MATH 2020 Test 1 Solutions.

Q1)

a) An equivalence relation on X is a relation $R \subset X \times X$ which is:

(i) Reflexive, meaning $x \sim x$ for all $x \in X$

(ii) Symmetric, meaning $x \sim y \Rightarrow y \sim x$ for all $x, y \in X$

(iii) Transitive, meaning $x \sim y$ and $y \sim z \Rightarrow x \sim z$ for all $x, y, z \in X$.

b) The equivalence class of $x \in X$ is the set

$$[x] = \{ y \in X \mid y \sim x \}.$$

c) The equivalence classes of "congruence mod n" are $[0], [1], \ldots, [n-1]$, where

$$[i] = \{ m \in \mathbb{Z} \mid m = i + kn \text{ for some } k \in \mathbb{Z} \}.$$

Q2)

a) A group is a set G together with a binary operation $\circ : G \times G \longrightarrow G$ satisfying:
$$(g, h) \longmapsto g \cdot h$$

(i) The binary operation is associative, so
$$f \cdot (g \cdot h) = (f \cdot g) \cdot h \text{ for all } f, g, h \in G.$$

(ii) There is an identity element $e \in G$ satisfying
$$e \cdot g = g \cdot e = g \text{ for all } g \in G.$$

(iii) For every $g \in G$ there exists an inverse element $g^{-1} \in G$, satisfying
$$g \cdot g^{-1} = g^{-1} \cdot g = e.$$

b) A group G is abelian if $gh = hg$ for all $g, h \in G$.

c) From part (a) we have to check 3 things:

(i) Associativity. We compute:
$$\begin{aligned} a * (b * c) &= a * (b + c + bc) \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + bc + ab + abc \end{aligned}$$

and

$$(a * b) * c = (a+b+ab) * c$$

$$= (a+b+ab)+c+(a+b+ab)c$$

$$= a+b+c+ab+ac+bc+abc$$

Since these two expressions are equal, $*$ is associative

(ii) Note that $0 \in \mathbb{R}\setminus\{-1\}$ serves as an identity, since

$a * 0 = a + 0 + a \cdot 0 = a$ and

$0 \cdot a = 0 + a + 0 \cdot a = a$ for all $a \in \mathbb{R}\setminus\{-1\}$.

(iii) If $a \in \mathbb{R}\setminus\{-1\}$ is to have an inverse, there must exist $b \in \mathbb{R}\setminus\{-1\}$ such that

$$a+b+ab=0$$

or in other words

$$b(a+1) = -a$$

$$\Rightarrow b = \frac{-a}{a+1}.$$

Note that $\frac{-a}{a+1} = -1 \iff -a = -a-1$

$\iff 0 = -1$, so our formula yields a number in $\mathbb{R}\setminus\{-1\}$, as required.

Thus inverses exist.

Remark. Note there is technically a fourth condition to check in Q2 (c), though this was not expected of you: We must also check that

$$a * b = a + b + ab$$

defines a map $\mathbb{R} \setminus \{-1\} \times \mathbb{R} \setminus \{-1\} \longrightarrow \mathbb{R} \setminus \{-1\}$, by verifying that $a+b+ab \neq -1$, as long as neither a nor b is -1.

We check:

$$\begin{aligned} & a+b+ab = -1 \\ \iff & ab + a + b + 1 = 0 \\ \iff & (a+1)(b+1) = 0 \\ \iff & a = -1 \text{ or } b = -1, \end{aligned}$$

so it works.

Q2 d) The symmetric group S_3 is not abelian, since

$$(1\ 2\ 3)(1\ 2) = (1\ 3)$$

while

$$(1\ 2)(1\ 2\ 3) = (2\ 3).$$

Q3

a) If a is a generator of G, then $(a^{n/m})^m = a^n = e$, so $a^{n/m} \in H$. Therefore H is nontrivial. H is a subgroup, because we can check:

(i) $e \in H$ since $e^m = e$, so H contains the identity.

(ii) If $h, g \in H$ then $h^m = e$ and $g^m = e$.

Therefore $$\underbrace{(hg)^m = h^m g^m}_{\text{because cyclic groups are abelian.}} = e \cdot e = e$$

so $gh \in H$.

(iii) If $g \in H$, then $g^m = e$. Therefore

$$(g^{-1})^m = (g^m)^{-1} = e^{-1} = e,$$

so $g^{-1} \in H$ as well.

b) Since $(a^{n/m})^m = a^n = e$, $a^{n/m} \in H = \langle a^d \rangle$.

Thus there exists k such that $(a^d)^k = a^{dk} = a^{n/m}$, so d divides n/m.

On the other case, since $(a^d)^m = e$ (because $a^d \in H$), we know that n must divide dm since a is a generator of G (by a theorem from class).

c) If $kn = dm$ and $\frac{n}{m} = d\ell$ for some $k, \ell \in \mathbb{Z}$

then $n = (dm)\ell \Rightarrow n = kn\ell \Rightarrow k\ell = 1$.

Thus we have $\ell = \pm 1$, so $\frac{n}{m} = \pm d$. We can assume that d is chosen so that $\frac{n}{m} = d$, as this still provides a generator of H.

d) By a theorem from class, the order of a^d in G (a is a generator) is

$$\frac{n}{\gcd(d,n)} = \frac{n}{\gcd(\frac{n}{m}, n)} = \frac{n}{\frac{n}{m}} = m.$$