MA2C03: TUTORIAL 7 PROBLEM SHEET
HOMOMORPHISMS AND ISOMORPHISMS

1) Let A be a finite set, and let A^* be the set of all words over the alphabet A. Consider $(A^*, \circ, \epsilon)$ with the operation of concatenation and empty word ϵ as the identity element. Let $(\mathbb{N}, +, 0)$ be the set of natural numbers with the operation of addition and 0 as the identity element. Let $f : A^* \to \mathbb{N}$ be the function that assigns to each word $w \in A^*$ its length, $f(w) = |w| \in \mathbb{N}$.

(a) What type of object is $(A^*, \circ, \epsilon)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(b) What type of object is $(\mathbb{N}, +, 0)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(c) Is f a homomorphism? Justify your answer.
(d) Is f an isomorphism? Justify your answer.

Solution: (a) $\circ$ is an associative binary operation as we proved in lecture, so $(A^*, \circ, \epsilon)$ is definitely a semigroup. As we showed in lecture, ϵ is the identity element for $\circ$ on A^*, which means $(A^*, \circ, \epsilon)$ is a monoid. We discussed in lecture during the abstract algebra unit that ϵ is the only invertible element in A^*, so $(A^*, \circ, \epsilon)$ cannot be a group.

(b) Addition is an associative binary operation as we showed in lecture, so $(\mathbb{N}, +, 0)$ is clearly a semigroup. 0 is the identity element for addition on $\mathbb{N}$ which means $(\mathbb{N}, +, 0)$ is a monoid. Note that 0 is the only invertible element in $\mathbb{N}$ so $(\mathbb{N}, +, 0)$ cannot be a group.

(c) To show that f is a homomorphism, we need to show that for any two words $w_1, w_2 \in A^*$, $f(w_1 \circ w_2) = |w_1| + |w_2|$, but we have already showed in lecture that this property holds. Therefore, f is a homomorphism.

(d) An isomorphism is a homomorphism that is also bijective. We know f is homomorphism. Now we need to decide whether it is bijective. The function f is clearly surjective because for any length $n \in \mathbb{N}$, we can construct a word in $w \in A^*$, whose length $|w| = n$. Is f injective? Well, the answer depends whether A has one element or several. If $A = \{a\}$ has only one element, there is one and only one word $a \cdots a$ of any given length n, so f is injective. However, if A has more than one element, then there exist letters $a, b \in A$ such that $a \neq b$. Then the words ab and ba that are distinct have the same length 2, which means f cannot be injective, so it is not an isomorphism.

2) Let $(\mathbb{Z}, +, 0)$ be the set of integers with the operation of addition and 0 as the identity element. Let E be the set of even integers, $E = \{2p \mid p \in \mathbb{Z}\}$. Consider $(E, +, 0)$ the set of even integers with the operation of addition and 0 as the identity element. Let $f : \mathbb{Z} \to E$ be the function $f(n) = 2n$.

(a) What type of object is $(\mathbb{Z}, +, 0)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(b) What type of object is $(E+, 0)$ in abstract algebra (semigroup, monoid, group)? Justify your answer.
(c) Is f a homomorphism? Justify your answer.
(d) Is f an isomorphism? Justify your answer.

Solution: (a) Addition on $\mathbb{R}$ hence on $\mathbb{Z}$ is an associative binary operation as we discussed in lecture. Therefore, $(\mathbb{Z}, +, 0)$ is a semigroup. 0 is the identity element for addition on $\mathbb{Z}$ as for any $n \in \mathbb{Z}$, $n + 0 = 0 + n = n$, so $(\mathbb{Z}, +, 0)$ is a monoid. Given any $n \in \mathbb{Z}$, $-n$ is its inverse as $n + (-n) = n - n = 0$, so every element of $(\mathbb{Z}, +, 0)$ is invertible. Therefore, $(\mathbb{Z}, +, 0)$ is a group.

(b) $E \subset \mathbb{Z}$. Since addition is associative on $\mathbb{Z}$, it is also associative on E. We do, however, have to prove it is a binary operation, i.e. closed. Consider $m, n \in E$. Thus, there exist $p, s \in \mathbb{Z}$ such that $m = 2p$ and $n = 2s$ by the definition of E. Then $m + n = 2p + 2s = 2(p + s)$. Since addition is a binary operation on $\mathbb{Z}$ hence closed, it follows

$$p, s \in \mathbb{Z} \implies p + s \in \mathbb{Z}.$$

Thus, $m + n \in E$, and addition is indeed closed on E. We conclude $(E+, 0)$ is a semigroup. Since $E \subset \mathbb{Z}$, the fact that 0 is the identity element for addition on $\mathbb{Z}$ carries over to E, so E has 0 as its identity element. Therefore, $(E+, 0)$ is a monoid. Now let $n \in E$. We know from part (a) that $-n \in \mathbb{Z}$ is the inverse of n under addition. We just have to prove $-n \in E$. Since $n \in E$, there exists $p \in \mathbb{Z}$ such that $n = 2p$. Therefore, $-n = -2p = 2(-p)$, so $-n \in E$ as needed, which means every element in E is invertible. Therefore, $(E+, 0)$ is a group.

(c) To show that f is a homomorphism, we need to show that for any two integers $p, s \in \mathbb{Z}$, $f(p + s) = f(p) + f(s)$. We apply the definition of f as follows: $f(p) + f(s) = 2p + 2s = 2(p + s) = f(p + s)$. Therefore, f is a homomorphism.

(d) An isomorphism is a homomorphism that is also bijective. We know f is homomorphism. We need to figure out whether it is bijective. The function f is clearly surjective by the definition of E because for every $n \in E$, there exists $p \in \mathbb{Z}$ such that $n = 2p = f(p)$. To show injectivity, assume there exist $p, s \in \mathbb{Z}$ such that $f(p) = f(s)$. Then by the definition of f, $2p = 2s \iff p = s$. Therefore, f is indeed injective. We have shown f is bijective hence an isomorphism from $(\mathbb{Z}, +, 0)$ to $(E, +, 0)$.