb{N}$:
Inductively defined with $1 \cdot a := a$ as the base case. If $n \cdot a$ is defined, then $(n + 1) \cdot a := n \cdot a + a$.
The Peano Axioms imply the following properties:

- Commutativity: $ab = ba$
- Associativity: $a(bc) = (ab)c$
- Distribution over Addition: $a(b + c) = ab + ac$

Defining $\mathbb{Z}$ from $\mathbb{N}$
Suppose we want to solve an equation like $x + 5 = 2$ in $\mathbb{N}$, there are no solutions, because $x = 2 - 5 \notin \mathbb{N}$. Therefore, we need to invent the notion of negative numbers.
To do this, we can say that $\mathbb{Z}$ is the set $\mathbb{N} \times \mathbb{N} = \{(a, b) \mid a, b \in \mathbb{N}\}$ with an equivalence relation $(a, b) = (a + c, b + c)$ for any $a, b, c \in \mathbb{N}$. The ordered tuple (a, b) represents $a - b$. We can see that $(a + c) - (b + c) = a - b$. More concretely, consider $(5, 0) = (6, 1) = (500, 495)$ and $5 - 0 = 6 - 1 = 500 - 495$. A negative number $-a$ could then be represented as $(0, a)$.
Induction in $\mathbb{Z}$
WP does not apply to $\mathbb{Z}$, so in practice we either treat +ive and -ive numbers separately, or we go by the absolute value of the numbers.

4 The Division Theorem in $\mathbb{Z}$

Theorem:
Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then there exists unique $q \in \mathbb{Z}, r \in (0, b)$ such that $a = qb + r$.
Proof: We proceed in two steps, showing existence then uniqueness.
Existence: We have $a \in \mathbb{Z}, b \in \mathbb{N}$, we define

$$X = \{n \in \mathbb{N} \cup \{0\} \mid n = a - qb\}$$

For some integer q. X is nonempty as $a - qb \geq 0$ by choice of q. If $a > 0$, we pick $q = 0$. If $a \leq 0$, we pick $q = a$. By WP, X has a minimal element that we will call r; $r = a - qb$ for some $q \in \mathbb{Z}$. Since $r \in \mathbb{N} \cup \{0\}$, $r \geq 0$. r also satisfies $r < b$. If $r \geq b$, then $r - b \in X$ as $r - b = (a - qb) - b = a - (q + 1)b$. This contradicts minimality of r. Rearranging $r = a - qb$ we get $a = qb + r$.
Uniqueness: Suppose we have (q_1, r_1) and (q_2, r_2) both satisfying the theorem, WTS $q_1 = q_2$ and $r_1 = r_2$.

We have $a = q_1 b + r_1 = q_2 b + r_2$ with $r_1, r_2 \in (0, b)$. If we collect the terms with b on one side, we have $(q_1 - q_2)b = r_2 - r_1$. So, $r_2 - r_1$ is a multiple of b. Given the constraint $r_1, r_2 \in (0, b)$, we can see that $r_2 - r_1 \in [-(b-1), (b-1)]$. Therefore it is only possible that $r_2 - r_1 = 0$ is a multiple a multiple of b. Therefore $r_2 = r_1$ and $(q_1 - q_2)b = 0 \Rightarrow q_1 = q_2$.

4.1 What if $b < 0$?

$a = qb + r \Leftrightarrow a = (-q)(-b) + r$. The theorem still works, but $0 \geq r \geq |b|$ needs to be guaranteed.

5 Divisibility in $\mathbb{Z}$

Definition: Let $d, a \in \mathbb{Z}$, we say that d divides a, written as $d|a$, if $a = qd$ for some $q \in \mathbb{Z}$.
Equivalently: d is a *divisor* of a, a is a *multiple* of d, or a is *divisible* by d.
Some Facts:

- $\forall d \in \mathbb{Z}\ \ d|0$ but $0 \nmid a$ unless $a = 0$.
- If d divides $a \neq 0$ then $|d| \leq |a|$. In particular, the set of divisors of a non-zero integer is finite.
- $d|a \Leftrightarrow |d| \mid |a|$

6 GCD in $\mathbb{Z}$

Definition: Let $a, b \in \mathbb{Z}$, not both 0. The *greatest common divisor* of a and b, $\gcd(a, b)$ is the greatest $d \in \mathbb{Z}$ such that $d|a$ and $d|b$.
Lemmas:

- $(d|a \wedge d|b) \rightarrow d|(a - b)$
- $(d|(a - b) \wedge d|b) \rightarrow d|a$

Note that these lemmas mean that if d is a common divisor of (a, b) then it is equivalent to d is a common divisor of $(b, a - b)$; $\gcd(a, b) = gcd(b, a - b)$.

7 Bezout's Identity in $\mathbb{Z}$

Theorem:
Let $g = \gcd(a, b)$. Then $g = ax + by$ for some $x, y \in \mathbb{Z}$.
Proof: Suppose we have two sets:

$$
\begin{aligned}
D &= \{d \in \mathbb{Z} \mid d|a \wedge d|b\} \\
I &= \{ax + by \mid x, y \in \mathbb{Z}\}
\end{aligned}
$$

D is the set of all common divisors between a, b and I is the set of all integer combinations of a, b.
From this we make claim (1): If $d \in D$ and $n \in I$, then $d|n$. In particular, if $n \neq 0$, $|d| \leq |n|$.
Since $d \in D$, we have $a = q_1 d$ and $b = q_2 d$ for some $q_1, q_2 \in \mathbb{Z}$. Similarly, since $n \in I$, we have $n = ax + by$ for some $x, y \in \mathbb{Z}$. We can see that $n = ax + by = q_1 dx + q_2 dy = d(q_1 x + q_2 y) \Rightarrow d|n$.
Suppose now we look at $I \cap \mathbb{N}$, the integer multiples of a, b that are natural numbers, we let $n^* = \min(I \cap \mathbb{N}) = ax^* + by^*$.
We proceed to make claim (2) that $n^*|a$ and $n^*|a$ (i.e. $n^* \in D$).
Suppose $n^* \nmid a$, we divide a by n^* to get $a = qn^* + r$, $r \in (0, n^*)$. By definition of n^*, we see that

$$
\begin{aligned}
r &= a - qn^* \\
&= a - q(ax^* + by^*) \\
&= a - qax^* + qby^* \\
&= a(1 - qx^*) + b(qy^*)
\end{aligned}
$$

This means that $n^* \in I$ and that contradicts the minimality of n^* as $r \in (0, n^*)$.
Finally, we make our last claim (3): $n^* = \max(D) = \gcd(a, b)$. By claim (2), n^* is a common divisor of a, b. If $d \in D$ is any other common divisor, then $d \leq n^*$ by claim (1). We can see that $d \leq |d| \leq |n^*| = n^*$.
Therefore, we have two interpretations of $\gcd(a, b)$:

- $\gcd(a, b) = \max(D)$
  maximal element in set of common divisors
- $\gcd(a, b) = \min(I \cap \mathbb{N})$
  smallest positive integer combination of a, b.

8 Euclidean Algorithm

Theorem:
If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.
Proof:
It is given that $\gcd(a, b) = \gcd(a - b, b)$. As $r = a - qb$, we can consider applying the $a - b$ operation q times: $\gcd(a, b) = \gcd(b, a - qb) = \gcd(b, r)$.
Algorithm
Given: (a, b) with $a > b > 0$ and repeatedly apply division theorem on (a, b). After each division, we replace a with b and b with the remainder of the division:

$$
\begin{aligned}
(a, b) &\quad a = q_1 b + r_1 \\
(b, r_1) &\quad b = q_2 r_1 + r_2 \\
(r_1, r_2) &\quad r_1 = q_3 r_2 + r_3 \\
\vdots &\quad \vdots \\
(r_{k-2}, r_{k-1}) &\quad r_{k-2} = q_k r_{k-1} + r_k \\
(r_{k-1}, r_k) &\quad r_{k-1} = q_{k+1} r_k + 0 \\
(r_k, 0) &
\end{aligned}
$$

The algorithm stops when we reach a point where the second value in the tuple is 0, in which case $\gcd(a, b) = r_k$. This algorithm is guaranteed to terminate as each of the r_i up to terminating r_k are strictly decreasing natural numbers. By WP there is a minimal element to which this procedure will terminate on.