# MATH 110AH – FALL 2021

Pablo S. Ocal

based on "Lectures on Abstract Algebra"

by Richard S. Elman.

## Section 2: Well-ordering and induction.

**The well-ordering principle:** Let $\emptyset \neq S \subseteq \mathbb{Z}^+$. Then $S$ contains a least element: there exists $a \in S$ such that $a \leq x$ for all $x \in S$.

**Proposition:** Let $\emptyset \neq T \subseteq \mathbb{Z}$. Suppose that there is an $N \in \mathbb{Z}$ such that $N \leq x$ for all $x \in T$ (i.e. $T$ is bounded from below). Then $T$ contains a least element.

Similarly, if $T$ is bounded from above, it contains a largest element.

**Proposition:** There is no integer $N$ satisfying $0 < N < 1$.

**Proof:** Let $S = \{n \in \mathbb{Z} \mid 0 < n < 1\}$. If $\emptyset \neq S$ then there exists a least element $N \in S$. Now $0 < N < 1$ implies $0 < N^2 < N < 1$ and since $N \in \mathbb{Z}$ then $N^2 \in \mathbb{Z}$, so $N^2 \in S$ contradicting minimality. $\square$.

**Proposition:** Let $S \subseteq \mathbb{Z}^+$ and $1 \in S$. Suppose that if $n \in S$, then

$n+1 \in S$. Then $S = \mathbb{Z}^+$.

Proof: Let $T = \{n \in \mathbb{Z}^+ \mid n \notin S\}$. If $T = \emptyset$ then $S = \mathbb{Z}^+$. If $T \neq \emptyset$ then there exists a least positive element $n \in T$. Then $n \notin S$ and $n-1 \notin T$. Since $1 \notin T$ then $n > 1$ and $n-1 \in \mathbb{Z}^+$. Then $n-1 \in S$, but by hypothesis $n \in S$, contradiction. □.

Theorem: (Induction) For each $n \in \mathbb{Z}^+$, let $P(n)$ be a true or false statement. Suppose we know that $P(1)$ is true, and that if $P(n)$ is true then $P(n+1)$ is true. Then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Theorem: (Induction) For each $n \in \mathbb{Z}^+$, let $P(n)$ be a true or false statement. Suppose that if $P(m)$ is true for all $m < n$ positive integers, then $P(n)$ is true. Then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Proposition: The product of any $n \geq 1$ consecutive positive integers is divisible by $n!$, i.e. for all $m, n \in \mathbb{Z}^+$ we have: $\frac{m \cdot (m+1) \cdots (m+n-1)}{n \cdot (n-1) \cdots 2 \cdot 1} \in \mathbb{Z}^+$.

Corollary: For every $n \in \mathbb{Z}^+$, there exist $n$ consecutive composite positive integers.

Corollary: Let $p > 1$ be a prime. Then $p$ divides $\binom{p}{n}$ for all $1 \leq n \leq p-1$.

## Section 3: The greatest integer function.

Another way of showing that the binomial coefficients are integers.

**Definition:** The greatest integer function: $[\,]: \mathbb{R} \longrightarrow \mathbb{Z}$

gives $[x]$ the greatest integer $[x] \leq x$ for $x \in \mathbb{R}$.

**Proposition:** For $x \in \mathbb{R}$ and $m, n \in \mathbb{Z}^+$, the following hold:

1) $[x] \leq x < [x]+1$.

2) $[x+m] = [x] + m$.

3) $\left[\frac{x}{m}\right] = \left[\frac{[x]}{m}\right]$.

4) $[x]+[y] \leq [x+y] \leq [x]+[y]+1$.

5) $\left[\frac{n}{m}\right]$ is the number of integers among $1, \ldots, n$ that are divisible by $m$.

**Proof:** (1), (2), (3), (4) are straightforward.

5) Let $m, 2m, \ldots, jm$ all the positive integers below $n$ and divisible by $m$. Now $jm \leq n < (j+1)m$ so $j \leq \frac{n}{m} < j+1$ so $\left[\frac{n}{m}\right] = j$. $\square$.

**Theorem:** Let $n \in \mathbb{Z}^+$ and $p > 1$ a prime. Suppose that $p^e \mid n!$ but

$$p^{e+1} \nmid n! \text{ then } e = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$$

$p \nmid n!$. Then: $e = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor$.

Corollary: Suppose that $a_1, \dots, a_r \in \mathbb{Z}^+$ with $a_1 + \cdots + a_r = n$. Then the multinomial coefficient $\frac{n!}{a_1! \cdots a_r!} \in \mathbb{Z}^+$.

## Section 4: Division and the greatest common divisor.

Proposition: Let $r, n, m \in \mathbb{Z}$, the following hold:

1) If $r \mid m$ and $r \mid n$ then $r \mid am + bn$ for all $a, b \in \mathbb{Z}$.

2) If $r \mid n$ then $r \mid mn$.

3) If $r \mid n$ and $n \neq 0$ then $|n| \geq |r| \geq r$.

4) If $m \mid n$ and $n \mid m$ then $n = \pm m$.

5) If $mn = 0$ then $m = 0$ or $n = 0$.

6) If $mr = nr$ then $m = n$ or $r = 0$.

Theorem: (Division Algorithm) Let $n \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. Then there exist unique $q, r \in \mathbb{Z}$ satisfying $n = qm + r$ and $0 \leq r < m$.

Proof: We need to show existence and uniqueness.

Uniqueness: Let $(q, r)$ and $(q', r')$ satisfy the conclusion.

We have $qm + r = n = q'm + r'$ and $0 \leq r < m$, $0 \leq r' < m$.

WLOG suppose $r \leq r'$, then $0 \leq r' - r = (q - q')m$. If $q = q'$ then $r' - r = 0$ and we are done. If $q \neq q'$ then $r' - r > 0$ and $m \mid r' - r$. Thus $m \leq r' - r < r' < m$, a contradiction.

Existence: If $n > 0$, let $S = \{ s \in \mathbb{Z}^+ \mid sm > n \} \subseteq \mathbb{Z}^+$. Since $m > 0$ we have $m \geq 1$ so $(n+1)m = mn + m \geq n + m > n$ so $n+1 \in S \neq \emptyset$. There exists a least integer $q+1 \in S$, so $qm \leq n$.

Now $qm \leq n < (q+1)n$, choose $r = n - qm \geq 0$, we then have:

$$0 \leq r = n - qm < (q+1)m - qm = m.$$

If $n < 0$, there exist $q', r' \in \mathbb{Z}$ with $|n| = q'm + r'$ and $0 \leq r' < m$. If $r' = 0$ then $q = -q'$ and $r = 0$ work. If $r' \neq 0$ then $q = -q' - 1$ and $r = m - r'$ work. □.

Definition: Let $n, m \in \mathbb{Z}$ at least one non-zero. A $d \in \mathbb{Z}$ is called a greatest common divisor if it satisfies the following:

i) $d > 0$,

ii) $d \mid m$ and $d \mid n$,

iii) If $e \in \mathbb{Z}$ satisfies $e \mid m$ and $e \mid n$, then $e \mid d$.

If $\gcd(u,m)=1$ we say that they are relatively prime.

**Theorem:** Let $m, u \in \mathbb{Z}$ with $u \neq 0$. Then $\gcd(m,u)$ exists and is unique.

**Theorem:** (Euclidean Algorithm) Let $a, b \in \mathbb{Z}^+$ with $b \nmid a$. Then there exists $k \in \mathbb{Z}^+$ and equations:

$$a = bq_1 + r_1, \quad b = r_1 q_2 + r_2, \quad \cdots, \quad r_{k-2} = r_{k-1} q_k + r_k, \quad r_{k-1} = r_k q_{k+1}$$

with: $0 < r_1 < b, \quad 0 < r_2 < r_1, \quad \cdots, \quad 0 < r_k < r_{k-1}$

for $q_1, \cdots, q_{k+1}, r_1, \cdots, r_k \in \mathbb{Z}$.

**Theorem:** (General Euclid's Lemma) Let $a, b \in \mathbb{Z}$ relatively prime, $a \neq 0$. If $a \mid bc$ for some $c \in \mathbb{Z}$, then $a \mid c$.

**Corollary:** If $p > 1$ prime satisfies $p \mid a_1 \cdots a_r$ with $a_1, \cdots, a_r \in \mathbb{Z}$, then $p \mid a_i$ for some $1 \leq i \leq r$.

**Corollary:** Let $p > 1$ be a prime. Then $p$ divides $\binom{p}{n}$ for all $1 \leq n \leq p-1$.

**Proof:** We know that $n! \mid p(p-1)\cdots(p-n+1)$ since these are $n$ consecutive positive integers. If $1 < s < p$, then $\gcd(s,p) = 1$, so $\gcd(n!, p) = 1$, so by Euclid's Lemma $n! \mid (p-1)\cdots(p-n+1)$.

Hence $p \cdot n! \mid p(p-1)\cdots(p-n+1)$, so $p \mid \frac{p(p-1)\cdots(p-n+1)}{n!}$. $\square$.

**Proposition:** Let $p \in \mathbb{Z}$, $|p|>1$. Then $p$ is prime if and only if whenever $p \mid ab$ with $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.

**Theorem:** (Fundamental Theorem of Arithmetic) Let $n \in \mathbb{Z}$, $n>1$. Then there exist unique primes $1 < p_1 < \cdots < p_r$ and $e_1, \ldots, e_r \in \mathbb{Z}$ such that $n = p_1^{e_1} \cdots p_r^{e_r}$.

**Proof:** We need to show existence and uniqueness.

**Existence:** Let $S = \{ n \in \mathbb{Z}^+ \mid n>1$ and it is not a product of primes$\}$. If $S = \emptyset$, we are done. Suppose $S \neq \emptyset$, then there exists a minimal $n \in S$. Since $S$ does not contain any primes, $n$ is not a prime. Hence there exist $n_1, n_2 \in \mathbb{Z}^+$ such that $n = n_1 \cdot n_2$, $1 < n_1$, and $1 < n_2$. By minimality of $n$ we have $n_1, n_2 \notin S$, so $n_1$ and $n_2$ are product of primes, so $n = n_1 \cdot n_2$ is a product of primes, contradiction.

**Uniqueness:** Suppose $p_1^{e_1} \cdots p_r^{e_r} = n = q_1^{f_1} \cdots q_s^{f_s}$ with $1 < p_1 < \cdots < p_r$ and $1 < q_1 < \cdots < q_s$ primes and $e_1, \ldots, e_r, f_1, \ldots, f_s \in \mathbb{Z}^+$. WLOG $p_1 \leq q_1$,

since $p_1 | n$ by Euclid's Lemma $p_1 | q_i$, but $p_1 \leq q_i$ and both are prime so $i=1$ and $p_1 = q_1$. Dividing by $p_1 = q_1$, we obtain $p_1^{e_1-1} \cdots p_r^{e_r} = n = q_1^{f_1-1} \cdots q_s^{f_s}$. Using induction, we are done. □.

## Section 5: Equivalence relations.

**Definition:** A relation on two sets $A$ and $B$ is a subset $R \subseteq A \times B$.

We write $aRb$ if $(a,b) \in R$.

**Example:** A function $f: A \longrightarrow B$ gives a relation $R = \{(a, f(a)) \mid a \in A\}$.

**Definition:** A relation $R$ on $A$ is called an equivalence relation if:

1) Reflexivity: $aRa$

2) Symmetry: if $aRb$ then $bRa$

3) Transitivity: if $aRb$ and $bRc$ then $aRc$ for all $a, b, c \in A$.

We denote an equivalence relation by $\sim$.

**Examples:**

1. Any set $A$ under equality: for $a, b \in A$ then $a \sim b$ if $a = b$.

2. Triangles in $\mathbb{R}^2$ under congruence (one can be transformed into the other by an isometry, i.e. a composition of translations, rotations,

and reflections).

3. $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ with $(a,b) \sim (c,d)$ if $ad = bc$ in $\mathbb{Z}$.

4. $\mathbb{Z}$ under equivalence modulo 2: $m \sim n$ if $m - n$ is even.

5. Let $R \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, set:

$M_n(R) := \{n \times n$ matrices with entries in $R\}$.

$A \sim B$ if there is $C$ invertible with $A = CBC^{-1}$.

This equivalence relation is called <u>similarity of matrices</u>.

6. Let $R$ be a ring, set:

$R^{m \times n} := \{m \times n$ matrices with entries in $R\}$.

$A \sim B$ if there is $C \in M_n(R)$ and $D \in M_n(R)$ invertible

with $A = CBD$.

This equivalence relation is called <u>equivalence of matrices</u>.

7. Let $R$ be a ring. On $M_n(R)$ set: (transpose)

$A \sim B$ if there is $C$ invertible with $A = CBC^t$.

8. On $M_n(\mathbb{C})$ set: (adjoint)

$A \sim_u B$ if there is $C$ invertible with $A = CBC^*$.

**Definition:** Let $\sim$ be an equivalence relation on $A$. Let $a \in A$, the set:

$\bar{a} = [a] = [a]_\sim := \{ b \in A \mid a \sim b \}$ is called the equivalence class of $a$ relative to $\sim$. We call $\bar{A} = A/\sim := \{ \bar{a} \mid a \in A \}$ the set of equivalence classes of $\sim$ on $A$. The map:

$$\begin{aligned} - : A &\longrightarrow \bar{A} \\ a &\longmapsto \bar{a} \end{aligned}$$

is called the natural or canonical surjection.

**Example:**

1. $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ with $(a,b) \sim (c,d)$ if $ad = bc$ in $\mathbb{Z}$. Then:

$$\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / \sim \quad \text{and} \quad \overline{(a,b)} = \frac{a}{b}.$$

2. $\mathbb{Z}$ under equivalence modulo 2: $m \sim n$ if $m - n$ is even. Then:

$$\bar{0} = \{ \text{all even integers} \} = \overline{2n} \text{ for all } n \in \mathbb{Z}.$$

$$\bar{1} = \{ \text{all odd integers} \} = \overline{2n+1} \text{ for all } n \in \mathbb{Z}.$$

We write $\overline{\mathbb{Z}} = \frac{\mathbb{Z}}{2\mathbb{Z}} = \{\bar{0}, \bar{1}\}$.

**Definition:** Let $A_i, i \in I$ be sets. Their union is the set:

$$\bigcup_{i \in I} A_i := \{ x \mid \exists i \in I \text{ with } x \in A_i \}.$$

Their intersection is the set:

$$\bigcap_{i\in I} A_i := \{x \mid x\in A_i \text{ for all } i\in I\}.$$

We call $I$ an indexing set. If $A_i\cap A_j=\emptyset$ for all $i,j\in I$, $i\neq j$, we call this union disjoint and denote it $\bigvee_{i\in I} A_i$ or $\coprod_{i\in I} A_i$.

Proposition: Let $\sim$ be an equivalence relation on $A$. Then $A=\bigvee_{\bar{a}\in\bar{A}} \bar{a}$. In particular if $a,b\in A$ then either $\bar{a}=\bar{b}$ or $\bar{a}\cap\bar{b}=0$. Hence $\bar{a}=\bar{b}$ if and only if $a\sim b$.

Proof: Note that if $a\in A$ then $a\in\bar{a}\in\bar{A}$ so $a\in\bigcup_{\bar{a}\in A}\bar{a}$ so $A\subseteq\bigcup_{\bar{a}\in\bar{A}}\bar{a}$.

If $b\in\bigcup_{\bar{a}\in\bar{A}}\bar{a}$ then $b\in\bar{a}$ for some $\bar{a}\in\bar{A}$, so $b\in A$ so $\bigcup_{\bar{a}\in\bar{A}}\bar{a}\subseteq A$.

Suppose $a,b\in A$ and $\emptyset\neq\bar{a}\cap\bar{b}\ni c$. Then $a\sim c$ and $b\sim c$, so $c\sim b$, so $a\sim b$, so $a\in\bar{b}$. If $d\in\bar{a}$ then $a\sim d$ so $d\sim a$, so $d\sim b$, so $d\in\bar{b}$, whence $\bar{a}\subseteq\bar{b}$. Similarly $\bar{b}\subseteq\bar{a}$, so $\bar{a}=\bar{b}$. □.

Definition: Let $\sim$ be an equivalence relation on $A$. An element $x\in\bar{a}$, $a\in A$, is called a representative of $\bar{a}$. A system of representatives for $A$ relative to $\sim$ is a set $S$ containing exactly one element from each equivalence class.

Remark: If $S$ is a system of representatives for $A$ relative to $\sim$, then:

$$A=\bigvee_{\bar{x}}.$$

$x \in S$

In particular, if $|A| < \infty$ then: $|A| = \sum_{x \in S} 1 \times 1$. This is sometimes called the Mantra of Equivalence Relations.

## Section 6: Modular arithmetic.