Ch 2 #9-11, 13, 16, 18, 21, 23, 25-27, 32-34, 46, 48

9) $(\{1,2,3\}, \times \bmod 4)$ is not a group b/c 2 does not have an inverse.

since $2\cdot1=2$, $2\cdot2=0$, $2\cdot3=2$

$(\{1,2,3,4\}, \times \bmod 5)$

- assoc. is inherited
- identity is $e=1$ since $1\cdot a=a=a\cdot1$ $\forall a\in\{1,2,3,4\}$
- closure :

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

- inverses : $1^{-1}=1$, $2^{-1}=3$, $3^{-1}=2$, $4^{-1}=4$

10) $A=\begin{bmatrix}1&0\\2&3\end{bmatrix}$ $B=\begin{bmatrix}1&2\\0&3\end{bmatrix}$

$AB=\begin{bmatrix}1&2\\2&4\end{bmatrix} \neq BA=\begin{bmatrix}5&6\\6&9\end{bmatrix}$

11) $GL(2,\mathbb{Z}_{11})$

$$\boxed{\begin{bmatrix}2&6\\3&5\end{bmatrix}^{-1}=\begin{bmatrix}9&9\\10&8\end{bmatrix}}$$

$$\frac{1}{\det A}\begin{bmatrix}d&-b\\-c&a\end{bmatrix}=\frac{1}{-8}\begin{bmatrix}5&-6\\-3&2\end{bmatrix}=\frac{1}{3}\begin{bmatrix}5&5\\8&2\end{bmatrix}=4\begin{bmatrix}5&5\\8&2\end{bmatrix}=\begin{bmatrix}20&20\\32&8\end{bmatrix}=\begin{bmatrix}9&9\\10&8\end{bmatrix}$$

$3(4)=1$
$\Rightarrow 4=\frac{1}{3}$

13) a) $a^2b^3 \rightarrow 2a+3b$

b) $a^{-2}(b^{-1}c)^2 \Rightarrow -2a+2(-b+c)$

c) $(ab^2)^{-3}c^2 = e \longrightarrow -3(a+2b)+2c = \underset{=0}{e}$

16) $(\{5, 15, 25, 35\},\ x \bmod 40)$

x mod 40	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

$e = 25$

$5^{-1} = 5,\ 15^{-1} = 15,\ 25^{-1} = 25,\ 35^{-1} = 35$

$U(8) = \{1, 3, 5, 7\}$

x mod 8	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$U(8)$ is the same except that the identity is not $25/5$ but is 1.

18) $H = \{x^2 \mid x \in D_4\}$

$= \{e, r_{180}\}$

$K = \{x \in D_4 \mid x^2 = e\}$

$= \{e, f, fr, fr^2, fr^3, r^2\}$

21) x mod 91 $\{1, 9, 16, 22, 53, 74, 79, 81, x\}$

	1	9	16	22	53	74	79	81
1	1	9	16	22	53	74	79	81
9	9	81	53	16	22	29		
16								

29

23) Let G be an Abelian grp and $a, b \in G$, Let $n \in \mathbb{Z}$.

$\underline{n>0}$ $(ab)^n = \underbrace{ababab\ldots ab}_{n\text{-pairs}}$ (*) could do this with induction

$= \underbrace{aa\ldots a}_{n\text{-times}}\underbrace{bb\ldots b}_{n\text{-times}}$ since G is abelian

$= a^n b^n$

This is not true for non-Abelian grps.

$\underline{n=0}$

$(ab)^0 = 1 = 1 \cdot 1$

$= a^0 b^0$

$\underline{n<0}$

$(ab)^n (ab)^{-n} = e$

$\Rightarrow (ab)^n a^{-n} b^{-n} = e$ since $-n>0$

$\Rightarrow (ab)^n = b^n a^n$

$= a^n b^n$ b/c Abelian

25) G grp Abelian iff $(ab)^{-1} = a^{-1}b^{-1}$ $\forall a,b \in G$

(G abelian) $\Rightarrow \forall a,b \in G$, $(ab) = (ba) \Leftrightarrow a^{-1}b^{-1} = b^{-1}a^{-1}$ since $a^{-1}, b^{-1} \in G$

$\Leftrightarrow a^{-1}b^{-1} = (ab)^{-1}$ by socks-shoes prop.

26) G grp, $a \in G$

$a^{-1}(a^{-1})^{-1} = e$ by def. $\Rightarrow aa^{-1}(a^{-1})^{-1} = ae \Rightarrow (a^{-1})^{-1} = a$.

27) G grp, $a,b \in G$, $n \in \mathbb{Z}$

If $\underline{n=0}$, $(a^{-1}ba)^0 = 1 = a^{-1}a = a^{-1}b^0 a$ so works

$\underline{n>0}$ $(a^{-1}ba)^n = \underbrace{(a^{-1}ba)(a^{-1}ba)(a^{-1}ba)\cdots(a^{-1}ba)}_{n\text{-times}}$

$= a^{-1}b(aa^{-1})b(aa^{-1})b(aa^{-1})\cdots(aa^{-1})ba$ by assoc.

$= a^{-1}bebeb\ldots eba$

$= a^{-1}\underbrace{bb\ldots b}_{n\text{-times}}a$

$= a^{-1}b^n a$

$\underline{n<0}$

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

$= (a^{-1}ba)^n a^{-1}b^{-n}a$ since $-n>0$

$\Rightarrow a^{-1}b^n a = (a^{-1}ba)^n$

multiplying on the right by a^{-1} then b^n then a.

3a) $U(12) = \{1, 5, 7, 11\}$

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

33)

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

34) G grp, $a,b \in G$.

$(ab)^2 = a^2 b^2 \iff abab = aabb$

$\iff bab = abb$ $\quad \times\, a^{-1}$ on left $\quad \times\, a$ on right

$\iff ba = ab$ $\quad \times\, b^{-1}$ on right $\quad \times\, b$ on right

46) $G = \{3^m 6^n \mid m,n \in \mathbb{Z}\} \subseteq \mathbb{Q}$. Show G grp.

- Assoc. inherited by $\mathbb{Q}$.
- $e = 1 = 3^0 6^0$ since $a(3^0 6^0) = (3^0 6^0)a = a \quad \forall a \in G$
- Closed: Let $3^m 6^n,\ 3^s 6^t \in \mathbb{Q}$.

  $(3^m 6^n)(3^s 6^t) = 3^m 3^s 6^n 6^t = 3^{m+s} 6^{n+t} \in G$ since $m+s, n+t \in \mathbb{Z}$
- Inverses: $(3^m 6^n)^{-1} = 3^{-m} 6^{-n}$ since

  $(3^m 6^n)(3^{-m} 6^{-n}) = 3^{m-m} 6^{n-n} = 3^0 6^0 = e$

  and $(3^{-m} 6^{-n})(3^m 6^n) = 3^{m-m} 6^{n-n} = 3^0 6^0 = e$

48) $H = \left(\left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| \, a,b,c \in \mathbb{R} \right\}, \times \right)$

• Associativity:

Let $A, D, J \in H$. Then:

$$A(DJ) = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \left(\begin{bmatrix} 1 & d & f \\ 0 & 1 & g \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & j & k \\ 0 & 1 & l \\ 0 & 0 & 1 \end{bmatrix} \right) = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & j+d & k+dl+f \\ 0 & 1 & l+g \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & j+d+a & k+dl+f+al+ag+b \\ 0 & 1 & l+g+c \\ 0 & 0 & 1 \end{bmatrix}$$

and

$$(AD)J = \left(\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & d & f \\ 0 & 1 & g \\ 0 & 0 & 1 \end{bmatrix} \right) \left(\begin{bmatrix} 1 & j & k \\ 0 & 1 & l \\ 0 & 0 & 1 \end{bmatrix} \right) = \begin{bmatrix} 1 & d+a & f+ag+b \\ 0 & 1 & g+c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & j & k \\ 0 & 1 & l \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & j+d+a & k+ld+la+f+ag+b \\ 0 & 1 & l+g+c \\ 0 & 0 & 1 \end{bmatrix}$$

Since addition on $\mathbb{R}$ is commutative, $A(DJ) = (AD)J$ $\forall A, D, J \in T$ so $\times$ is associative

• Closure

$$AD = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & d & f \\ 0 & 1 & g \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & d+a & f+ag+b \\ 0 & 1 & g+c \\ 0 & 0 & 1 \end{bmatrix}$$

Since $+$ on $\mathbb{R}$ is closed, all entries of AD are real so $AD \in H$ and H is closed

• Identity. I claim $I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ is e.

$$AI = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = A \quad \text{and}$$

$$IA = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = A \quad \text{so } I \text{ is the identity}$$

Moreover, I is of the correct form so $I \in H$.

• Inverses To find A^{-1}, $d+a=0 \Rightarrow d=-a$, $g+c=0 \Rightarrow g=-c$,
$f+ag+b=0 \Rightarrow f+-ac+b=0 \Rightarrow f=ac-b$.

con →

' Claim $A^{-1} = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}$

$$AA^{-1} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -a+a & ac-b-ac+b \\ 0 & 1 & -c+c \\ 0 & 0 & 1 \end{bmatrix} = I$$

and

$$A^{-1}A = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a-a & b-ac+ac-b \\ 0 & 1 & c-c \\ 0 & 0 & 1 \end{bmatrix} = I$$

Since $AA^{-1} = I = A^{-1}A$, A^{-1} is the inverse of A. Moreover A^{-1} is of the form to be in H.

$\therefore$ H is a group