Homework 1

Milan Capoor

19 September 2023

1.14

Which of the following binary relations are reflexive, symmetric, antisymmetric, and/or transitive? Which are equivalence relations? Which are partial orders?

(a) $S = \mathbb{R}$ and $a \ \mathsf{R}_{\mathcal{B}} \ b$ iff $a \geq b$

- Reflexive:

  Claim: $a \ \mathsf{R}_{\mathcal{B}} \ a$

  Proof: By definition, iff $a \geq a$ then $a \ \mathsf{R}_{\mathcal{B}} \ a$. As $a = a$, the claim is clearly true.

- Transitive:

  Claim: $a \ \mathsf{R}_{\mathcal{B}} \ c$

  Proof:

$$\begin{aligned}
&(a \ \mathsf{R}_{\mathcal{B}} \ b \iff a \geq b) \land (b \ \mathsf{R}_{\mathcal{B}} \ c \iff b \geq c) \\
&\implies a \geq b \geq c \\
&\therefore a \geq c \iff a \ \mathsf{R}_{\mathcal{B}} \ c \quad \blacksquare
\end{aligned}$$

- Antisymmetric:

  Claim: $a = b$

Proof:

$$\begin{aligned}
&(a \mathrel{\mathsf{R}_{\mathcal{B}}} b \iff a \geq b) \land (b \mathrel{\mathsf{R}_{\mathcal{B}}} a \iff b \geq a)\\
&\implies a \geq b \geq a\\
&\implies a = b \quad \blacksquare
\end{aligned}$$

So (a) is a $\boxed{\text{partial order}}$

(b) $S = \mathbb{N}$ and $a \mathrel{\mathsf{R}_{\mathcal{B}}} b$ iff $\gcd(a, b) = b$

- Reflexive:

  $$a \mathrel{\mathsf{R}_{\mathcal{B}}} a \iff \gcd(a, a) = a$$

  To show the RHS holds, observe that

  $$\gcd(a, a) = d \implies d \leq a$$

  Moreover, d is larger than any other factor of a. As $a = a * 1$, however, $a \leq d \leq a$ so $d = a \implies \gcd(a, a) = a$✓

- Transitive:

  Claim: $a \mathrel{\mathsf{R}_{\mathcal{B}}} b \land b \mathrel{\mathsf{R}_{\mathcal{B}}} c \implies a \mathrel{\mathsf{R}_{\mathcal{B}}} c$

  Proof:

  $$\gcd(a, b) = b \land \gcd(b, c) = c \implies (b|a) \land (c|b)$$

  Hence, $b = cn$ for some $n \in \mathbb{N}$ and $a = bm$ for some $m \in \mathbb{N}$. Thus

  $$a = bm = (cn)m \implies c|a \implies \gcd(a, c) = c$$

- Antisymmetric:

  $$\begin{aligned}
  a \mathrel{\mathsf{R}_{\mathcal{B}}} b &\iff \gcd(a, b) = b\\
  b \mathrel{\mathsf{R}_{\mathcal{B}}} a &\iff \gcd(b, a) = a\\
  (a \mathrel{\mathsf{R}_{\mathcal{B}}} b) \land (b \mathrel{\mathsf{R}_{\mathcal{B}}} a) &\implies (\gcd(a, b) = b) \land (\gcd(b, a) = a)\\
  \gcd(a, b) = b &\implies b|a\\
  \gcd(b, a) = a &\implies a|b\\
  (b|a) \land (a|b) &\implies (a \leq b) \land (b \leq a)\\
  \therefore \quad a &= b \quad \blacksquare
  \end{aligned}$$

(c) $S = \mathbb{N}$ and $a \mathsf{R}_{\mathcal{B}} b$ iff $a|b$

- Reflexive:

$$a \mathsf{R}_{\mathcal{B}} a \iff a|a \quad \checkmark$$

- Transitive:
- Anti-Symmetric:

$$(a \mathsf{R}_{\mathcal{B}} b \wedge b \mathsf{R}_{\mathcal{B}} a) \iff (a|b \wedge b|a) \implies a = b$$

So (c) is a $\boxed{\text{partial order}}$.

(d) S is the set of students at your school, and $a \mathsf{R}_{\mathcal{B}} b$ iff a and b have the same birthday

- Reflexive:

$$a \mathsf{R}_{\mathcal{B}} a \iff \text{a has the same birthday as themselves} \quad \checkmark$$

- Transitive:

$$\begin{aligned} &(a \mathsf{R}_{\mathcal{B}} b \iff \text{a and b have the same birthday}) \\ &\qquad \wedge (b \mathsf{R}_{\mathcal{B}} c \iff \text{b and c have the same birthday}) \\ &b \mathsf{R}_{\mathcal{B}} b \implies \text{a and b and c all share a birthday} \implies a \mathsf{R}_{\mathcal{B}} c \quad \checkmark \end{aligned}$$

- Symmetric:

$$\begin{gathered} (a \mathsf{R}_{\mathcal{B}} b) \implies (b \mathsf{R}_{\mathcal{B}} a) \\ \iff \\ \text{a and b share a birthday} \implies \text{b and share a birthday} \end{gathered}$$

which is of course true because it is the same day. $\checkmark$

So (d) is an $\boxed{\text{equivalence relation}}$.

(e) S is a graph, and $a \mathsf{R}_{\mathcal{B}} b$ iff $a = b$ or there is an edge connecting a to b

Trivially, (e) is reflexive because $a = a \iff a \mathsf{R}_{\mathcal{B}} a$. Further, it is symmetric because edges are unordered so

$$[a, b] = [b, a] \implies a \mathsf{R}_{\mathcal{B}} b = b \mathsf{R}_{\mathcal{B}} a$$

Finally, it is transitive because if a is connected to b and b is connected to c, we have a path between a and c so a is connected to c by definition. Thus $a \mathsf{R}_{\mathcal{B}}\, b \wedge b \mathsf{R}_{\mathcal{B}}\, c \implies a \mathsf{R}_{\mathcal{B}}\, c$ so (e) is an $\boxed{\text{equivalence relation}}$.

(f) S is a graph, and $a \mathsf{R}_{\mathcal{B}}\, b$ iff $a = b$ or a sequence of edges connects a to b

If there is a sequence of edges connecting a to b, then a and b are in the same connected component and by definition, the relation between a and b is an $\boxed{\text{equivalence relation}}$.

2.5

Let G be a group. Prove the remaining parts of Proposition 2.9, justifying each step using the group axioms and previous proofs.

(a) G has exactly one identity element

Suppose e and e' are both identity elements of G. Since e is an identity, $e \star e' = e'$. But simultaneously, because e' is an identity, $e \star e' = e$. Therefore, $e' = e$ ■

(b) Let $g, h \in G$, Then $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$

Assume they are not equal. Then,

$$\begin{aligned} (g \cdot h)^{-1} \cdot (g \cdot h) &\neq h^{-1} \cdot g^{-1} \cdot (g \cdot h) \\ e &\neq h^{-1} \cdot g^{-1} \cdot g \cdot h \\ &\neq h^{-1} \cdot (g^{-1} \cdot g) \cdot h \\ &\neq h^{-1} \cdot e \cdot h \\ &\neq h^{-1} \cdot h \\ &\neq e \end{aligned}$$

but this is a contradiction so $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$. ■

(c) Let $g \in G$. Then $(g^{-1})^{-1} = g$

Assume $(g^{-1})^{-1} \neq g$. But then

$$(g^{-1})^{-1} \cdot (g^{-1}) \neq g \cdot g^{-1}$$

which by the definition of inverses is

$$e \neq e$$

But this is a contradiction. ■

2.7

Suppose that G is a group satisfying weaker axioms – a Right-Identity Axiom, a Right-Inverse Axiom, and an Associative law. Prove that G is a group.

Hint: First show that the right-inverse of g is also a left-inverse of g, and then show that the right-identity element is also a left-identity element.

Let g' be the inverse of g. We want to show that $g'g = gg' = e$:

$$\begin{aligned} g'g &= g'ge \quad \text{(right-identity)} \\ &= g'g \cdot (g'g \cdot (g'g)') \quad \text{(right-inverse)} \\ &= g' \cdot (gg') \cdot g \cdot (g'g)' \quad \text{(associativity)} \\ &= g'eg \cdot (g'g)' \quad \text{(right-inverse)} \\ &= g'g \cdot (g'g)' \quad \text{(right-identity)} \\ &= e \quad \text{(right-inverse)} \end{aligned}$$

So $g'g = gg'$ and a right-inverse is also a left-inverse.

Now to show the bidirectional identities, consider

$$geg = geg$$

which by the inverses is

$$g(gh)g = g(hg)g$$

then by associativity,

$$\begin{aligned} g(gh)g &= (gh)gg \\ geg &= egg \end{aligned}$$

Lemma: If $g_1a = g_2a$, $g_1 = g_2$

Proof: Let a^{-1} be the inverse of a. Then,

$$\begin{aligned} (g_1a)a^{-1} &= (g_2a)a^{-1} \\ g_1(aa^{-1}) &= g_2(aa^{-1}) \quad \text{(by associativity)} \\ g_1e &= g_2e \quad \text{(by right inverse)} \\ g_1 &= g_2 \end{aligned}$$

Applying this lemma to $geg = egg$,

$$ge = eg$$

proving that a right-identity is also a left-identity.

2.10

Let G be a finite cyclic group of order n, and let g be a generator of G. Prove that g^k is a generator of G iff $\gcd(k, n) = 1$

If $\gcd(k, n) = 1$, then $ka + nb = 1 \quad a, b \in \mathbb{Z}$. But as g is a generator, we can write

$$g = g^1 = g^{\gcd(k,n)} = g^{ka+nb} = g^{ka} \cdot g^{nb} = (g^k)^a \cdot (g^n)^b$$

But as G is a finite cyclic group of order n, $g^n = e$ so

$$(g^k)^a \cdot (g^n)^b = (g^k)^a \cdot e^b = (g^k)^a$$

Thus $(g^k)^a = g$ for some a so $\langle g^k \rangle = \langle g \rangle = G$. ■

2.15b

Let $SL_2(\mathbb{R})$ be the set of 2×2 matrices

$$SL_2(\mathbb{R}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R},\ ad - bc = 1\}$$

Prove that $SL_2(\mathbb{R})$ is a group with group law multiplication.

To be a group, $SL_2(\mathbb{R})$ must have an identity element, and inverse element, and be associative.

The identity element for matrices holds for $SL_2(\mathbb{R})$ because

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{R}) \impliedby (1)(1) - (0)(0) = 1$$

Similarly, the normal inverse works:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad - bc & -ab + ba \\ cd - dc & -cb + da \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in SL_2(\mathbb{R})$$

because

$$da - (-b)(-c) = 1 \impliedby ad - bc = 1$$

Finally, we observe that

$$\begin{aligned}
\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right)\begin{pmatrix} i & j \\ k & l \end{pmatrix} &= \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}\begin{pmatrix} i & j \\ k & l \end{pmatrix} \\
&= \begin{pmatrix} aei+bgi+afk+bhk & aej+bgj+afl+bhl \\ cei+dgi+cfk+dhk & cej+dgj+cfl+dhl \end{pmatrix} \\
\begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\begin{pmatrix} e & f \\ g & h \end{pmatrix}\begin{pmatrix} i & j \\ k & l \end{pmatrix}\right) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} ei+fk & ej+fl \\ gi+hk & gj+hl \end{pmatrix} \\
&= \begin{pmatrix} aei+afk+bgi+bhk & aek+afl+bgj+bhl \\ cei+cfk+dgi+dhk & cej+cfl+dgj+dhl \end{pmatrix} \\
\begin{pmatrix} aei+bgi+afk+bhk & aej+bgj+afl+bhl \\ cei+dgi+cfk+dhk & cej+dgj+cfl+dhl \end{pmatrix} &= \begin{pmatrix} aei+afk+bgi+bhk & aej+afl+bgj+bhl \\ cei+cfk+dgi+dhk & cej+cfl+dgj+dhl \end{pmatrix} \\
\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right)\begin{pmatrix} i & j \\ k & l \end{pmatrix} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\begin{pmatrix} e & f \\ g & h \end{pmatrix}\begin{pmatrix} i & j \\ k & l \end{pmatrix}\right)
\end{aligned}$$

so associativity holds.

Thus, $SL_2(\mathbb{R})$ is a group. $\blacksquare$

2.16

Prove or disprove that each of the following subsets of $GL_2(\mathbb{R})$ is a group.

(a) $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in GL_2(\mathbb{R}) : \; ad - bc = 2\}$

This subset is not a group because the identity for $GL_2(\mathbb{R})$ is not in the given subset:

$$\det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = (1)(1) - (0)(0) = 1 \neq 2 \quad \blacksquare$$

(b) $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in GL_2(\mathbb{R}) : \; ad - bc = \{-1, 1\}\}$

Let B denote the subset in question. Then because $SL_2(\mathbb{R})$ is a subgroup of B (notice the inclusion mapping of $SL_2(\mathbb{R})$ to B via the addition of the condition $ad - bc = -1$) so B must be a group since $SL_2(\mathbb{R})$ is a group. $\blacksquare$

(c) $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in GL_2(\mathbb{R}) : \; c = 0\}$

Let the subset in question be C. Then the inverse of $GL_2(\mathbb{R}) \in C$ because

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} \frac{d}{ad} & -\frac{b}{ad} \\ 0 & \frac{a}{ad} \end{pmatrix} = \begin{pmatrix} \frac{ad+0}{ad} & \frac{-ab}{ad} + \frac{ba}{ad} \\ 0 & \frac{da}{a} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and $\frac{d}{ad} \cdot \frac{a}{ad} - 0 \neq 0$.

Also, the identity of $GL_2(\mathbb{R})$ has $c = 0$ so it is in C.

Finally, observe that

$$\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right) \begin{pmatrix} i & j \\ k & l \end{pmatrix} = \begin{pmatrix} iae + ibg + kaf + kbh & laf + lbh + aei + bgi \\ dgi + dhk & dhl + dgi \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \left(\begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} i & j \\ k & l \end{pmatrix}\right) = \begin{pmatrix} aei + afk + bgi + bhk & afl + aei + bhl + bgi \\ dgi + dhk & dhl + dgi \end{pmatrix}$$
$$\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right) \begin{pmatrix} i & j \\ k & l \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \left(\begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} i & j \\ k & l \end{pmatrix}\right)$$

so we have associativity. Thus, C is a group. $\blacksquare$

(d) $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in GL_2(\mathbb{R}) : \; d = 0\}$

Denote the subgroup in question D. D is not a group because the identity for $GL_2(\mathbb{R})$ is not in D:

$$\begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \forall a,b,c$$

(e) $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in GL_2(\mathbb{R}) : \; a = d = 1 \text{ and } c = 0\}$

The subset has an inverse because

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Further, it has an identity because

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

Finally it satisfies associativity because

$$\begin{aligned}
\left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & a+b+c \\ 0 & 1 \end{pmatrix} \\
\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\right) &= \begin{pmatrix} 1 & a+b+c \\ 0 & 1 \end{pmatrix} \\
\begin{pmatrix} 1 & a+b+c \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & a+b+c \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

So it is a group. $\blacksquare$

2.20

If ϕ is a bijective homomorphism , the inverse map $\phi^{-1} : G_2 \to G_1$ exists. Prove that that ϕ^{-1} is a homomorphism from G_2 to G_1

ϕ^{-1} is a homomorphism from G_2 to G_1 if for $g_1, g_2 \in G_2$,

$$\phi^{-1}(g_1 g_2) = \phi^{-1}(g_1)\phi^{-1}(g_2)$$

But as ϕ is bijective, we know that $a = \phi^{-1}(g_1)$ and $b = \phi^{-1}(g_2)$ are unique. Thus,

$$\phi(a) = g_1$$
$$\phi(b) = g_2$$

and as ϕ is a homomorphism,

$$\phi(a)\phi(b) = \phi(ab) = g_1 g_2$$

so

$$\phi^{-1}(g_1 g_2) = ab = \phi^{-1}(g_1)\phi^{-1}(g_2) \quad \blacksquare$$

2.21

Let G be a group and consider

$$\phi : G \to G, \quad \phi(g) = g^{-1}$$

(a) *Prove that $\phi(\phi(g)) = g \quad \forall g \in G$*

Using the definition of ϕ,

$$\phi(\phi(g)) = \phi(g^{-1}) = (g^{-1})^{-1}$$

By Exercise 2.5c, this quantity equals g ■

(b) *Prove that ϕ is a bijection*

To be a bijection, ϕ must be injective and surjective.

For ϕ to be injective,

$$\phi(g_1) = \phi(g_2) \implies g_1 = g_2 \quad \forall g_1, g_2 \in G$$

By definition of ϕ, this is simply

$$g_1^{-1} = g_2^{-1} \implies g_1 = g_2$$

which follows directly from the uniqueness of inverses (consider $g_1 \cdot g_1^{-1} = g_1 \cdot g_2^{-1} = e$) so g_1 and g_2 have the same inverse and thus $g_1 = g_2$.

Surjectivity is established iff $\forall g_1 \in G$, $\exists g_2 \in G : \phi(g_1) = g_2$. By the inverse axiom, $\phi(g_1)$ exists for all $g_1 \in G$ and by the uniqueness of inverses, $\exists! g_2 \in G : g_1^{-1} = g_2$ which is a stronger claim than the barrier for surjectivity.

Then as ϕ is injective and surjective, it is bijective. ■

(c) *Prove that ϕ is a group homomorphism iff G is an abelian group.*

Because $\phi : G \to G$, it is a homomorphism if

$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$$

by definition of ϕ, this is just saying

$$(g_1 \cdot g_2)^{-1} = g_1^{-1} \cdot g_2^{-1}$$

Recall exercise 2.5b which proves for all groups with $g, g_2 \in G$,

$$(g_1 \cdot g_2)^{-1} = g_2^{-1} \cdot g_1^{-1}$$

Thus, all that remains is to show that

$$g_1^{-1} \cdot g_2^{-1} = g_2^{-1} \cdot g_1^{-1}$$

which by composition and association is

$$g_1^{-1} \cdot (g_2^{-1} \cdot g_2) \cdot g_1 = g_2^{-1} \cdot g_1^{-1} \cdot g_2 \cdot g_1$$

$$e = g_2^{-1} \cdot g_1^{-1} \cdot g_2 \cdot g_1$$

if and only if $g_1 \cdot g_2 = g_2 \cdot g_1$ such that

$$g_2^{-1} \cdot g_1^{-1} \cdot g_2 \cdot g_1 = g_2^{-1} \cdot g_1^{-1} \cdot g_1 \cdot g_2 = g_2^{-1} \cdot e \cdot g_2 = e$$

which is true precisely when G is an abelian group. $\blacksquare$