Abstract Algebra Hw #2 Solns — Joe Cutrone

1. p. 28 #10.

Let G be the group of rigid motions of a cube in $\mathbb{R}^3$. Label any two adjacent vertices ① and ②. Then there are 8 choices of vertices to map ① to. Given this vertex, there are then 3 choices for ②, since it must go to an adjacent vertex. Thus there are $8 \cdot 3 = 24$ elements in G.

p. 33 #5

$|(1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)| = \text{lcm}(5,2,3) = 30$

p. 33 #11

Let σ be an m-cycle

($\Rightarrow$) Then σ^i is an m-cycle $\Rightarrow |\sigma^i| = m \iff |i| = m$ for $i \in \mathbb{Z}/m\mathbb{Z} \iff (m,i) = 1$

($\Leftarrow$) View σ^i as a function where σ^i takes $a \mapsto a+i \bmod m$

since $|i| = m$ in $\mathbb{Z}/m\mathbb{Z}$, the number of times you need to apply σ to return to given a is $|i| = m$

$\therefore \sigma = (1a, 2a, \ldots, ma)$. Relabel to get $\sigma = (1, 2, \ldots, m)$ so σ is an m-cycle

3. p. 35 #11

Let $H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix} \in GL_3(F) \right\}$. Let $X = \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix}$, $Y = \begin{pmatrix} 1 & d & e \\ & 1 & f \\ & & 1 \end{pmatrix} \in H(F)$

a) $XY = \begin{pmatrix} 1 & a+d & e+af+b \\ & 1 & f+c \\ & & 1 \end{pmatrix} \in H(F)$ $\therefore$ closed w.r.t $\times$

if $X = \begin{pmatrix} 1 & 2 & 3 \\ & 1 & 4 \\ & & 1 \end{pmatrix}$, $Y = \begin{pmatrix} 1 & 5 & 6 \\ & 1 & 7 \\ & & 1 \end{pmatrix}$, then $XY = \begin{pmatrix} 1 & 7 & 23 \\ & 1 & 11 \\ & & 1 \end{pmatrix} \neq YX = \begin{pmatrix} 1 & 7 & 29 \\ & 1 & 11 \\ & & 1 \end{pmatrix}$

b) $X^{-1} = \begin{pmatrix} 1 & -a & -b+ac \\ & 1 & -c \\ & & 1 \end{pmatrix} \in H(F)$

c) I'll let you work out it is associative. Since $|F|$ choices for each of a, b, c, $|H(F)| = |F|^3$

d) $H(\mathbb{Z}_2) = \left\{ \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & 1 \\ & 1 & \\ & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & 1 & 1 \\ & & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ & 1 & \\ & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & 1 \\ & 1 & 1 \\ & & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & \\ & 1 & 1 \\ & & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{pmatrix} \right\}$ $(\cong D_4)$

orders: 1 2 2 2 2 2 4 4

e) If $X \in H(\mathbb{R})$, $X \neq I$, $|X| = n$, then $X^n = I$

Let $X = \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix}$. Then $X^n = \begin{pmatrix} 1 & na & bn + f(a,c) \\ & 1 & nc \\ & & 1 \end{pmatrix}$ where $f(a,c) \in \mathbb{R}[a,c]$ s.t $f(0,0) = 0$

equating entries gives $na = 0$, $nc = 0 \Rightarrow a, c = 0 \Rightarrow bn = 0 \Rightarrow b = 0$

$\therefore I = X$ ↯ $\therefore |X| = \infty$

Abstract Algebra Hw #2 Solns — Joe Cutrone

4. Let G grp, $\varphi: G \to G$ def by $x \mapsto x^{-1}$

Then $\varphi(xy) = \varphi(x)\varphi(y) \leftrightarrow (xy)^{-1} = x^{-1}y^{-1} \leftrightarrow y^{-1}x^{-1} = x^{-1}y^{-1} \leftrightarrow 1 = x^{-1}y^{-1}xy \leftrightarrow xy = yx \leftrightarrow G$ abelian

5. Let $|G| = 4$

By exhausting possible group operations, easy to see G must be abelian.

$\therefore$ by Fundamental Thm of Finitely Generated Abelian Groups (Thm 3 p.158) $G \cong \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$

6. Define $\varphi: \{e^{\frac{2\pi i k}{n}} \mid k \in \mathbb{Z}\} \to \mathbb{Z}/n\mathbb{Z}$ by $e^{\frac{2\pi i k}{n}} \mapsto k \bmod n$

This is clearly well-defined & surjective

φ is easily seen to be a homomorphism

φ injective since if $e^{\frac{2\pi i k}{n}} \in \ker \varphi$, $k \equiv 0 \bmod n$, ie $k = nt$ for $t \in \mathbb{Z}$

so $e^{\frac{2\pi i k}{n}} = e^{\frac{2\pi i n t}{n}} = (e^{2\pi i})^t = 1^t = 1$

$\therefore \varphi$ isomorphism

7. Let p be prime. Let $|G| = p$, $x \in G$, $x \neq 1$. By Lagrange's Thm, $|\langle x \rangle| \mid |G| = p$

$\therefore |\langle x \rangle| = 1$ or p. Since $x \neq 1$, $|\langle x \rangle| = p$

$\therefore$ every grp of order p is cyclic, and $G \cong \mathbb{Z}/p\mathbb{Z}$

8. The element $(0,1)$ has order 2 in $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, whereas no element in $\mathbb{Z}$ has order 2

9. Let p prime, $a \in \mathbb{Z}$. $|(\mathbb{Z}/p\mathbb{Z})^\times| = \varphi(p) = p-1$ by Prop 16, p.135

since $\bar{a}^{p-1} = \bar{1}$, mult both sides by $\bar{a}$ to get $\bar{a}^p = \bar{a}$ in $\mathbb{Z}/p\mathbb{Z}$

(ps - this is Fermat's Little Thm: $a^{\varphi(n)} \equiv 1 \bmod n$ for $(a,n) = 1$

10. Let $G = (\mathbb{Z}/2^k\mathbb{Z})^\times$ for $k \geq 3$

1. Let $(2^k, n) = 1$. Then $\bar{n} \in G$ by Prop 4 pg 10

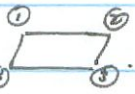
2. $|G| = \varphi(2^k) = 2^{k-1}$ by prop 16 p 135

Abstract Algebra Hw 2 — Joe Cutmore

3. $(2^{k+1}\pm 1)(2^{k+1}\pm 1) = 2^{2k+2} \pm 2\cdot 2^{k+1} + 1 \equiv 1 \bmod 2^k$

$(2^k-1)(2^k-1) = (2^k)^2 - 2\cdot 2^k + 1 \equiv 1 \bmod 2^k$

4. $\mathbb{Z}/2m\mathbb{Z}$ cyclic of order $2m$. Clearly $m \in \mathbb{Z}/2m\mathbb{Z}$ is the only element of order 2 so $\underline{1}$ element

11. Label the vertices of a rectangle 

. Then the only rigid motions are $\{1, (13)(24), (12)(34), (14)(23)\}$ which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ (The Klein 4-group)

12. Let $\mathbb{Q}/\mathbb{Z} = (\mathbb{Q},+)/\sim$ where $\frac{p}{q} \sim \frac{a}{b} \iff \frac{p}{q} - \frac{a}{b} \in \mathbb{Z}$

Show $\mathbb{Q}/\mathbb{Z}$ a group: For $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}/\mathbb{Z}$, $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in \mathbb{Q}/\mathbb{Z}$ $\therefore$ closed

Assoc follows from associativity of $(\mathbb{Q},+)$

Identity is $0 = \frac{0}{1}$

Inverse of $\frac{p}{q} = \frac{-p}{q} \in \mathbb{Q}/\mathbb{Z}$ $\therefore$ Group

1. For $\bar{r} \in \mathbb{Q}/\mathbb{Z}$, let $\bar{r} = \frac{p}{q}$ and WOLOG, say $\frac{p}{q} \geq 0$.

If $\frac{p}{q} \in [0,1)$ done, so assume not

Then $\frac{p}{q} - \lfloor \frac{p}{q} \rfloor \in [0,1)$, where $\lfloor \frac{p}{q} \rfloor$ is the floor function. Call this representative $r' \in [0,1)$

Then $\frac{p}{q} \sim r'$ since $\frac{p}{q} - r' = \lfloor \frac{p}{q} \rfloor \in \mathbb{Z}$.

2. Let $n \in \mathbb{N}$. Then $\frac{1}{n} \in \mathbb{Q}/\mathbb{Z}$, and $\langle \frac{1}{n} \rangle = \{1, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}\}$, so $|\langle \frac{1}{n} \rangle| = n$

by part a), $\exists!$ copy of $\mathbb{Z}/n\mathbb{Z}$ in $\mathbb{Q}/\mathbb{Z}$

3. Any $\varphi \in \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$ is completely determined where $\bar{1}$ gets mapped

mapping $1 \xmapsto{\varphi} d/n$ for any $n \in \mathbb{N}$ gives all homomorphisms from $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\varphi} \mathbb{Q}/\mathbb{Z}$

$\therefore \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$

$\mathrm{card}\,|\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z})| = \mathrm{card}\,|\mathbb{Z}/n\mathbb{Z}| = \mathrm{card}\,|\mathbb{N}| =$ countable

4. Any $\varphi \in \mathrm{Hom}(\mathbb{Q}/\mathbb{Z}, \mathbb{Z})$ must take an element $\frac{p}{q}$ to 0, since every element in $\mathbb{Q}/\mathbb{Z}$ has finite order and 0 is the only element of $\mathbb{Z}$ with finite order

$\therefore \mathrm{Hom}(\mathbb{Q}/\mathbb{Z}, \mathbb{Z}) = 0$

$\mathrm{card}\,|\{0\}| = 1$

note: see remark in ex 2 p 787 on "Pontrigin Dual Group"