Intro Modern Algebra I HW2 Solution

Zhaocheng Dong

September 27, 2023

Problem 1

1. Not an equivalence relation since $x + x = 2x$ is even for all $x \in \mathbb{R}$, so $\neg xRx \forall x$, R is not reflexive.

2. R is an equivalence relation.

   - Reflexive: The trivial rotation(identity map) takes any x to itself.
   - Symmetric: If there is a rotation $r : u \mapsto v$, the rotation is invertible and its inverse $r^{-1} : v \mapsto u$ takes v to u, so R is symmetric.
   - Transitive: If there is a rotation $r_1 : u \mapsto v$ and another rotation $r_2 : v \mapsto w$, then $r_2 \circ r_1 : u \mapsto w$ is also a rotation, so R is transitive.

   The equivalence classes are the points that are equidistant from the origin, since rotation preserves distance. i.e., they are concentric spheres centered at the origin.
   Remark: Rotations in $\mathbb{R}^3$ are characterized by action of the group $SO_3(\mathbb{R})$, and the fact that the identity map, inverse and composition maps still belongs to SO_3 relies on its property as a group. The equivalence classes are the orbits of $\mathbb{R}^3$ under the action.

3. R is an equivalence relation. Reasoning provided via high school geometry knowledge.

   - Reflexive: Any triangle is similar to itself.

- Symmetric: If triangle A is similar to triangle B, then triangle B is similar to triangle A since, for example, their respective angles equal.
- Transitive: If triangle A is similar to triangle B, and triangle B is similar to triangle C, then triangle A is also similar to triangle C since their respective angles will equal from the transitivity of =.

The equivalence classes are the sets in which the triangles are equal. One characterization is $\{(\alpha_1, \alpha_2, \alpha_3) : \alpha_1 + \alpha_2 + \alpha_3 = 180°\}$ up to permutation.

4. R is not an equivalence relation because it is not symmetric. Take, for example, $f(x) = 1$ and $g(x) = 2$ two constant functions. Clearly gRf since $g(x) - f(x) = 1$, but $f(x) - g(x) = -1$ so $\neg fRg$.

Problem 2

- Reflexive: For any $f \in X$, $\int_0^1 f(x)dx = \int_0^1 f(x)dx$ so fRf.
- Symmetric: If fRg, $\int_0^1 f(x)dx = \int_0^1 g(x)dx$ which means $\int_0^1 g(x)dx = \int_0^1 f(x)dx$ and gRf.
- Transitive: If fRg and gRh, $\int_0^1 f(x)dx = \int_0^1 g(x)dx$ and $\int_0^1 g(x)dx = \int_0^1 h(x)dx$ so $\int_0^1 f(x)dx = \int_0^1 h(x)dx$ and fRh.

So R is indeed an equivalence relation. The equivalence classes are functions that have the same integral value. A bijection $F : X/\sim \to \mathbb{R}$ would be

$$F([f]) = \int_0^1 f(x)dx$$

Injectivity: If $[f]$ and $[g]$ in $X/\sim$ such that $F([f]) = F([g])$, then $\int_0^1 f(x)dx = \int_0^1 g(x)dx$ which means fRg and $[f] = [g]$.
Surjectivity: For any $c \in \mathbb{R}$, the equivalence class containing the constant function $f(x) = c$ maps to c since $\int_0^1 f(x)dx = \int_0^1 cdx = c$.

Problem 3

1. $[5] \cdot [5] = [25] = [8]$

2. $[0]^2 = [0].[1]^2 = [1], [2]^2 = [4], [3]^2 = [9], [4]^2 = [16].[5]^2 = [8], [6]^2 = [2], [7]^2 = [15], [8]^2 = [13], [9]^2 = [13], [10]^2 = [15], [11]^2 = [2], [12]^2 = [8], [13]^2 = [16], [14]^2 = [9], [15]^2 = [4], [16]^2 = 1$, so $[3]$ is not a quadratic residue.

3. If $[n]$ and $[m]$ are quadratic residues, $[n] = [a][a]$ and $[m] = [b][b]$, so $[nm] = [n][m] = [a][a][b][b] = [a][b][a][b] = ([a][b])^2 = [ab]^2$, so $[nm]$ is a quadratic residue.

4. Towards a contradiction, assume $[n]$ and $[nm]$ are quadratic residues and $[m]$ is not. Then $[n] = [d][d]$ and $[nm] = [c][c]$. By Bezout's theorem, there exist $[f]$ such that $[d][f] = [1]$. Then

$$\begin{aligned} [nm] &= [c][c] \\ [n][m] &= [c][c] \\ [d][d][m] &= [c][c] \\ [f][f][d][d][m] &= [f][f][c][c] \\ [m] &= [f][f][c][c] \\ [m] &= [fc]^2 \end{aligned}$$

which means $[m]$ is a quadratic residue, which is a contradiction.

Problem 4

1

$$\begin{aligned} 865 &= 8 \times 107 + 9 \\ 17 &= 11 \times 9 + 8 \\ 9 &= 1 \times 8 + 1 \\ \Rightarrow & \gcd(107, 865) = 1, \\ & \operatorname{lcm}(107, 865) = 107 \times 865/1 = 92555 \end{aligned}$$

2

$$\begin{aligned}
5291 &= 28 \times 185 + 111 \\
185 &= 1 \times 111 + 74 \\
111 &= 1 \times 74 + 37 \\
74 &= 2 \times 37 \\
&\Rightarrow \text{gcd}(5291, 185) = 37, \\
&\quad \text{lcm}(5291, 185) = 5291 \times 185/37 = 26455
\end{aligned}$$

Problem 5

(24)

Let $X = \{p : p \text{ prime}, p|a \text{ or } p|b\}$ be the set of all prime factors of a and b combined, then X is finite and we can order the primes in X increasingly as $p_1, p_2, ..., p_r$. Then we can write

$$|a| = \prod_{i=1}^{r} p_i^{a_i}, |b| = \prod_{i=1}^{r} p_i^{b_i}$$

where $a_i, b_i \in \mathbb{Z}_{\geq 0}$. Then

$$d = \prod_{i=1}^{r} p_i^{\min(a_i,b_i)}, m = \prod_{i=1}^{r} p_i^{\max(a_i,b_i)}.$$

Therefore,

$$dm = \prod_{i=1}^{r} p_i^{\min(a_i,b_i)+\max(a_i,b_i)} = \prod_{i=1}^{r} p_i^{a_i+b_i} = |ab|.$$

Note: Since the course slides defined lcm to be $\frac{|ab|}{gcd(a,b)}$, credit is granted to those that use the formula in this problem due to lack of clarification. However, using the definition of lcm in terms of gcd will result in circular proof in this problem and is technically incorrect.

(25)

Using the formula in (24),

$$\mathrm{lcm}(a,b) = ab \Leftrightarrow \frac{|ab|}{\gcd(a,b)} = ab \Leftrightarrow \gcd(a,b) = \pm 1$$

but $\gcd(a,b) > 0$ by definition so $\gcd(a,b) = 1$.