1.1.5 Equivalence relations

Consider a relation $\sim$ on a set $X$ as in ch. 1 §1.3 def. 1, but with the properties

i) $x \sim x \quad \forall x \in X$ (reflexivity)

ii) $x \sim y \Rightarrow y \sim x \quad \forall x, y \in X$ (symmetry)

iii) $(x \sim y \land y \sim z) \Rightarrow x \sim z$ (transitivity)

Such a relation is called an equivalence relation. Which of the following are equivalence relations?

a) $n$ divides $m$ on $\mathbb{N}$.

b) $x \leq y$ on $\mathbb{R}$.

c) $g$ is perpendicular to $h$ on the set of straight lines $\{g, h, \ldots\}$ in the cartesian plane.

d) $a$ equals $b$ modulo $n$ on $\mathbb{Z}$, with $n \in \mathbb{N}$ fixed.

*hint*: “$a$ equals $b$ modulo $n$”, or $a = b \mod(n)$, with $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, is defined to be true if $a - b$ is divisible on $\mathbb{Z}$ by $n$; i.e., if $(a - b)/n \in \mathbb{Z}$.

(3 points)

1.1.6 Bounds for $n!$

Prove by mathematical induction that

$$\frac{n^n}{3^n} < n! < \frac{n^n}{2^n} \quad \forall n \geq 6$$

*hint*: $(1 + 1/n)^n$ is a monotonically increasing function of $n$ that approaches Euler’s number $e$ for $n \to \infty$.

(4 points)

1.1.7 All ducks are the same color

Find the flaw in the “proof” of the following

*proposition*: All ducks are the same color.

*proof*: $n = 1$: There is only one duck, so there is only one color.

$n = n$: The set of ducks is one-to-one correspondent to $\{1, 2, \ldots, m\}$, and we assume that all $m$ ducks are the same color.

$n = m + 1$: Now we have $\{1, 2, \ldots, m, m + 1\}$. Consider the subsets $\{1, 2, \ldots, m\}$ and $\{2, \ldots, m, m + 1\}$. Each of these represent sets of $m$ ducks, which are all the same color by the induction assumption. But this means that ducks #2 through $m$ are all the same color, and ducks #1 and $m + 1$ are the same color as, e.g., duck #2, and hence all ducks are the same color.

*remark*: This demonstration of the pitfalls of inductive reasoning is due to George Pólya (1888 - 1985), who used horses instead of ducks.

(2 points)
1.2.1 Pauli group

The Pauli matrices are complex $2 \times 2$ matrices defined as

\[
\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},
\]

Now consider the set $P_1$ that consists of the Pauli matrices and their products with the factors $-1$ and $\pm i$:

\[
P_1 = \{ \pm \sigma_0, \pm i\sigma_0, \pm \sigma_1, \pm i\sigma_1, \pm \sigma_2, \pm i\sigma_2, \pm \sigma_3, \pm i\sigma_3 \}
\]

Show that this set of 16 elements forms a (nonabelian) group under matrix multiplication called the Pauli group. It plays an important role in quantum information theory.

(3 points)
1.1.5) a) No, since it is not symmetric. E.g., $2 \approx 4 \text{ but } 4 \not\approx 2$.

b) No, since it is not symmetric. E.g., $2 \leq 4 \text{ but } 4 \not\leq 2$.

c) No, since it is not reflexive: No line is perpendicular to itself.

d) Yes.

Proof:

(i) $a - a = 0$ is divisible by $m$ \implies $a = a \mod (m)$

(ii) Let $a = b \mod (m) \Rightarrow \exists \lambda \in \mathbb{Z}; a - b = \lambda m$

$\Rightarrow b - a = (-\lambda)m \Rightarrow b - a$ is divisible by $m$

$\Rightarrow b = a \mod (m)$

(iii) Let $a - b \mod (m) \text{ and } b - c \mod (m)$

$\Rightarrow \exists \lambda, \kappa \in \mathbb{Z}; a - b = \lambda m \text{ and } b - c = \kappa m$

$\Rightarrow a - c = (a - b) + (b - c) = \lambda m + \kappa m = (\lambda + \kappa)m$

$\Rightarrow a - c \mod (m)$

$\Rightarrow a = b \mod (m)$ is an equivalence relation on $\mathbb{Z}$. 

1.1. 6) First prove \( n^5 / 2^n < n! \) if \( n \geq 6 \)

\( n = 6 \):
\[ 6^6 / 2^6 = 2^6 = 64 < 720 = 6! \]

Assume \( m^m / 2^m < m! \)

Then
\[
\frac{(m+1)^{m+1}}{2^{m+1}} = \frac{m^m}{2^m} \left( 1 + \frac{1}{m} \right)^m < \frac{m^m}{2^m} \frac{e}{2} (m+1)
\]
\[< \frac{m^m}{2^m} (m+1) < m! (m+1) = (m+1)!\]

Now prove \( n^5 / 2^n > n! \) if \( n \geq 6 \)

\( n = 6 \):
\[ 6^6 / 2^6 = 2^6 = 729 > 720 = 6! \]

Assume \( m^m / 2^m > m! \)

Then
\[
\frac{(m+1)^{m+1}}{2^{m+1}} = \frac{m^m}{2^m} \left( 1 + \frac{1}{m} \right)^m \geq \frac{m^m}{2^m} \frac{2}{2} (m+1) > m! (m+1) = (m+1)!\]

\[\Rightarrow \frac{n^5}{2^5} < n! < \frac{n^5}{2^5} \text{ if } n \geq 6 \]
1.1.7.) The problem this will \( n = 2 \).

The inductive step from \( n = m \) to \( n = m + 1 \) relies on the fact that the subsets \( \{1, 2, \ldots, m\} \) and \( \{1, 3, \ldots, m+1\} \) have common chants. But for \( n = 2 \), \( m = 1 \), both sets are \( \{1\} \) and \( \{2\} \), which have no common chant!

In order for the proof to be valid, one must prove that any two subsets have the same color, which is not possible.
1.2.1. The Pauli matrices obey:

\[
\begin{array}{|c|c|c|c|}
\hline
\sigma_0 & \sigma_1 & \sigma_2 & \sigma_3 \\
\hline
\sigma_0 & \sigma_0 & \sigma_1 & \sigma_2 \\
\sigma_1 & \sigma_1 & -\sigma_0 & \sigma_3 \\
\sigma_2 & \sigma_2 & \sigma_3 & -\sigma_0 \\
\sigma_3 & \sigma_3 & -\sigma_2 & \sigma_1 \\
\hline
\end{array}
\]

i.e., \( \sigma_0 \) is real, while \( \sigma_1 \) or \( \sigma_2 \) times \( \iota \).

Next write \( P_3 \):

\[
\begin{array}{|c|c|c|c|c|c|c|c|c|c|}
\hline
\sigma_0 & \sigma_0 & \sigma_0 & \sigma_0 & \sigma_0 & \sigma_0 & \sigma_0 & \sigma_0 & \sigma_0 & \sigma_0 \\
\hline
\sigma_1 & \sigma_1 & \sigma_1 & \sigma_1 & \sigma_1 & \sigma_1 & \sigma_1 & \sigma_1 & \sigma_1 & \sigma_1 \\
\hline
\sigma_2 & \sigma_2 & \sigma_2 & \sigma_2 & \sigma_2 & \sigma_2 & \sigma_2 & \sigma_2 & \sigma_2 & \sigma_2 \\
\hline
\sigma_3 & \sigma_3 & \sigma_3 & \sigma_3 & \sigma_3 & \sigma_3 & \sigma_3 & \sigma_3 & \sigma_3 & \sigma_3 \\
\hline
\end{array}
\]

etc. Without any special line to the table or not

(i) The set is closed under matrix multiplication, i.e. \( \sigma_0 \)
    is always some \( \iota \) times \( 1 \) or \( \iota \).

(ii) Matrix multiplication is associative.

(iii) \( \sigma_0 \) is the unit element.
(iv) End what has a term, wit

\[
\begin{align*}
5_0 \times 5_0 &= 5_0 \\
(-5_0)(-5_0) &= 5_0 \\
(5_0)(-5_0) &= 5_0 \\
(-5_0)(5_0) &= 5_0
\end{align*}
\]