## MA103

## Solutions

## Question 1

(a) We are dealing with three statements $p, q, r$, each of which can be true ("T") or false ("F"). Using the simple truth tables for $a \vee b$ and $a \Rightarrow b$, we get the following truth table, showing both $(p \Rightarrow r) \vee(q \Rightarrow r)$ and $(p \vee q) \Rightarrow r$ :

| $p$ | $q$ | $r$ | $p \Rightarrow r$ | $q \Rightarrow r$ | $(p \Rightarrow r) \vee(q \Rightarrow r)$ | $p \vee q$ | $(p \vee q) \Rightarrow r$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| T | T | T | T | T | T | T | T |
| T | T | F | F | F | F | T | F |
| T | F | T | T | T | T | T | T |
| T | F | F | F | T | T | T | F |
| F | T | T | T | T | T | T | T |
| F | T | F | T | F | T | T | F |
| F | F | T | T | T | T | F | T |
| F | F | F | T | T | T | F | T |

We see that there are two lines in which the truth values for $(p \Rightarrow r) \vee(q \Rightarrow r)$ and $(p \vee q) \Rightarrow r$ differ, which means that the two statements are not logically equivalent.
[ $4+2$ pts, Standard question]
(b) Since $S_{1}=1$ and $S_{2}=2$, the statement is true for $n=1$ and $n=2$.

Now suppose that the statement is true for all $n \leq k$, for some $k \geq 2$, and consider the number $S_{k+1}$. Since $k+1 \geq 3$, we know that $S_{k+1}=2 S_{k}+S_{k-1}-2$.
Now if $k+1$ is even, then $k$ is odd and $k-1$ is even, and hence by the induction hypothesis we have that $S_{k}$ is odd and $S_{k-1}$ is even. This means that $2 S_{k}+S_{k-1}-2$ is even ("two times odd plus even minus even" is even).
And if $k+1$ is odd, then $k$ is even and $k-1$ is odd, and hence by the induction hypothesis we have that $S_{k}$ is even and $S_{k-1}$ is odd. This means that $2 S_{k}+S_{k-1}-2$ is odd ("two times even plus odd minus even" is odd).
We have shown that the statement is true for $n=k+1$.
By the Principle of Induction, we can can conclude that $P(n)$ is true for all $n \in \mathbb{N}$. [8 pts, Similar to many questions, although more involved than most seen]
(c) (i) If $z=R e^{i \theta}$, then $z^{2}=R^{2} e^{2 i \theta}$ and $2 \bar{z}=2 R e^{-i \theta}$. So to have $z^{2}=2 \bar{z}$ we must have $R^{2}=2 R$ and $e^{2 i \theta}=e^{-i \theta}$.
Since $R^{2}=2 R$ is equivalent to $R(R-2)=0$, we have $R=0$ or $R=2$.
And to have $e^{2 i \theta}=e^{-i \theta}$, we must have that $2 \theta$ and $-\theta$ differ by a multiple of $2 \pi$. So we have $2 \theta=-\theta+2 k \pi$ for some integer $k$, while we also want that $0 \leq \theta<2 \pi$. This gives $3 \theta=2 k \pi$. If $k=0$, then we get $\theta=0$; if $k=1$, then we get $\theta=\frac{2}{3} \pi$; and if $k=2$, then we get $\theta=\frac{4}{3} \pi$. For all other values of $k$, we don't find $0 \leq \theta<2 \pi$.
Combining it all, if $R=0$, then we have the one solution $z=0$. And if $R=2$, then we have $z=2 e^{0 i}=2, z=2 e^{2 i \pi / 3}$ and $z=2 e^{4 i \pi / 3}$. [8 pts, Unseen]
(ii) We can write $0=0+0 i$ and $2=2+0 i$. For the other two solutions we find

$$
\begin{aligned}
& 2 e^{2 i \pi / 3}=2\left(\cos \left(\frac{2}{3} \pi\right)+i \sin \left(\frac{2}{3} \pi\right)\right)=2\left(-\frac{1}{2}+i \frac{1}{2} \sqrt{3}\right)=-1+i \sqrt{3}, \\
& 2 e^{4 i \pi / 3}=2\left(\cos \left(\frac{4}{3} \pi\right)+i \sin \left(\frac{4}{3} \pi\right)\right)=2\left(-\frac{1}{2}-i \frac{1}{2} \sqrt{3}\right)=-1-i \sqrt{3} .
\end{aligned}
$$

[3 pts, Standard]

## Question 2

(a) (i) We have that $d$ is a divisor of $m$ if there exists an integer $k$ such that $m=k \cdot d$.

The greatest common divisor $\operatorname{gcd}(m, n)$ of two integers $m, n$, not both zero, is the largest integer $d$ such that $d$ is a divisor of both $m$ and $n$.
[ $1+1$ pts, Bookwork]
(ii) Every integer is a divisor of 0 , since we have $0=0 \cdot d$ for every integer $d$. That means that if we would ask for common divisors of 0 and 0 , then we would have the set of all integers. Hence there would be no largest common divisor.
[3 pts, Discussed in lectures]
(iii) We first note that $\operatorname{gcd}(-51,141)=\operatorname{gcd}(141,51)$, and then start taking the steps in Euclid's algorithm as follows.

$$
\begin{aligned}
141 & =2 \times 51+39 \\
51 & =1 \times 39+12 \\
39 & =3 \times 12+3 \\
12 & =4 \times 3+0
\end{aligned}
$$

As the final line ends in 0 , we have found the greatest common divisor: $\operatorname{gcd}(-51,141)=$ $\operatorname{gcd}(141,51)=3$.
[4 pts, Standard]
(b) (i) If we have $x=0.0 \overline{119}$, then $1000 x=11.9 \overline{119}$. This means that $999 x=1000 x-x=$ $11.9 \overline{119}-0.0 \overline{119}=11.9=\frac{119}{10}$. And hence we have $x=\frac{119}{10 \cdot 999}=\frac{119}{9,990}$. [3 pts, Bookwork]
(ii) We can write $x=0.01191 \overline{191}$. This shows immediately that $r=0.01191=\frac{1191}{100,000}$ satisfies $0.0119<r<0.0 \overline{119}$. [3 pts, Standard]
(iii) From a result in the course we know that $\sqrt{2}$ is irrational. We also know that $1<$ $\sqrt{2}<2$. This means that $0<\frac{\sqrt{2}}{200,000}<\frac{2}{200,000}$. Since $\sqrt{2}$ is irrational, also $z=\frac{119}{10,000}+\frac{1}{200,000} \sqrt{2}$ is irrational. Note that $z$ satisfies $z>\frac{119}{10,000}=0.0119$ and $z<\frac{119}{10,000}+\frac{2}{200,000}=0.0119+0.00001=0.01191<0.0 \overline{119}$. So $z$ has indeed the desired properties. [5 pts, Unseen]
(c) Let $x \in(A \cup B) \backslash C$. That means that $x \in A \cup B$ and $x \notin C$. And from $x \in A \cup B$ we know that $x \in A$ or $x \in B$. If $x \in A$, then together with $x \notin C$ we have $x \in A \backslash C$, and hence $x \in(A \backslash C) \cup(B \backslash C)$. While if $x \in B$, then together with $x \notin C$ we have $x \in B \backslash C$, giving $x \in(A \backslash C) \cup(B \backslash C)$ again. So we can conclude that $(A \cup B) \backslash C \subseteq(A \backslash C) \cup(B \backslash C)$. [5 pts, Unseen]

## Question 3

(a) (i) The contrapositive of the statement is "if $p / q$ can not be expressed as an Egyptian fraction with $k+1$ terms, then $p / q$ can not be expressed as an Egyptian fraction with $k$ terms".
The converse of the statement is "if $p / q$ can be expressed as an Egyptian fraction with $k+1$ terms, then $p / q$ can be expressed as an Egyptian fraction with $k$ terms". [2 +1 pts, Standard]
(ii) We need to show that we can write $1 / a=1 / b+1 / c$, for some natural numbers $b, c$, $b \neq c$. We greedily take $1 / b<1 / a$ as large as possible, hence we take $b=a+1$. We find that $\frac{1}{a}-\frac{1}{a+1}=\frac{1}{a(a+1)}$. Hence we have $\frac{1}{a}=\frac{1}{a+1}+\frac{1}{a(a+1)}$. And since $a \geq 2$, we have $a(a+1) \neq a+1$, as required. [4 pts, Unseen]
(iii) Let $p / q, 0<p / q<1$, be a rational number and suppose that we can express $p / q$ as an Egyptian fraction with $k \geq 2$ terms. In other words we can write $\frac{p}{q}=$ $\frac{1}{a_{1}}+\frac{1}{a_{2}}+\cdots+\frac{1}{a_{k}}$, where $a_{1}, a_{2}, \ldots, a_{k}$ are different natural numbers. So we can assume that $a_{1}<a_{2}<\ldots<a_{k}$. Now in part (ii) we have seen that we can write $\frac{1}{a_{k}}=\frac{1}{a_{k}+1}+\frac{1}{a_{k}\left(a_{k}+1\right)}$, with $a_{k}<a_{k}+1<a_{k}\left(a_{k}+1\right)$ (since $\left.a_{k}>a_{1} \geq 1\right)$. Putting it together gives $\frac{p}{q}=\frac{1}{a_{1}}+\frac{1}{a_{2}}+\cdots+\frac{1}{a_{k-1}}+\frac{1}{a_{k}+1}+\frac{1}{a_{k}\left(a_{k}+1\right)}$, which gives an expression of $p / q$ as an Egyptian fraction with $k+1$ terms. [6 pts, Unseen]
(iv) The contrapositive of a statement is logically equivalent to the statement itself. Since we proved in (iii) that $P$ is always true, that means that the contrapositive of $P$ is also always true.
[2 pts, Bookwork]
(b) (i) If $c=1$, the system becomes $\left\{\begin{array}{r}5 x+3 y=2 \text {, Multiplying the second equation by } 50 \text { } 5 x+2 y=1 .\end{array}\right.$ gives $5 x+10 y=5$. Since $10=3$ in $\mathbb{Z}_{7}$, that equation is equivalent to $5 x+3 y=5$. But as the first equation is $5 x+3 y=2$, we get $5=2$, which is not valid in $\mathbb{Z}_{7}$. [3 pts, Standard]
(ii) Multiplying the first equation by 2 gives $10 x+6 y=4$, which is equivalent to $3 x+6 y=$ 4 in $\mathbb{Z}_{7}$. Multiplying the second equation by 3 gives $3 c x+6 y=3$. Subtracting the new first equation from the new second one gives $(3 c-3) x=-1=6$ in $\mathbb{Z}_{7}$. Since 7 is a prime number, every element $a \in \mathbb{Z}_{7}, a \neq 0$, has an inverse $a^{-1} \in \mathbb{Z}_{7}$. Since $3 c-3 \neq 0$ if $c \neq 1$, there is an inverse $(3 c-3)^{-1}$. That means that $(3 c-3) x=6$ has the solution $x=6(3 c-3)^{-1}$.
Substituting this value for $x$ in the first equation leads to $5 \cdot 6(3 c-3)^{-1}+3 y=2$, which gives $3 y=2-30(3 c-3)^{-1}=2+5(3 c-3)^{-1}$ (since $-30=-2=5$ in $\mathbb{Z}_{7}$ ). The inverse of 3 in $\mathbb{Z}_{7}$ is 5 (since $3 \cdot 5=15=1$ in $\mathbb{Z}_{7}$ ). So for $y$ we find the solution $y=5 \cdot\left(2+5(3 c-3)^{-1}\right)=10+25(3 c-3)^{-1}=3+4(3 c-3)^{-1}$ in $\mathbb{Z}_{7}$.
So the solution for the case $c \neq 1$ is $x=6(3 c-3)^{-1}$ and $y=3+4(3 c-3)^{-1}$. [7 pts, Unseen in this form]

## Question 4

(a) (i) A function is surjective if for all $y \in Y$ there exists an $x \in X$ such that $f(x)=y$.

A function is injective if for all $x_{1}, x_{2} \in X$ with $x_{1} \neq x_{2}$ we have that $f\left(x_{1}\right) \neq f\left(x_{2}\right)$.
A function is bijective if it is both surjective and injective.
$[1+1+1$ pts, Bookwork]
(ii) Form 1: For all natural numbers $m, n \in \mathbb{N}$, if there is an injection from $\mathbb{N}_{m}$ to $\mathbb{N}_{n}$ (where $\mathbb{N}_{m}=\{1,2,3, \ldots, m\}$ ), then $m \leq n$.
Form 2: Let $A, B$ be two finite sets, and let $f$ be a function from $A$ to $B$. If $|A|>|B|$, then there exist $a_{1}, a_{2} \in A, a_{1} \neq a_{2}$, such that $f\left(a_{1}\right)=f\left(a_{2}\right)$.
[2 pts, Bookwork]
(iii) Suppose $f: X \rightarrow X$ is injective, but not surjective. Let $X^{\prime}$ be the set of elements in $X$ that appear as an image $f(x)$ for $x \in X$. Since $f$ is not surjective, we have that $X^{\prime} \neq X$. But since we also have $X^{\prime} \subseteq X$, this means that $\left|X^{\prime}\right|<|X|$. Since we can consider $f$ as a function from $X$ to $X^{\prime}$, by the Pigeonhole Principle there are $x_{1}, x_{2} \in X, x_{1} \neq x_{2}$, such that $f\left(x_{1}\right)=f\left(x_{2}\right)$. But that contradicts that $f$ is injective. Hence $f$ must be surjective.
[6 pts, Unseen, and quite hard]
(iv) Define the function $f: \mathbb{N} \rightarrow \mathbb{N}$ by $f(x)=x+1$. Then $f$ is injective, but not surjective (since there is no element $x \in \mathbb{N}$ such that $f(x)=1$ ).
[3 pts, Unseen]
(b) (i) $R$ is reflexive on $\mathbb{N}$. For this, we use that $\operatorname{gcd}(a, a)=a$ (if $a \in \mathbb{N}$ ). And if $x \in \mathbb{N}$, then $x+1 \geq 2$, hence $\operatorname{gcd}(x+1, x+1)=x+1 \geq 2$. So we have that $x R x$ for all $x \in \mathbb{N}$. [2 pts, Unseen, though similar to many exercises]
(ii) $R$ is symmetric on $\mathbb{N}$. For all $a, b \in \mathbb{N}$ we have $\operatorname{gcd}(a, b)=\operatorname{gcd}(b, a)$. This means that $\operatorname{gcd}(x+1, y+1) \geq 2$ if and only if $\operatorname{gcd}(y+1, x+1) \geq 2$. So we have that $x R y \Rightarrow y R x$ for all $x, y \in \mathbb{N}$.
[3 pts, Unseen, though similar to many exercises]
(iii) $R$ is not transitive on $\mathbb{N}$. Take $x=1, y=5$ and $z=2$. Then we have that $\operatorname{gcd}(x+1, y+1)=\operatorname{gcd}(2,6)=2 \geq 2$ and $\operatorname{gcd}(y+1, z+1)=\operatorname{gcd}(6,3)=3 \geq 2$, hence $x R y$ and $y R z$ hold. But $\operatorname{gcd}(x+1, z+1)=\operatorname{gcd}(2,3)=1 \nsupseteq 2$, hence $x R z$ does not hold. So it is not the case that $(x R y \wedge y R z) \Rightarrow x R z$ for all $x, y, z \in \mathbb{N}$, and hence $R$ is not transitive.
[4 pts, Unseen]
(iv) Since $R$ is not transitive, it cannot be an equivalence relation.
[2 pts, Bookwork]

## Question 5

(a) (i) $s$ is an upper bound for $A$ if $s \geq a$ for all $a \in A$. $s$ is the supremum of $A$ if $s$ is the least upper bound of $A$, i.e., $s$ is an upper bound for $A$, and $s \leq t$ whenever $t$ is an upper bound for $A$.
[3pts, Bookwork]
(ii) To show that $\sup (A \cup B) \geq \sup (A)$, it suffices to show that $t=\sup (A \cup B)$ is an upper bound for $A$, since it then follows that $\sup (A) \leq t$. But this is immediate, since, for every $a \in A, a \in A \cup B$, and so $a \leq t$. [2pts, Similar to exercise]
(iii) Suppose that $A$ dominates $B$, let $s=\sup (A)$, and take any $c \in A \cup B$. Either (i) $c \in A$, in which case $c \leq s$ since $s$ is an upper bound for $A$, or (ii) $c \in B$, in which case there is some $a \in A$ with $c \leq a \leq s$, since $A$ dominates $B$ and $s$ is an upper bound for $A$. Thus $s$ is an upper bound for $A \cup B$.
This implies that $\sup (A \cup B) \leq s=\sup (A)$, and combining this with the previous part gives $\sup (A \cup B)=\sup A$. [5pts, Unseen]
(iv) This is false. Consider $A=(0,1), B=(0,1]$. Then $\sup (A \cup B)=\sup (A)=1$, but $A$ does not dominate $B$ since $1 \in B$ but there is no element $a \in A$ with $a \geq 1$. [2pts, Unseen]
(v) This is true. Take any $b \in B$. As $s$ is an upper bound for $B$, but $s \notin B$, we have $b<s$. Now, as $s$ is the supremum of $A, b$ is not an upper bound for $A$, and so there is some $a \in A$ with $a>b$. Hence $A$ dominates $B$. [4pts, Unseen]
(b) To show that there is at least one such value, we use the Intermediate Value Theorem: if $g:[a, b] \rightarrow \mathbb{R}$ is a continuous function, and $g(a) \leq c \leq g(b)$, then there is some $x \in[a, b]$ with $g(x)=c$.
[2pts]
We apply the Intermediate Value Theorem with $g(x)=\sqrt{x}-f(x)$, and $[a, b]=[0,1]$. We know that $g$ is continuous as it is the sum of the continuous functions $\sqrt{x}$ and $-f(x)$. Also $g(0)=-f(0)=-1$, and $g(1)=1-f(1) \geq 1-f(0)=0$, since $f$ is decreasing. Hence $g(0) \leq 0 \leq g(1)$, and so there is some $x \in[0,1]$ with $g(x)=0$, i.e., $f(x)=\sqrt{x}$. [5pts, Unseen but routine]
To see that there is at most one such $x$, note that $g(x)$ is strictly increasing. Explicitly, suppose there are two solutions $x_{1}$ and $x_{2}$ with $x_{1}<x_{2}$. Then $f\left(x_{1}\right)=\sqrt{x_{1}}<\sqrt{x_{2}}=f\left(x_{2}\right)$, contradicting the assumption that $f$ is decreasing.
[2pts, Unseen]

## Question 6

(a) (i) To say that $\left(a_{n}\right)_{n \in N}$ is convergent, with limit 1 , means that, for every $\varepsilon>0$, there is some $N \in \mathbb{N}$ such that, for $n>N,\left|a_{n}-1\right|<\varepsilon$.
[3pts, Bookwork]
(ii) Suppose that $a_{n} \rightarrow 1$. We show that $a_{n}^{2} \rightarrow 1$.

Fix $\varepsilon>0$. As $a_{n} \rightarrow 1$, there is some $N \in \mathbb{N}$ such that, for $n>N,\left|a_{n}-1\right|<$ $\min (1, \varepsilon / 3)$. Now we have, for $n>N, a_{n} \leq 2$, and therefore

$$
\left|a_{n}^{2}-1\right|=\left|a_{n}-1\right|\left|a_{n}+1\right|<3\left|a_{n}-1\right|<3 \frac{\varepsilon}{3}=\varepsilon
$$

Hence indeed $a_{n}^{2} \rightarrow 1$.
[6pts, essentially Bookwork]
(iii) We now show that $b_{n}=\max \left(a_{n}, a_{n}^{2}\right) \rightarrow 1$.

Fix $\varepsilon>0$. Take $N_{1} \in \mathbb{N}$ such that, for $n>N_{1},\left|a_{n}-1\right|<\varepsilon$. Take also $N_{2} \in \mathbb{N}$ such that, for $n>N_{2},\left|a_{n}^{2}-1\right|<\varepsilon$. Now take $N=\max \left(N_{1}, N_{2}\right)$. For $n>N$, we have $a_{n}<1+\varepsilon$ and $a_{n}^{2}<1+\varepsilon$, so $b_{n}<1+\varepsilon$. Also we have $b_{n} \geq a_{n}>1-\varepsilon$. So $\left|b_{n}-1\right|<\varepsilon$. Hence indeed $b_{n} \rightarrow 1$.
[4pts, Unseen, but related to a recent past exam question]
(b) (i) We note that

$$
\begin{aligned}
\sqrt{n+1}-\sqrt{n-1} & =\frac{(\sqrt{n+1}-\sqrt{n-1})(\sqrt{n+1}+\sqrt{n-1})}{\sqrt{n+1}+\sqrt{n-1}} \\
& =\frac{(n+1)-(n-1)}{\sqrt{n+1}+\sqrt{n-1}}=\frac{2}{\sqrt{n+1}+\sqrt{n-1}}
\end{aligned}
$$

and hence $a_{n}=\frac{2 \sqrt{n}}{\sqrt{n+1}+\sqrt{n-1}}=\frac{2}{\sqrt{1+\frac{1}{n}}+\sqrt{1-\frac{1}{n}}}$.
[5pts, Similar examples have been seen]
By the Algebra of Limits, we have

$$
\begin{aligned}
\lim _{n \rightarrow \infty} a_{n} & =\frac{2}{\lim _{n \rightarrow \infty} \sqrt{1+\frac{1}{n}}+\lim _{n \rightarrow \infty} \sqrt{1-\frac{1}{n}}} \\
& =\frac{2}{\sqrt{1+\lim _{n \rightarrow \infty} \frac{1}{n}}+\sqrt{1-\lim _{n \rightarrow \infty} \frac{1}{n}}}=\frac{2}{\sqrt{1+0}+\sqrt{1-0}}=1
\end{aligned}
$$

[3pts]
(ii) We proved in the course that $2^{1 / n} \rightarrow 1$ as $n \rightarrow \infty$. Hence there is some $N \in \mathbb{N}$ such that $2^{1 / n}>\frac{1}{2}$ for $n>N$. We see that $b_{n}>\frac{1}{2}$ for even $n>N$, and $b_{n}<-\frac{1}{2}$ for odd $n>N$. This implies that $\left(b_{n}\right)_{n \in N}$ does not converge. (One could write more, but I think this should suffice.)
[4pts, Unseen]

## Question 7

(a) (i) A function $\phi: G \rightarrow G^{\prime}$ is a homomorphism if, for every $a, b \in G, \phi(a * b)=\phi(a) *^{\prime} \phi(b)$. [2pts, Bookwork]
(ii) The kernel of $\phi$ is $\operatorname{ker}(\phi)=\left\{a \in G \mid \phi(a)=e^{\prime}\right\}$, where $e^{\prime}$ is the identity element of $\left(G^{\prime}, *^{\prime}\right)$.
[2pts, Bookwork]
(iii) To see that $\operatorname{ker}(\phi)$ is a subgroup of $(G, *)$, we have three things to check:

1) If $a, b \in \operatorname{ker}(\phi), \phi(a)=\phi(b)=e^{\prime}$, so $\phi(a * b)=\phi(a) * \phi(b)=e^{\prime} *^{\prime} e^{\prime}=e^{\prime}$, so $a * b \in \operatorname{ker}(\phi)$.
2) We are given that $\phi(e)=e^{\prime}$, so that $e \in \operatorname{ker}(\phi)$.
3) If $a \in \operatorname{ker}(\phi)$, then $\phi\left(a^{-1}\right)=(\phi(a))^{-1}=\left(e^{\prime}\right)^{-1}=e^{\prime}$, so $a^{-1} \in \operatorname{ker}(\phi)$.

Hence indeed $\operatorname{ker}(\phi)$ is a subgroup.
[5pts, Bookwork]
(b) (i) We show first that $g * \operatorname{ker}(\phi) \subseteq S_{h}$. An element of $g * \operatorname{ker}(\phi)$ is of the form $g * a$, where $a \in \operatorname{ker}(\phi)$. Now $\phi(g * a)=\phi(g) *^{\prime} \phi(a)=h *^{\prime} e^{\prime}=h$, so $g * a \in S_{h}$, as required. [3pts, Unseen]
Now suppose that $f \in S_{h}$, so that $\phi(f)=h$. We note that $f=g *\left(g^{-1} * f\right)$, and we claim that $g^{-1} * f \in \operatorname{ker}(\phi)$. Indeed, $\phi\left(g^{-1} * f\right)=(\phi(g))^{-1} *^{\prime} \phi(f)=h^{-1} *^{\prime} h=e^{\prime}$. Hence $f \in g * \operatorname{ker}(\phi)$, as required. [3pts, Unseen]
(ii) For the next part, we know that all left cosets of $\operatorname{ker}(\phi)$ have size $|\operatorname{ker}(\phi)|$, and there is one coset for each element of $\operatorname{im}(\phi)$. As the cosets (or indeed the inverse images of elements of $\operatorname{im}(\phi))$ partition the group, we have that $|G|$ is equal to the number of cosets times the size of each coset, as given.
[2pts, Unseen]
(c) The function $\theta$ is a homomorphism iff we have $\theta(a * b)=\theta(a) * \theta(b)$ for all $a, b \in G$, i.e., $a * b * a * b=a * a * b * b$ for all $a, b \in G$. This certainly holds if $b * a=a * b$ for all $a, b \in G$, i.e., if $G$ is Abelian. Conversely, if, for all $a, b \in G$, we have $a * b * a * b=a * a * b * b$, then we also have $a^{-1} * a * b * a * b * b^{-1}=a^{-1} * a * a * b * b * b^{-1}$, and so $b * a=a * b-$ hence $G$ is Abelian.
[6pts, Unseen, though related to material in lectures/exercises]
(d) If $G$ is Abelian, then the function $\theta$ is a homomorphism. Its kernel is $\{g \mid g * g=e\}$, and its image is $\{a \mid a=g * g$ for some $g \in G\}$. The result now follows from (b).
[2pts, Unseen]

## Question 8

(a) (i) A basis of a vector space $V$ is a set $B$ of vectors in $B$ such that (i) $B$ is linearly independent, and (ii) $B$ spans $V$.
The vector space $V$ has dimension $d$ if there is a basis of cardinality $d$. [4pts, Bookwork]
(ii) We follow the hint and take bases $\left\{\mathbf{u}_{1}, \mathbf{u}_{2}\right\}$ of $U$ and $\left\{\mathbf{w}_{1}, \mathbf{w}_{2}\right\}$ of $W$. Now consider $\mathbf{u}_{1}, \mathbf{u}_{2}, \mathbf{w}_{1}, \mathbf{w}_{2}$. As there are four vectors here (though not necessarily distinct) and $V$ has dimension 3, they are linearly dependent. Thus there are real numbers $\alpha_{1}, \alpha_{2}, \beta_{1}, \beta_{2}$, not all zero, with

$$
\alpha_{1} \mathbf{u}_{1}+\alpha_{2} \mathbf{u}_{2}+\beta_{1} \mathbf{w}_{1}+\beta_{2} \mathbf{w}_{2}=\mathbf{0}
$$

We can then rewrite this as

$$
\alpha_{1} \mathbf{u}_{1}+\alpha_{2} \mathbf{u}_{2}=-\beta_{1} \mathbf{w}_{1}-\beta_{2} \mathbf{w}_{2}:=\mathbf{v}
$$

The vector $\mathbf{v}$ is in $U$, since it is a linear combination of the basis elements of $U$, and similarly it is in $W$. Suppose that $\mathbf{v}=\mathbf{0}$. As $\mathbf{0}=\mathbf{v}=\alpha_{1} \mathbf{u}_{1}+\alpha_{2} \mathbf{u}_{2}$, then as $\mathbf{u}_{1}, \mathbf{u}_{2}$ are linearly independent, we have $\alpha_{1}=\alpha_{2}=0$. Similarly, as $\mathbf{0}=\mathbf{v}=-\beta_{1} \mathbf{w}_{1}-\beta_{2} \mathbf{w}_{2}$, we have $\beta_{1}=\beta_{2}=0$. But this contradicts the assumption that not all of $\alpha_{1}, \alpha_{2}, \beta_{1}, \beta_{2}$ are zero. Therefore the vector $\mathbf{v}$ is a non-zero vector in $U \cap W$. [11pts, Unseen]
(b) We have three things to check:
(i) The set $L$ is closed under addition. Suppose then that $f$ and $g$ are in $L$; there are constants $K_{f}$ and $K_{g}$ such that, for all $x, y \in \mathbb{R},|f(x)-f(y)| \leq K_{f}|x-y|$, and $\mid g(x)-$ $g(y)\left|\leq K_{g}\right| x-y \mid$. So we have, for all $x, y \in \mathbb{R}$,

$$
\begin{aligned}
|(f+g)(x)-(f+g)(y)| & \leq|f(x)-f(y)|+|g(x)-g(y)| \\
& \leq K_{f}|x-y|+K_{g}|x-y|=\left(K_{f}+K_{g}\right)|x-y|
\end{aligned}
$$

So the function $f+g$ is Lipschitz, with constant $K_{f}+K_{g}$.
(ii) The zero function is in $L$ : this is clear: we can take $K_{0}=0$.
(iii) The set $L$ is closed under scalar multiplication. Indeed, for $f$ in $L$ with Lipschitz constant $K_{f}$, and $\alpha \in \mathbb{R}$, we have

$$
|\alpha f(x)-\alpha f(y)|=|\alpha||f(x)-f(y)| \leq|\alpha| K_{f}|x-y|
$$

for all $x, y \in \mathbb{R}$, so the function $\alpha f$ is Lipschitz, with constant $|\alpha| K_{f}$.
Thus indeed $L$ is a subspace of $X$.
[10pts, Unseen]

