

Problem Assignment # 2

10/04/2023
due 10/11/2023

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) $(x \sim y \wedge y \sim z) \Rightarrow x \sim z$ (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 $a = b \pmod{n}$, 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

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

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

(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.

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

$n = m + 1$: Now we have $\{1, 2, \dots, m, m + 1\}$. Consider the subsets $\{1, 2, \dots, m\}$ and $\{2, \dots, m, m + 1\}$. 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)

... /over

1.2.1 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)

- 1.1.5.)
- a) No, since it is not symmetric. E.g., $2 \sim 4$, but $4 \not\sim 2$.
- b) No, since it is not symmetric. E.g., $2 \leq 4$ but $4 \not\leq 2$.
- c) No, since it is not reflexive: No line is perpendicular to itself.

①

d) Yes.

proof: (i) $a - a = 0$ is divisible by $n \rightarrow \underline{a = a \pmod{n}}$

(ii) let $\underline{a = b \pmod{n}} \rightarrow \exists k \in \mathbb{Z} : a - b = kn$

$\rightarrow b - a = (-k)n \rightarrow b - a$ is divisible by n

$\rightarrow \underline{b = a \pmod{n}}$

(iii) let $\underline{a = b \pmod{n}}$ and $\underline{b = c \pmod{n}}$

$\rightarrow \exists k, l \in \mathbb{Z} : a - b = kn$ and $b - c = ln$

$\rightarrow a - c = (a - b) + (b - c) = kn + ln = (k+l)n$

with $k+l \in \mathbb{Z}$

$\rightarrow \underline{a = c \pmod{n}}$

$\rightarrow \underline{a = b \pmod{n}}$ is an equivalence relation on \mathbb{Z} .

②

1.1.6.1 First prove $n^n/3^n < n!$ $\forall n \geq 6$

$$n=6: \quad 6^6/3^6 = 2^6 = 64 < 720 = 6! \quad \checkmark$$

Assume $n^n/3^n < n!$

$$\begin{aligned} \text{Then } \frac{(n+1)^{n+1}}{3^{n+1}} &= \frac{n^n}{3^n} \cdot \frac{1}{3} \left(1 + \frac{1}{n}\right)^n (n+1) < \frac{n^n}{3^n} \cdot \frac{e}{3} (n+1) \\ &< \frac{n^n}{3^n} (n+1) < n! (n+1) = \underline{(n+1)!} \end{aligned}$$

②

Now prove $n^n/2^n > n!$ $\forall n \geq 6$

$$n=6: \quad 6^6/2^6 = 3^6 = 729 > 720 = 6! \quad \checkmark$$

Assume $n^n/2^n > n!$

$$\begin{aligned} \text{Then } \frac{(n+1)^{n+1}}{2^{n+1}} &= \frac{n^n}{2^n} \cdot \underbrace{\frac{(1+1/n)^n}{2}}_{> 1} (n+1) \geq \frac{n^n}{2^n} (n+1) > n! (n+1) \\ &= \underline{(n+1)!} \end{aligned}$$

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

②

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 $\{1, 2, \dots, m\}$ and $\{2, 3, \dots, m+1\}$ have common elements. But for $n=2$, we have $m=1$, and hence the two sets are $\{1\}$ and $\{2\}$, which have no common element!

\rightarrow In order for the proof to be valid, one has to prove that any two decks have the same color, which is not possible.

(2)

1.2.1.) The Pauli matrices obey

	t_0	t_1	t_2	t_3
t_0	t_0	t_1	t_2	t_3
t_1	t_1	t_0	it_2	$-it_3$
t_2	t_2	$-it_1$	t_0	it_3
t_3	t_3	it_1	$-it_2$	t_0

i.e., $t_i t_j$ equals either
some t_k or some t_k
times $\pm i$

(1)

Now write P_i :

	t_0	$-t_0$	it_0	$-it_0$	t_1	$-t_1$	it_1	$-it_1$	t_2	$-t_2$	it_2	$-it_2$	t_3	$-t_3$	it_3	$-it_3$
t_0	t_0	$-t_0$	it_0	$-it_0$	t_1	$-t_1$	it_1	$-it_1$	t_2	$-t_2$						
$-t_0$	$-t_0$	t_0	$-it_0$	it_0	$-t_1$	t_1	$-it_1$	it_1	$-t_2$	t_2						
it_0	it_0	$-it_0$	t_0	$-t_0$	it_1	$-it_1$	$-t_1$	t_1	it_2	$-it_2$						
$-it_0$	$-it_0$	it_0	$-t_0$	t_0	$-it_1$	it_1	t_1	$-t_1$	$-it_2$	it_2						
t_1																
$-t_1$																
it_1																
$-it_1$																
t_2																
$-t_2$																
it_2																
$-it_2$																
t_3																
$-t_3$																
it_3																
$-it_3$																

etc. Without we complete the table we see that

(i) The set is closed under matrix multiplication, since $t_i t_j$ is always some t_k times $\pm i$.

(ii) Matrix multiplication is associative.

(iii) t_0 is the unit element

(1)

(iv) Each sheet has a given, viz

$$t_0 t_0 = t_0$$

$$t_1 t_1 = t_0$$

same for

$$(-t_0)(-t_0) = t_0$$

$$(-t_1)(-t_1) = t_0$$

 t_2, t_3

$$(it_0)(-it_0) = t_0$$

$$(it_1)(-it_1) = t_0$$

$$(-it_0)(it_0) = t_0$$

$$(-it_1)(it_1) = t_0$$

①