I.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) $(x \sim y \wedge y \sim z) \Rightarrow x \sim z$ (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 $\{g, h, \dots\}$ 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 $a = b \bmod(n)$, 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)

Solution

a) No, since it is not symmetric. E.g., $2 \sim 4$, but $4 \nsim 2$.

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

c) No, since it is not reflexive: No line is perpendicular to itself. 1pt

d) Yes.

Proof. i) $a - a = 0$ is divisible by $n \quad \Rightarrow \quad a = a \bmod(n)$

ii) Let $a = b \bmod(n) \Rightarrow \exists\, k \in \mathbb{Z} :\ a - b = n$
$\Rightarrow b - a = (-k)n \Rightarrow b - a$ is divisible by n
$\Rightarrow b = a \bmod(n)$

iii) Let $a = b \bmod(n)$ and $b = c \bmod(n)$
$\Rightarrow \exists\, k, \ell \in \mathbb{Z} :\ a - b = kn$ and $b - c = \ell n$
$\Rightarrow a - c = (a - b) + (b - c) = kn + \ell n = (k + \ell)n$ with $k + \ell \in \mathbb{Z}$
$\Rightarrow a = c \bmod(n)$

$\Rightarrow a = b \bmod(n)$ is an equivalence relation on $\mathbb{Z}$. □

2pts

I.1.6 **Bounds for $n!$**

Prove by mathematical induction that

$$n^n/3^n < n! < n^n/2^n \quad \forall\, n \geq 6$$

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

(4 points)

Solution

Proof. First prove $n^n/3^n < n!$ $\forall n \geq 6$:
For $n = 6$ we have $6^6/3^6 = 2^6 = 64 < 720 = 6!$, so the inequality holds.
Now assume $m^m/3^m < m!$. Then it follows that

$$\begin{aligned}
\frac{(m+1)^{m+1}}{3^{m+1}} &= \frac{m^m}{3^m}\frac{1}{3}(1+1/m)^m(m+1) \\
&< \frac{m^m}{3^m}\frac{e}{3}(m+1) \qquad \text{by the hint} \\
&< \frac{m^m}{3^m}(m+1) < m!\,(m+1) \qquad \text{by the assumption} \\
&= (m+1)!
\end{aligned}$$

2pts

Now prove $n^n/2^n > n!$ $\forall n \geq 6$:
For $n = 6$ we have $6^6/3^6 = 2^6 = 64 < 720 = 6!$, so the inequality holds.
Now assume $m^m/2^m > m!$. Then it follows that

$$\begin{aligned}
\frac{(m+1)^{m+1}}{2^{m+1}} &= \frac{m^m}{2^m}\frac{(1+1/m)^m}{2}(m+1) \\
&\geq \frac{m^m}{2^m}(m+1) \qquad \text{by the hint} \\
&> m!(m+1) \qquad \text{by the assumption} \\
&= (m+1)!
\end{aligned}$$

□

2pts

I.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.

$n = m$: 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)

Solution

The problem lies with $n = 2$.

The induction step from $n = m$ to $n = m+1$ relies on the fact that the subsets $\{1, 2, \ldots, m\}$ and $\{2, 3, \ldots, m+1\}$ have common elements. But for $n = 2$ we have $m = 1$, and the the two sets are $\{1\}$ and $\{2\}$, which have no common elements!

$\Rightarrow$ In order for the proof to be valid, one first has to prove that any **two** ducks have the same color, which is not possible. 2pts

I.2.1. **Pauli group**

The Pauli matrices are complex 2×2 matrices defined as

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

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)

Solution

The Pauli matrices obey

	σ_0	σ_1	σ_2	σ_3
σ_0	σ_0	σ_1	σ_2	σ_3
σ_1	σ_1	σ_0	iσ_3	-iσ_2
σ_2	σ_2	-iσ_3	σ_0	iσ_1
σ_3	σ_3	iσ_2	-iσ_1	σ_0

i.e., $\sigma_i\sigma_j$ equals either some σ_k or some σ_k times $\pm i$. 1pt

Now consider P_1:

	σ_0	$-\sigma_0$	$i\sigma_0$	$-i\sigma_0$	σ_1	$-\sigma_1$	$i\sigma_1$	$-i\sigma_1$	σ_2	$-\sigma_2$	...
σ_0	σ_0	$-\sigma_0$	$i\sigma_0$	$-i\sigma_0$	σ_1	$-\sigma_1$	$i\sigma_1$	$-i\sigma_1$	σ_2	$-\sigma_2$	...
$-\sigma_0$	$-\sigma_0$	σ_0	$-i\sigma_0$	$i\sigma_0$	$-\sigma_1$	σ_1	$-i\sigma_1$	$i\sigma_1$	$-\sigma_2$	σ_2	...
$i\sigma_0$	$i\sigma_0$	$-i\sigma_0$	$-\sigma_0$	σ_0	$i\sigma_1$	$-i\sigma_1$	$-\sigma_1$	σ_1	$i\sigma_2$	$-i\sigma_2$	...
$-i\sigma_0$	$-i\sigma_0$	$i\sigma_0$	σ_0	$-\sigma_0$	$-i\sigma_1$	$i\sigma_1$	σ_1	$-\sigma_1$	$-i\sigma_2$	$i\sigma_2$	...
σ_1	σ_1	$-\sigma_1$	$i\sigma_1$	$-i\sigma_1$	σ_0	...	...	...	...	...	...
...											

etc. Even without completing the table, we see that

(i) The set is closed under matrix multiplication, since $\sigma_i\sigma_j$ is always some σ_k times either 1 or $\pm i$.

(ii) Matrix multiplication is associative. 1pt

(iii) σ_0 is the unit element.

(iv) Each element has an inverse:

$$\begin{array}{rclrclrclrcl}
\sigma_0\sigma_0 & = & \sigma_0 & \sigma_1\sigma_1 & = & \sigma_0 & \sigma_2\sigma_2 & = & \sigma_0 & \sigma_4\sigma_4 & = & \sigma_0 \\
(-\sigma_0)(-\sigma_0) & = & \sigma_0 & (-\sigma_1)(-\sigma_1) & = & \sigma_0 & (-\sigma_3)(-\sigma_3) & = & \sigma_0 & (-\sigma_4)(-\sigma_4) & = & \sigma_0 \\
(i\sigma_0)(-i\sigma_0) & = & \sigma_0 & (i\sigma_1)(-i\sigma_1) & = & \sigma_0 & (i\sigma_3)(-i\sigma_3) & = & \sigma_0 & (i\sigma_4)(-i\sigma_4) & = & \sigma_0 \\
(-i\sigma_0)(i\sigma_0) & = & \sigma_0 & (-i\sigma_1)(i\sigma_1) & = & \sigma_0 & (-i\sigma_3)(i\sigma_3) & = & \sigma_0 & (-i\sigma_4)(i\sigma_4) & = & \sigma_0
\end{array}$$

1pt