§2

2.1 (i) $\mathbb{Z}_2 \times \mathbb{Z}_2$

element	order
$(0,0)$	1
$(1,0)$	2
$(0,1)$	2
$(1,1)$	2

$\mathbb{Z}_2 \times \mathbb{Z}_3$

element	order
$(0,0)$	1
$(0,1)$	3
$(0,2)$	3
$(1,0)$	2
$(1,1)$	6
$(1,2)$	6

$\mathbb{Z}_2 \times S_3$

element	order	element	order
$(0,(1))$	1	$(1,(1))$	2
$(0,(123))$	3	$(1,(123))$	6
$(0,(132))$	3	$(1,(132))$	6
$(0,(12))$	2	$(1,(12))$	2
$(0,(13))$	2	$(1,(13))$	2
$(0,(23))$	2	$(1,(23))$	2

(ii) NO as $\mathbb{Z}_2 \times \mathbb{Z}_2$ has no elements of order 4, but $\mathbb{Z}_4$ does have elements of order 4.

(iii) YES $|\mathbb{Z}_2 \times \mathbb{Z}_3| = 6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ contains an element of order 6. So $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic. $\therefore \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$

(two finite cyclic groups of the same order must be isomorphic)

2.2

element	order
1	1
2	6
4	3
5	6
7	3
8	2

G is cyclic as $|G|=6$ and G contains an element of order 6.

2.3 (G1) Let $x, y \in G$ with $x * y = z$. So $xy \equiv z \pmod{n}$ with $z \in \{0, 1, \ldots, n-1\}$. Hence $xy - z = kn$, some $k \in \mathbb{Z}$. If $\mathrm{hcf}(n, z) > 1$, then $\exists$ prime p s.t. $p \mid n$ and $p \mid z$. $\therefore p \mid xy$. Since p is a prime, we deduce that either $p \mid x$ or $p \mid y$. But then either $\mathrm{hcf}(n, x) > 1$ or $\mathrm{hcf}(n, y) > 1$, contradicting $x, y \in G$. Hence $\mathrm{hcf}(n, z) = 1$ and so $z \in G$.

(G2) holds as multiplication modulo n is associative (see "An introduction to Mathematical Reasoning" by Peter J. Eccles).

(G3) $1 \in G$ and for $x \in G$, $x * 1 = x = 1 * x$.
So 1 is the identity element.

(G4) Let $x \in G$. By HINT $\exists\ \lambda, \mu \in \mathbb{Z}$ s.t. $\lambda x + \mu n = 1$. So $\lambda x \equiv 1 \pmod{n}$ (and note that $\lambda \not\equiv 0 \pmod{n}$). Let $y \in \{1, \ldots, n-1\}$ be s.t. $\lambda \equiv y \pmod{n}$. Then $yx \equiv 1 \pmod{n}$. Note that this means $\mathrm{hcf}(y,n)$ must divide 1. So $\mathrm{hcf}(y,n) = 1$. Thus $y * x = 1$ (and $x * y = 1$) with $y \in G$. $\therefore$ (G4) holds.

2.4 (i) $\det\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = 1$; order $= 3$.

(ii) $\det\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = 1$; order $= 3$.

(iii) $\det\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = 1.2 - 2.2 = 2 - 4 = -2 \equiv 1 \pmod{3}$; order $= 4$.

(iv) $\det\begin{pmatrix}1 & 2\\ 1 & 0\end{pmatrix} = 1.0 - 2.1 = -2 \equiv 1 \pmod 3$;

order $= 6$.

Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of G of order 2.

So $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2+bc & ab+bd \\ ac+dc & cb+d^2 \end{pmatrix}$

$\therefore$ $a^2+bc = 1 = cb+d^2$ and $ab+bd = 0 = ac+dc$.

Also $1 = \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad-bc$. (All arithmetic being done mod 3.)

Suppose $c \neq 0$. Since $(\mathbb{Z}_3, \oplus, \odot)$ is a field we may cancel c in $0 = ac+dc$ and get $a = -d$.

$a^2+bc=1$

$\therefore 1 = ad-bc = -a^2-bc = -(a^2+bc) = -1$

So $1 \equiv -1 \pmod 3 \Rightarrow 3 \mid 2$, impossible. $\therefore c = 0$.

A similar argument gives $b = 0$.

So $1 = ad$. By checking possibilities in $\mathbb{Z}_3$ either $a = 1 = d$ or $a = 2 = d$. Since g has order 2 we must have $g = \begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$. $\therefore \begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$ is the only element of G of order 2.

2.5 We have q^n n-tuples with entries from F (F a finite field with q elements).

So q^n possibilities for each of the rows of a matrix $A \in GL(n,q)$.

For the first row of A there are $q^n - 1$ possibilities ($(0,0,\ldots,0)$ isn't allowed as we require the rows of A to be linearly independent).

If $(a_{11}, a_{12}, \ldots, a_{1n})$ is the first row of A, then the second row cannot be of the form $\lambda(a_{11}, a_{12}, \ldots, a_{1n})$ for any $\lambda \in F$. $\therefore$ $q^n - q$ possibilities for the second row of A.

If $(a_{21}, a_{22}, \ldots, a_{2n})$ is the second row of A, then the third row cannot be of the form

$$\lambda(a_{11}, a_{12}, \ldots, a_{1n}) + \mu(a_{21}, a_{22}, \ldots, a_{2n})$$

for any $\lambda, \mu \in F$.

$\therefore$ $q^n - q^2$ possibilities for the third row of A. Continuing gives

$$|GL(n,q)| = (q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{n-1}).$$

2.6 Since $\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix} = \begin{pmatrix}1&0\\0&1\end{pmatrix}$, we see that $H = \left\langle \begin{pmatrix}0&1\\1&0\end{pmatrix} \right\rangle$ and so $H \leq G$.

There are 4 right cosets of H in G:-

$$\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}\right\} (=H) \quad \left\{\begin{pmatrix}\lambda&0\\0&1/\lambda\end{pmatrix}, \begin{pmatrix}0&1/\lambda\\\lambda&0\end{pmatrix}\right\}$$

$$\left\{\begin{pmatrix}\lambda^2&0\\0&1/\lambda^2\end{pmatrix}, \begin{pmatrix}0&1/\lambda^2\\\lambda^2&0\end{pmatrix}\right\} \quad \left\{\begin{pmatrix}\lambda^3&0\\0&1/\lambda^3\end{pmatrix}, \begin{pmatrix}0&1/\lambda^3\\\lambda^3&0\end{pmatrix}\right\}$$

2.7 (i) $(1376)(2548) = (13)(17)(16)(25)(24)(28)$

even permutation

(ii) $(12473)(58)(6) = (12)(14)(17)(13)(58)$

odd permutation

(iii) $(18)(256374) = (18)(25)(26)(23)(27)(24)$

even permutation

(iv) $(1)(274)(3)(586) = (27)(24)(58)(56)$

even permutation.

2.8 Multiplication table just for elements of H:-

	(1)	$(12)(34)$	$(13)(24)$	$(14)(23)$
(1)	(1)	$(12)(34)$	$(13)(24)$	$(14)(23)$
$(12)(34)$	$(12)(34)$	(1)	$(14)(23)$	$(13)(24)$
$(13)(24)$	$(13)(24)$	$(14)(23)$	(1)	$(12)(34)$
$(14)(23)$	$(14)(23)$	$(13)(24)$	$(12)(34)$	(1)

(Note $\forall\, x \in H$, $x^{-1} = x$)

$H \leq G$ by the subgroup criterion.

2.9 Let $\sigma \in S_n$ be an odd permutation. Then $\sigma(12)$ is an even permutation. That is $\sigma(12) = \mu \in A_n$. So $\sigma = \mu(12) \in A_n(12)$.

$\therefore$ all odd permutations of S_n are in $A_n(12)$

$\therefore$ $S_n = A_n \cup A_n(12)$, whence $[S_n : A_n] = 2$.

By Lagrange's theorem (Thm 1.6(i)) and Theorem 1.7(ii) $|A_n| = n!/2$.

2.10 (1), $(12)(34)$, $(13)(24)$, $(14)(23)$, (123), (132), (124), (142), (134), (143), (234), (243)