Problem 10.B.2

$6^n = 6 + 6 + \cdots + 6 \bmod 16 = 6n \bmod 16$ where $6^n = e = 0$ if and only if $6^n = 0 \bmod 16$

$\text{ord}(6)$ is the smallest integer such that $6n$ is divisible by 16.

$lcm(6,16) = 48 = 6 \times 8 \Rightarrow \textbf{ord}(\mathbf{6}) = \mathbf{8}$ **(in $\mathbb{Z}_{16}$)**

Problem 10.B.3

$$f(x) = \frac{2}{2-x} \Rightarrow f(f(x)) = \frac{2}{2 - \frac{2}{2-x}} = \frac{2-x}{1-x} \Rightarrow f\left(f(f(x))\right) = \frac{2 - \frac{2}{2-x}}{1 - \frac{2}{2-x}} = \frac{2(x-1)}{x}$$

$$\Rightarrow f\left(f\left(f(f(x))\right)\right) = \frac{2\left(\frac{2}{2-x} - 1\right)}{\frac{2}{2-x}} = x \Rightarrow \text{ord}(f(x)) = 4 \text{ in } S_A$$

3|3

Problem 10.C.6

Suppose that $\text{ord}(ab) = n$, then $(ab)^n = e$ where $e =$ identity element of G

$(ab)(ab)^{n-1} = (ab)^n = e = b^{-1}a^{-1}$

$(ba)^n = (ba)(ba) \ldots (ba) = b(ab)(ab) \ldots (ab)a = b(ab)^{n-1}a = b(b^{-1}a^{-1})a = e$

Thus, $(ab)^n = (ba)^n = e \Rightarrow \textbf{ord}(\boldsymbol{ab}) = \textbf{ord}(\boldsymbol{ba}) = \boldsymbol{n}$

Problem 10.D.1

Suppose that $|a| = n < p$, then $a^n = e$

$$\begin{cases} a^{3n+1} = a^{2n+1} = a^{n+1} \neq e \\ \quad a^{3n} = a^{2n} = a^n = e \\ a^{2n-1} = a^{2n-1} = a^{n-1} \neq e \end{cases} \Rightarrow a^k = e \text{ if and only if } k \text{ is a multiple of } n$$

However, *p* is a prime number thus cannot be a multiple of *n*.

Thus, *p* must be the order of *a*.

3|3

Problem 10.D.2

$$\begin{cases} a^{\text{ord}(a)} = e \\ \left(a^{\text{ord}(a)}\right)^k = e^k = e \Rightarrow \text{ord}(a^k) \mid \text{ord}(a) \\ a^{k \cdot \text{ord}(a)} = e \end{cases}$$

Problem 10.D.3

$$e = a^{km} = \left(a^k\right)^m \Rightarrow \text{ord}\left(a^k\right) \mid m$$

$$\text{Let } x = \text{ord}\left(a^k\right) \Rightarrow \left(a^k\right)^x = a^{kx} = e \Rightarrow \text{ord}(a) \mid kx$$

$$\begin{cases} \text{ord}(a) = km \\ x = \text{ord}\left(a^k\right) \end{cases} \Rightarrow \begin{cases} km \mid k \cdot \text{ord}\left(a^k\right) \\ m \mid \text{ord}\left(a^k\right) \end{cases} \Rightarrow \text{ord}\left(a^k\right) = m$$

Problem 10.D.5

Let $\text{ord}(a) = n$

$a^r = a^s \Rightarrow \dfrac{a^r}{a^s} = e \Rightarrow a^{r-s} = e \Rightarrow \text{ord}(a) | r - s| \Rightarrow n|r - s$ 3/3

Problem 11.A.2

$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 2 & 5 & 4 \end{pmatrix} \Rightarrow f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 1 & 5 & 2 \end{pmatrix} \Rightarrow f^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 5 & 1 \end{pmatrix}$

$\Rightarrow f^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = e$

$\Rightarrow \langle f \rangle = \{e, f, f^2, f^3\}$

Problem 11.A.3

$\left\langle \frac{1}{2} \right\rangle$ in $\mathrm{R}^* = \left\{ \left(\frac{1}{2}\right)^n : n \in \mathbb{Z} \right\} = \left\{ \dots \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16 \right\} \cdots$

$\left\langle \frac{1}{2} \right\rangle$ in $\mathrm{R} = \left\{ \frac{1}{2} n : n \in \mathbb{Z} \right\} = \left\{ \dots -1, -\frac{1}{2}, 0, \frac{1}{2}, 1, \dots \right\}$ 2/2

Problem 11.B.3

Let $G = \langle a \rangle$ and $b \in G \Rightarrow \begin{cases} G = \{a^n | \, n \in \mathbb{Z}\} \\ \exists\, m \in \mathbb{Z} \text{ such that } b = a^m \end{cases}$

Let p be the order of a and q be the order of $b \Rightarrow \begin{cases} a^p = e \\ b^p = e \end{cases} \Rightarrow a^p = b^q \Rightarrow a^p = (a^m)^q = a^{mq}$

$\Rightarrow p = mq \Rightarrow q = \dfrac{p}{m} \Rightarrow q$ is a factor of $p \Rightarrow$ the order of b is a factor of a 3/3

Problem 11.B.4

Let G be a cyclic group of order n and $G = \langle a \rangle$ where $a^n = e$ and $a^k \neq e \; \forall \, k \in \{1, 2, \dots, n-1\}$
$\Rightarrow \text{ord}(a) = n$
Let k be any integer divides n, thus $\exists \, w \in \mathbb{N}$ such that $n = kw$
If p is any integer such that $(a^w)^p = a^{wp} = e$, since $a^k \neq e \; \forall \, k \in \{1, 2, \dots, n-1\}$,
then $wp \geq n \Rightarrow p \geq k$ where $(a^w)^k = a^{wk} = a^n = e$
$\Rightarrow k$ is the smallest positive value of m such that $(a^w)^m = e \Rightarrow \text{ord}(a^w) = k$
Hence, there are elements of order k for every integer k which divides n.

Problem 11.E.2

Let $G \times H = \{(a, b) \mid a \in G, b \in H\}$ as $G \times H$ is a cyclic group.
$\exists \, (x, y) \in G \times H$ such that $(x, y)^n = (e_x, e_y) = (x^n, y^n)$ 3/3
$\exists \, x \in G$ and $y \in H$ such that $x^n = e_x$ and $y^n = e_y$
Let (x_1, e_y) be an element of $G \times H \Rightarrow (x_1, e_y) = (x, y)^n = (x^n, y^n)$ for some integer n
Then $x_1 = x^n \Rightarrow x$ is a generator of $G \Rightarrow G$ is cyclic
Let (e_x, y_1) be an element of $G \times H \Rightarrow (e_x, y_1) = (x, y)^n = (x^n, y^n)$ for some integer n
Then $y_1 = y^n \Rightarrow y$ is a generator of $H \Rightarrow H$ is cyclic

Problem 11.E.3

Claim that $G \times H$ is not always a cyclic group even if G and H are both cyclic.

Take $G = \mathbb{Z}_2$ and $H = \mathbb{Z}_2$ such that G and H are both under addition operation

Therefore, $\langle 1 \rangle$ generates G and H where G and H are both cyclic.

However, $G \times H = \{(0,0), (0,1), (1,0), (1,1)\}$ where order of the elements in $G \times H$ are $\{1,2,2,2\}$, respectively. There is no single element that can generates $G \times H$ which indicates that $G \times H$ is not cyclic.

Problem 11.E.4

Let $(a, b) \in G \times H$ where $\text{ord}(a) = m$ and $\text{ord}(b) = n$

$(a, b)^n = (a^n, b^n) = (e_a, e_b)$ 3/3

$\Rightarrow \text{ord}(a) \mid n$ and $\text{ord}(b) \mid n$

$\Rightarrow n$ is a common multiple of $\text{ord}(a)$ and $\text{ord}(b)$

$\Rightarrow$ The order of (a, b) is the least ommon multiple of $\text{ord}(a)$ and $\text{ord}(b)$

$16 / \gcd(16.6) = 16/2 = 8$

$f^2 = \frac{2}{2-\frac{2}{2-x}} = \frac{4-2x}{4-2x-2} = \frac{2-x}{1-x} = 1+\frac{1}{1-x}$

$f^3 = 1+\frac{1}{1-\frac{2}{2-x}} = 1+\frac{2-x}{2-x-2} = 1+\frac{x-2}{x} = \frac{2x-2}{x}$

$f^4 = \frac{2\frac{2}{2-x}-2}{\frac{2}{2-x}} = \frac{4-4+2x}{2} = x$

thus the order is 4. 2/2

18/20

suppose order of ab is n, then $(ab)^n = e$, $a(ba)^{n-1}b = e$

then $(ba)^{n-1} = a^{-1}eb^{-1} = a^{-1}b^{-1} = (ba)^{-1}$

multiply ba on both side, $(ba)^n = e$.

suppose a does not have order p, suppose it has order K. then $K < p$ and $a^K = e$.
because p is prime, their gcd is 1, suppose $p \div K = x \cdots y$. clearly reminder y is between 0 and K. because why? $a^p = a^K = e$, $a^y = a^{p-xK} = a^p(a^{-K})^x = e$, since $y < K$ and $a^y = e$
K is not the order of a, get a contradiction. 3/3

suppose order of a^K is x and order of a is y. If x is not a factor of y.
$\gcd(x.y) < x$. let $t = \gcd(x.y)$. then $\frac{xy}{t}$ is a multiple of x and y, and $a^{\frac{xy}{t}} = e$.
then $a^t = a^{xy-(t-1)\frac{xy}{t}} = (a^{xy})(a^{\frac{xy}{t}})^{1-t} = e \cdot e^{1-t} = e$
Since $t < x$, $a^t = e$, x is not the order of a^K, get a contradiction.

this cannot be proved. order of a is $K \cdot m$, if $K < 0$ and $m < 0$,
order of a^K is $-m$ instead of m. I will prove this with condition $K > 0$.
since $K > 0$, $m > 0$, suppose order of a^K is t instead of m, then $a^{Kt} = e$ and $t <$
$\because t < m$, $K > 0$, $Kt < Km$, $a^{Kt} = e$, order of a should be Kt instead of Km.

suppose n is not a factor of $r-s$, $\gcd(n, r-s) < n$. suppose $t = \gcd(n, r-s)$, $t < n$.
then $\frac{n(r-s)}{t}$ is a multiple of n and $r-s$, and $a^{\frac{n(r-s)}{t}} = e$.
then $a^t = a^{n(r-s)-(t-1)\frac{n(r-s)}{t}} = a^{n(r-s)}(a^{\frac{n(r-s)}{t}})^{1-t} = e \cdot e^{1-t} = e$ 3/3
since $t < n$, $a^t = e$, the order of a is not n. get a contradiction.

1	2	3	4	5	6
6	1	3	2	5	4
4	6	3	1	5	2
2	4	3	6	5	1
1	2	3	4	5	6

it should be: e, (6421), $(41)(62)$, (2461)

3 $\{x \mid x = 2^K, K \in \mathbb{Z}\}$ $\{x \mid x = \frac{K}{2}, K \in \mathbb{Z}\}$ ∝ 1/2 need to specify them!

if $b \in G$, $b = a^K$ where $K \in \mathbb{Z}$. this is the same as chapter 10, D_2 above. 3/3

suppose $G = \langle a \rangle$ has order n, then $\forall K$ divides n, let $t = \frac{n}{K}$ and $t \in \mathbb{Z}$, $K, t > 0$.
then $a^{tK} = a^n = e$. if order of a^t is not K, suppose it is x, then $x < K$, $x > 0$.
then $a^{tx} = e = a^n = a^{tK}$, since $tx < n$, order of a should be tx instead of n,
get a contradictory, thus the order of a^K must be K.
thus $\forall K$, the order of $a^{\frac{n}{K}} = K$.

let $G' = \{(a.e_H) \mid a \in G\}$ where e_H is the identity of H. why? need details
obviously, G' is a subgroup of $G \times H$, and obviously it is isomorphic to G. 2/3
since subgroup of cyclic group is cyclic, G' is cyclic, then G is cyclic.

$\mathbb{Z}_2 \times \mathbb{Z}_2$,

	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

since each element a has $a^2 = e$,
it is not possible to obtain $\mathbb{Z}_2 \times \mathbb{Z}_2$ by any $\langle a \rangle$.

$(a,b)^K = (a^K . b^K)$, suppose $(a.b)^K = (e.e)$, then $a^K = e$ and $b^K = e$,
then K must be a multiple of both n and m. 3/3
if $(a.b)$ has order K, of course K has to be the least one. which is $\mathrm{lcm}(m.n)$