HOMEWORK #7 : Some solutions

Section 3.3 #5

Let $C = \{\pm 1, \pm i\}$.
Define R by $xRy \Leftrightarrow xy = \pm 1$ for $x, y \in C$.
Find C/R.

Answer: Find equiv. class of each element.
To find class of 1 notice

$1 \cdot 1 = 1$ ✓
$1 \cdot i = i$ ✗
$1 \cdot -1 = -1$ ✓
$1 \cdot -i = -i$ ✗

Thus $\overline{1} = \{1, -1\}$
Similarly $\overline{i} = \{i, -i\}$.

Thus $\boxed{C/R = \{\{1,-1\},\{i,-i\}\}}$

is the associated partition.

Section 3.3 #6

Let $C = \{\pm 1, \pm i\}$ and define S on $C \times C$ by $(x,y)\, S\, (u,v)$ if $xy = uv$. Find $C \times C / S$.

Answer: Like #5 just find equiv classes until every element is in a class.

$$\overline{(1,1)} = \{(u,v) \in C^2 : uv = 1\}$$
$$= \{(1,1), (i,-i), (-i,i), (-1,-1)\}$$
$$\overline{(1,-1)} = \{(1,-1), (-1,1), (i,i), (-i,-i)\}$$
$$\overline{(1,i)} = \{(1,i), (i,1), (-i,-1), (-1,-i)\}$$
$$\overline{(1,-i)} = \{(1,-i), (-i,1), (-1,i), (i,-1)\}.$$

We found all 16 elements of $C \times C$

Thus $C \times C / S = \{\overline{(1,1)}, \overline{(1,-1)}, \overline{(1,i)}, \overline{(1,-i)}\}$.

Section 3.3 #11

Let R be a relation on A which is sym & refl but <u>not transitive</u>.

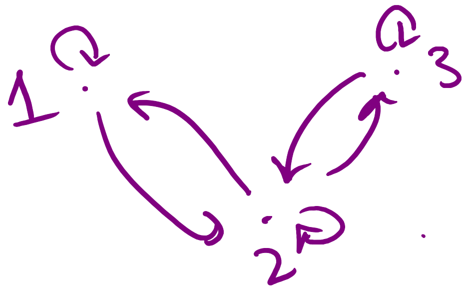
Let $R(x) = \{y \in A : xRy\}$.

Does $\{R(x) : x \in A\}$ always form a partition on A?

Answer: NO

Proof: Consider $A = \{1,2,3\}$ and $R = \{(1,1),(2,2),(3,3),(1,2),(2,1),(2,3),(3,2)\}$

Picture



Then
$$R(1) = \{1,2\}$$
$$R(2) = \{1,2,3\}$$
$$R(3) = \{2,3\}$$

Note $\{R(x) : x \in A\} = \{\{1,2\},\{1,2,3\},\{2,3\}\}$ is <u>not</u> a partition since the sets are not pairwise disjoint. $\blacksquare$

Section 3.4 #5

Try to define $\leq$ on $\mathbb{Z}_m$ by

$$\bar{x} \leq \bar{y} \text{ if } x \leq y.$$

What's wrong?

Answer: Not well defined!

For instance in $\mathbb{Z}_5$ $\bar{1} = \bar{6}$ but

$$\bar{1} \leq \bar{2} \quad \text{since } 1 \leq 2$$

while $\bar{6} \nleq \bar{2}$ since $6 \nleq 2$ //

Section 3.4 #9

(a) Claim: Let $x, y, z \in \mathbb{Z}$ with $\bar{x}\bar{y} = \bar{x}\bar{z}$ in $\mathbb{Z}_p$ ($p \in \mathbb{Z}$ prime) and $\bar{x} \neq \bar{0}$. Then
$$\bar{y} = \bar{z}.$$

Pf: Let $x, y, z \in \mathbb{Z}$ with $\bar{x}\bar{y} = \bar{x}\bar{z}$ in $\mathbb{Z}_p$ and $\bar{x} \neq \bar{0}$ in $\mathbb{Z}_p$.

Then
$$\bar{x}\bar{y} + \overline{(-1)}\bar{x}\bar{z} = \bar{0} \quad \text{in } \mathbb{Z}_p$$
$$\Rightarrow \overline{(xy - xz)} = \bar{0}$$
$$\Rightarrow \bar{x} \cdot \overline{y - z} = \bar{0}.$$

By Thm 3.4.4 there are no zero divisors in $\mathbb{Z}_p$,

so $\bar{x} = \bar{0}$ or $\overline{y-z} = \bar{0}$

But $\bar{x} \neq \bar{0}$ by assumption so $\overline{y-z} = \bar{0}$ in $\mathbb{Z}_p$ so $p \mid y - z$

so $\bar{y} = \bar{z}$ in $\mathbb{Z}_p$. ∎

Section 3.4 #10

Claim: $\forall m \in \mathbb{N}$

$$x \equiv y \pmod{m} \Rightarrow x^k \equiv y^k \pmod{m}$$

$\forall k \in \mathbb{N}$.

Pf: We proceed by induction on $k \in \mathbb{N}$.

Fix some $m \in \mathbb{N}$.

Notice the claim is trivial for $k=1$, since

$$x \equiv y \pmod{m} \Rightarrow x^1 \equiv y^1 \pmod{m}$$

is true for any $x, y \in \mathbb{Z}$.

Now assume $k \in \mathbb{Z}$ is such that

$$x \equiv y \pmod{m} \Rightarrow x^k \equiv y^k \pmod{m}$$

$\forall x, y \in \mathbb{Z}$.

Assume $x, y \in \mathbb{Z}$ are such that

$$x \equiv y \pmod{m}$$

and we will show $x^{k+1} \equiv y^{k+1} \pmod{m}$

By assumption since $x \equiv y \pmod{m}$ we can conclude

$$x^k \equiv y^k \pmod{m}.$$

Now multiply both sides by x to get

$$x^{k+1} = y^k x \pmod{m}$$

and since $x = y \pmod{m}$ we can substitute y for x on the right to get

$$x^{k+1} = y^{k+1} \pmod{m}$$

as desired. $\blacksquare$