Ch 3 Sltns # 2, 3, 5, 7, 12, 15, 18, 22, 23, 32, 33, 37, 38, 42-44, 49-51, 58, 60, 61, 63, 67, 71, 79

2) $(\mathbb{Q}, +)$ $\langle \frac{1}{2} \rangle = \{ \ldots -2, -\frac{3}{2}, -1, -\frac{1}{2}, 0, \frac{1}{2}, 1, \frac{3}{2}, \ldots \} = \{ k\frac{1}{2} \mid k \in \mathbb{Z} \}$

$(\mathbb{Q}^*, \times)$ $\langle \frac{1}{2} \rangle = \{ \ldots 8, 4, 2, 1, \frac{1}{2}, \frac{1}{4}, \ldots \} = \{ \frac{1}{2^n} \mid n \in \mathbb{Z} \}$

3) In $\mathbb{Q}$

$|0| = 1$

$|x| = \infty \ \forall x \neq 0$

In $\mathbb{Q}^*$

$|1| = 1$

$|-1| = 2$

$|x| = \infty \ \forall x \neq \pm 1$

5) each pair are an element and its inverse, and $|g| = |g^{-1}|$ from #4

7) $|a| = 6$, $|b| = 7$

$(a^4 c^{-2} b^4)^{-1} = (b^4)^{-1} (c^{-2})^{-1} (a^4)^{-1} = b^{-4} c^2 a^{-4} = \boxed{b^3 c^2 a^2}$

12) $a, b \in G$ and $ab \neq ba$, prove $aba \neq e$.

Assume $aba = e$. Then $ab = a^{-1} \Rightarrow b = a^{-1}a^{-1} = a^{-2}$

So $ab = a a^{-2} = a^{-1} = a^{-2} a = ba$. $\Rightarrow\Leftarrow$

15) $a \in G$, $|a| = 7$ show a is a cube.

$|a| = 7 \Rightarrow a^7 = e \Rightarrow a^{14} = e$ so $a = ae = aa^{14} = a^{15} = (a^5)^3$ and $a^5 \in G$ by closure

18) $a \in G$, $a^6 = e$

$|a| \leq 6$ since $a^6 = e$

$|a|$ can be 1, 2, 3, or 6 since $a^6 = (a^3)^2 = (a^2)^3 = (a^1)^6 = e$

$|a|$ can not be 4 b/c $|a| = 4 \Rightarrow a^4 = e \Rightarrow a^6 = a^2 \neq e$ $\Rightarrow\Leftarrow$

$|a|$ can not be 5 b/c $|a| = 5 \Rightarrow a^5 = e \Rightarrow a^6 = a \neq e$ $\Rightarrow\Leftarrow$

22) Show $\mathcal{U}(14) = \langle 3 \rangle = \langle 5 \rangle$; is $U(14) = \langle 11 \rangle$?

$\mathcal{U}(14) = \{1, 3, 5, 9, 11, 13\}$

$\langle 3 \rangle = \{3,\ 3^2 = 9,\ 3^3 = 27 = 13,\ 3^4 = 39 = 11,\ 3^5 = 33 = 5,\ 3^6 = 15 = 1\} = \mathcal{U}(14)$

$\langle 5 \rangle = \{5,\ 5^2 = 25 = 11,\ 5^3 = 55 = 13,\ 5^4 = 65 = 9,\ 5^5 = 45 = 3,\ 5^6 = 15 = 1\} = \mathcal{U}(14)$

$\langle 11 \rangle = \{11,\ 11^2 = 121 = 11, \ldots\}$ oh no! $\langle 11 \rangle = \{11\} \neq \mathcal{U}(14)$

23) Show $\mathcal{U}(20) \neq \langle k \rangle$

$\mathcal{U}(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$\langle 1 \rangle = \{1\}$

$\langle 3 \rangle = \{3, 9, 7, 1\} = \langle 7 \rangle$, $\langle 9 \rangle = \{9, 1\}$

$\langle 11 \rangle = \{11, 1\}$

$\langle 13 \rangle = \{13, 9, 17, 1\} = \langle 17 \rangle$, $\langle 19 \rangle = \{19, 1\}$

32) H, K subgrps of G, show $H \cap K$ is a subgrp of G.

* $e \in H \cap K$ so $H \cap K \neq \emptyset$

Let H, K be subgrps of G. Consider $H \cap K$, with $a, b \in H \cap K$.

Since $a, b \in H \cap K$, $a, b \in H$ and $a, b \in K$. H, K subgrps means they are closed

So $ab \in H$ and $ab \in K$. Thus $ab \in H \cap K$ so $H \cap K$ is closed.

Also $a \in H$ and $a \in K$ implies $a^{-1} \in H$ and $a^{-1} \in K$ b/c subgrps are closed under inverses. Thus $H \cap K$ is a subgrp of G.

33) G grp, Show $Z(G) = \bigcap_{a \in G} C(a)$.

- Let $x \in Z(G)$. Then $xa = ax$ $\forall a \in G$. So $x \in C(a)$ $\forall a \in G$. Thus $x \in \bigcap_{a \in G} C(a)$

  So $Z(G) \subseteq \bigcap_{a \in G} C(a)$.

- Let $x \in \bigcap_{a \in G} C(a)$. Then $x \in C(a)$ $\forall a \in G)$ so $xa = ax$ $\forall a \in G$. So $x \in Z(G)$ by def.

  So $\bigcap_{a \in G} C(a) \subseteq Z(G)$.

37) a) $C(1)=\{1,2,3,4,5,6,7,8\}=G$

$C(2)=\{1,2,5,6\}$

$C(3)=\{1,3,5,7\}$

$C(4)=\{1,4,5,8\}$

$C(5)=\{1,2,3,4,5,6,7,8\}=G$

$C(6)=\{1,2,5,6\}$

$C(7)=\{1,3,5,7\}$

$C(8)=\{1,4,5,8\}$

b) $Z(G)=\{1,5\}$

c) $|1|=1$, $|2|=2$, $|3|=4$, $|4|=2$, $|5|=2$, $|6|=2$, $|7|=4$, $|8|=2$

the orders of the elements divide the order of the group

38) Let $a\neq b\in G$ grp. Prove either $a^2\neq b^2$ or $a^3\neq b^3$.

Assume not. Then $a^2=b^2$ and $a^3=b^3$. So $a^3=a(a^2)=b(b^2)=b^3$

But $a^2=b^2$ so $a(a^2)=a(b^2)=b(b^2)$. Using right cancellation, $a=b$. $\Rightarrow\Leftarrow$

42) $C(H)=\{x\in G \mid xh=hx \ \forall h\in H\}$ is the centralizer of H.

Show $C(H)$ is a subgrp of G. $* \ e\in C(H)$ so $C(H)\neq\emptyset$

Let $a,b\in C(H)$. Then $ah=ha$ and $bh=hb$ $\forall h\in H$. So

$(ab)h=a(bh)=a(hb)=(ah)b=h(ab)$ $\forall h\in H$. Thus $ab\in H$.

Now $ah=ha$ also implies $aha^{-1}=h \Rightarrow ha^{-1}=a^{-1}h$ $\forall h\in H$. so $h^{-1}\in C(H)$.

Thus $C(H)$ is a subgrp.

43) Must $C(a)$ be Abelian?

i.e. if $x,y\in C(a)$, does $xy=yx$?

No. Let $G=D_4$. $C(r^2)=D_4$! (but D_4 is not Abelian)

44) Must $Z(G)$ be Abelian? Yes b/c elements in $Z(G)$ commute w/ all of G, including each other.

49) Suppose $a, b \in G$ s.t. $|a| = 4$, $|b| = 2$, and $a^3 b = ba$. Find $|ab|$.

$(ab)^2 = abab = a(ba)b = a(a^3b)b = a^4 b^2 = e$ so $|ab| = 2$.

50) Suppose $a, b \in G$ s.t. $|a| = 2$, $b \neq e$ and $aba = b^2$. Find $|b|$.

$b^4 = aba\,aba = aba^2ba = ab^2a = aabaa = a^2ba^2 = b$.

So $b^4 = b \Rightarrow b^3 = e \Rightarrow |b| \leq 3$. $b \neq e$ so $|b| \neq 1$; if $|b| = 2$ then $b^3 = bb^2 = be = b = b^4$ $\Rightarrow b = e \Rightarrow \Leftarrow$

51) $a \in G$ with $|a| = n$

Suppose $d > 0$ is a divisor of n. Show $|a^d| = n/d$

$|a| = n \Rightarrow a^n = e$. Since $d | n$, $\frac{n}{d} \in \mathbb{Z}_{>0}$ and $a^n = (a^d)^{\frac{n}{d}} = e$. Thus $|a^d| \leq \frac{n}{d}$.

Assume $|a^d| = k < \frac{n}{d}$. Then $(a^d)^k = a^{dk} = e$ so $|a| \leq dk$

but $dk < d\left(\frac{n}{d}\right) = n$ $\Rightarrow \Leftarrow$ so $|a^d| = \frac{n}{d}$

58) $\mathcal{U}(15)$ has 6 cyclic subgrps. List them.

$\mathcal{U}(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$

(1): $\langle 1 \rangle = \{1\}$

(2): $\langle 2 \rangle = \{2, 4, 8, 1\}$

(3): $\langle 4 \rangle = \{1, 4\}$

(4): $\langle 7 \rangle = \{7, 4, 13, 1\}$

(5): $\langle 11 \rangle = \{11, 1\}$

(6): $\langle 14 \rangle = \{14, 1\}$

60) G grp s.t. G has 8 elements of order 3; How many subgrps of order 3?

Let $|H| = 3$ for H a subgrp of G. Then $H = \{e, a, b\}$.

Now $ab \in H$, so $ab = a$ or $ab = b$ or $ab = e$. . .

If $ab = a \Rightarrow b = e \Rightarrow \Leftarrow$. If $ab = b \Rightarrow a = e \Rightarrow \Leftarrow$. So $ab = e \Rightarrow a^{-1} = b$.

So $H = \{e, a, a^{-1}\}$. Now $a^2 \neq a$, so $a^2 = e$ or $a^2 = a^{-1}$. If $a^2 = e$, $a = a^{-1}$ $\Rightarrow \Leftarrow$

Thus $a^2 = a^{-1}$. So $H = \{e, a, a^2\}$. so $|a| = |a^2| = 3$ which means every subgrp of order 3 has exactly 2 elements of order 3. Since $H = \langle a \rangle$ we know that these subgroups have trivial intersection. Thus there are $8/2 = \boxed{4}$ subgrps.

61) H subgrp of G, $|G| < \infty$, Suppose $g \in G$ and $g^n \in H$ (n smallest).

Prove $n \mid |g|$.

Let $|g| = m$. Then $m = qn + r$ where $q, r \in \mathbb{Z}_{\geq 0}$, $0 < r < n$.

So $e = g^m = g^{qn+r} = g^{qn} g^r = (g^n)^q g^r = e g^r = g^r$.

But $e \in H$ since e is a subgrp so $g^r \in H$. $\Rightarrow \Leftarrow$ b/c $r < n$ and n is smallest.

63) $\mathbb{R}^*$, $H = \{x \in \mathbb{R}^* \mid x^2 \in \mathbb{Q}\}$.

- Prove H subgrp $*$ $1^2 \in \mathbb{Q}$ so $1 \in H$ so $H \neq \emptyset$

  Closure: $x, y \in H \Rightarrow x^2 \in \mathbb{Q}$ and $y^2 \in \mathbb{Q}$.

  Now $\mathbb{R}^*$ is abelian so $(xy)^2 = x^2 y^2 \in \mathbb{Q}$.

  so $xy \in H$.

  Inverse: $x \in H \Rightarrow x^2 \in \mathbb{Q}$

  Now $(x^{-1})^2 = (x^2)^{-1} \in \mathbb{Q}$ since $(p/q)^{-1} = q/p$

  so $x^{-1} \in H$.

- yes, 2 can be replaced w/ any pos int.

67) $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in \mathbb{Z} \right\}$ under +

$H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G \middle| a+b+c+d = 0 \right\}$

- Show H subgrp

$*$ $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in H$ so $H \neq \emptyset$

- Closure: $\underbrace{\begin{bmatrix} a & b \\ c & d \end{bmatrix}}_{\in H} + \underbrace{\begin{bmatrix} f & g \\ h & i \end{bmatrix}}_{\in H} = \begin{bmatrix} a+f & b+g \\ c+h & d+i \end{bmatrix} \in H$ since

  $(a+f) + (b+g) + (c+h) + (d+i) = (a+b+c+d) + (f+g+h+i) = 0 + 0 = 0$

- Inverse: $-\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \in H$ since $-a + -b + -c + -d = -(a+b+c+d) = -(0) = 0$.

- No if $0 = 1$ since you won't get closure (sum of two will be 2)

  or identity since $0 \neq 1$.

71) $G = GL(2, \mathbb{R})$

$H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| \; a, b \in \mathbb{Z}_{\neq 0} \right\}$

Is H a subgrp?

$A, C \in H \Rightarrow \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix}$, $ac \neq 0$ and $bd \neq 0$ since $a, b, c, d \neq 0$.

so closed.

$A^{-1} = \begin{bmatrix} 1/a & 0 \\ 0 & 1/b \end{bmatrix}$ since $AA^{-1} = I = A^{-1}A$. Further $A^{-1} \notin H$ since $\frac{1}{a}$ and $\frac{1}{b}$ might not be in $\mathbb{Z}$.

79) $G = GL(2, \mathbb{R})$

a) $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} a+b & a \\ c+d & c \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ a & b \end{bmatrix}$

so $a+b = a+c$, $a = b+d$, $c+d = a$, $c = b$

$\Rightarrow b = c$ $\quad$ $b+d = a$

so $\left\{ \begin{bmatrix} b+d & b \\ b & d \end{bmatrix} \in G \right\}$

b) $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$

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

$\Rightarrow b = c, \; a = d$

so $\left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \in G \middle| \; a^2 - b^2 \neq 0 \right\}$

c) $Z(G)$

By above, $a = d$, $b = c$, and $a = b+d$

$\Rightarrow d = b + d$

$\Rightarrow b = 0 \Rightarrow c = 0$

so $\left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \middle| \; a^2 \neq 0 \right\}$ i.e. $a \neq 0$

$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}\begin{bmatrix} b & c \\ f & g \end{bmatrix} = \begin{bmatrix} ab & ac \\ af & ag \end{bmatrix}$

$\begin{bmatrix} b & c \\ f & g \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} ab & ac \\ af & ag \end{bmatrix}$

So $\left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \right\} \subseteq Z(G)$