3.23 Show that $\mathbb{Z}_6$ under addition is isomorphic to $\mathbb{Z}_7^*$ under addition

	$\mathbb{Z}_6$	$\mathbb{Z}_7^*$
the unit	0	1
a generator	1	3

Consider the map $T: \mathbb{Z}_6 \to \mathbb{Z}_7^*$

$1 \mapsto 3$

extended by $T(n) = T(\underbrace{1+\cdots+1}_{n\text{-times}}) = T(1)^n = 3^n$

n	T(n)
0	1
1	3
2	2
3	6
4	4
5	5

Check that T is 1-1 and surjective

By Construction it is a group homomorphism

3.2.5a) Show that if T is a group isomorphism so is T^{-1}

Since T is 1-1 and surjective T^{-1} is also 1-1 and surjective. Remains to show that T^{-1} is a group homomorphism

$$T\left(T^{-1}(ab)\right) = ab$$

$$T\left(T^{-1}(a)\,T^{-1}(b)\right) = T\left(T^{-1}(a)\right)T\left(T^{-1}(b)\right) = ab$$

↑ T is a group homomorphism

So $T\left(T^{-1}(a)\,T^{-1}(b)\right) = T\left(T^{-1}(ab)\right)$

$\Rightarrow T^{-1}(a)\,T^{-1}(b) = T^{-1}(ab)$ since T is 1-1

Hence T^{-1} is a group homomorphism

3.2.5 b) Suppose $T: G \to H$ and $S: H \to K$ are group homomorphisms

Show $S \circ T: G \to K$ is a group homomorphism.

We know from facts on functions that $S \circ T$ is 'onto' and 1-1. Short proof:

Let $k \in K$, then $\exists h \in H$ s.t. $S(h) = k$ and

$\exists g \in G$ s.t. $T(g) = h$.

then $S \circ T(g) = S(h) = k$ so $S \circ T$ is onto

Assume $S \circ T(g) = S \circ T(g')$, since S is 1-1

we have $T(g) = T(g')$. Since T is 1-1 $g = g'$

Hence $S \circ T$ is 1-1.

Finally we check that $S \circ T$ is a group homomorphism:

$$S \circ T(ab) = S(T(ab)) = S(T(a)T(b)) = S(T(a))\,S(T(b))$$

(T is a group homomorphism; S is a group homomorphism)

$$= S \circ T(a)\, S \circ T(b)$$

3.2.7 See ~~textbook~~ for problem statement

Fix notation $id = g_1$ $(23) = g_4$

$(12) = g_2$ $(123) = g_5$

$(13) = g_3$ $(132) = g_6$

a	$\sigma(a)$
id	$\begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 \\ g_1 & g_2 & g_3 & g_4 & g_5 & g_6 \end{pmatrix}$
(12)	$\begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 \\ g_2 & g_1 & g_6 & g_5 & g_4 & g_3 \end{pmatrix}$ Keep computations: $(12)(13) = (132)$ $(12)(23) = (123)$
(13)	$\begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 \\ g_3 & g_5 & g_1 & g_6 & g_2 & g_4 \end{pmatrix}$
(23)	$\begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 \\ g_4 & g_5 & g_6 & g_1 & g_2 & g_3 \end{pmatrix}$
(123)	$\begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 \\ g_5 & g_4 & g_2 & g_3 & g_6 & g_1 \end{pmatrix}$
(132)	$\begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 \\ g_6 & g_3 & g_4 & g_2 & g_1 & g_5 \end{pmatrix}$

Trick: The order of a and $\sigma(a)$ are equal

3.2.9 Consider $\mathbb{Z}_5$ under addition with elements $[1], [2], \ldots, [5]$

Find the permutations of S_5 coming from Cayley's theorem

$[1] \rightsquigarrow (12345)$

$[2] \rightsquigarrow (13524)$

$[3] \rightsquigarrow (14253)$

$[4] \rightsquigarrow (15432)$

$[5] \rightsquigarrow id$

3.2.17 State whether the following statements are true or false

a) The groups S_4 and D_{12} are isomorphic

False D_{12} has an element of order 12

S_4 has no element of order greater than 4

b) $f: \mathbb{Z} \to \mathbb{Z}$, $f(x) = 2x$ is a group isomorphism

False f is not surjective

c) $\mathbb{Z}$ and $\mathbb{Q}$ are isomorphic (under addition)

False

$\mathbb{Q}$ is divisible for any $q \in \mathbb{Q}$, $m \in \mathbb{Z}$, there is an $r \in \mathbb{Q}$ s.t. $m \cdot r = q$

$\mathbb{Z}$ is not divisible, if $|n| < |m|$ no $k \in \mathbb{Z}$ such that $mk = n$

d) All infinite groups are isomorphic

False see problem c)

3.2.18 Show that $\mathrm{Aut}(\mathbb{Z}_n)$ is isomorphic to $\mathbb{Z}_n^*$

Hint, use $f(\sigma) = \sigma(1)$

$$f(\sigma\circ\tau) = \sigma\circ\tau(1) = \tau(\sigma(1)) = \tau(\overbrace{1+\cdots+1}^{\sigma(1)\text{ times}})$$

$$= \tau(1)+\cdots+\tau(1) = \sigma(1)\tau(1)$$

↑ τ is an automorphism of $\mathbb{Z}_n$ under addition

$$f(\sigma)f(\tau) = \sigma(1)\tau(1)$$

So f is a group homomorphism.

Furthermore f is 1-1 since if $\sigma(1) = \sigma'(1)$, then $\sigma = \sigma'$

($\mathbb{Z}_n$ is cyclic, so $\sigma(x) = \sigma(1)+\cdots+\sigma(1)$)

Finally $|\mathrm{Aut}(\mathbb{Z}_n)| = \phi(n) = |\mathbb{Z}_n^*|$, so f is onto

Since $\sigma \in \mathrm{Aut}(\mathbb{Z}_n)$ is defined by mapping 1 to a generator of $\mathbb{Z}_n$, and there are $\phi(n)$ choices of generators

3.3.1 Find all subgroups of $\mathbb{Z}_7^*, \mathbb{Z}_8^*, \mathbb{Z}_9^*, \mathbb{Z}_{10}^*$

$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$

$|\mathbb{Z}_7^*| = 6$, so we need to check for subgroups of order 0, 2, 3, 6

order 0: only the trivial group

order 6: only the entire group

order 2: Sub group generated by 6

order 3: Subgroups generated by 2 and by 4,

but $\langle 2 \rangle = \langle 4 \rangle$, so only one sub group

$\mathbb{Z}_8^* = \{1,3,5,7\}$

$|\mathbb{Z}_8^*| = \phi(8) = 4$. So any proper subgroup has order 2

The elements of order 2 are 3, 5, 7

So these generate 3 subgroups

$\mathbb{Z}_9^* = \{1,2,4,5,7,8\}$

$|\mathbb{Z}_9^*| = \phi(9) = 6$, Check for subgroups of order 2 and 3

$2^6 = 1$, $4^3 = 1$, $5^6 = 1$, $7^3 = 1$, $8^2 = 1$

So the subgroups are $\langle 4 \rangle, \langle 7 \rangle, \langle 8 \rangle$

3.3.7 $|\mathbb{Z}_{10}^*| = \phi(10) = 4$ $\mathbb{Z}_{10} = \{1, 3, 7, 9\}$

$3^4 = 1$, $7^4 = 1$, $9^2 = 1$

So the only proper subgroup is $\langle 9 \rangle$

3.3.2 Find all left cosets of the subgroup $H = \{1, 11 \pmod{20}\}$ in the multiplicative group $\mathbb{Z}_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$H = \{1, 11\}$ $\quad$ $11H = \{11, 1\}$

$3H = \{3, 13\}$ $\quad$ $13H = \{13, 3\}$

$7H = \{7, 17\}$ $\quad$ $17H = \{17, 7\}$

$9H = \{9, 19\}$ $\quad$ $19H = \{19, 9\}$

3.3.5 Find all normal subgroups of S_3

$$S_3 = \{id, R, R^2, F, FR, FR^2\}$$

The subgroups are $H_0 = \{id, R, R^2\}$

$$H_1 = \{id, F\}$$

$$H_2 = \{id, FR\}$$

$$H_3 = \{id, FR^2\}$$

$$FH_0F^{-1} = \{id, FRF, FR^2F\} = \{id, R^2, R\}$$

$$RH_0R^{-1} = \{id, RRR^2, RR^2R^2\} = \{id, R, R^2\}$$

Since F, R generate S_3, this proves that H_0 is normal

$$RH_1R^{-1} \{id, RFR^2\} = \{id, FR\}$$

So H_1 is not normal,

Similarly, H_2, H_3 are not normal

3.3.7 Show that if $H \subseteq G$ is a subgroup and $|G/H| = 2$ then H is normal.

Let $g \in G$, gH is either H or $G \setminus H$

Since $|gH| = |H|$, similarly Hg is either H or $G \setminus H$

If $g \in H$, $gH = Hg$

If $g \notin H$, ~~H~~ subgroup generated by g and H ~~must be all of G~~ since $\langle g, H \rangle \neq H$ ~~$H \neq \frac{|G|}{2}$~~ $\frac{|G|}{2}$

gH and Hg both contain $g \notin H$, so

gH and Hg must both be $G \setminus H$, hence equal.

Thus H is normal.