Math 100B - Abstract Algebra

Due: Wednesday, April 2

Assignment 1

1

a) $(2+7\mathbb{Z})^{-1} = 4+7\mathbb{Z}$

b) $(6+7\mathbb{Z})^{-1} = 6+7\mathbb{Z}$

c) $(2+17\mathbb{Z})^{-1} = 9+17\mathbb{Z}$

d) $(10+17\mathbb{Z})^{-1} = 12+17\mathbb{Z}$

e) $(2+37\mathbb{Z})^{-1} = 19+37\mathbb{Z}$

f) $(2+107\mathbb{Z})^{-1} = 54+107\mathbb{Z}$

2 Let F be a field. For any $a \in F$, let $m_a \colon F \to F$ be the function $m_a(x) = a \cdot x$.

a) We show that $m_{a+b}(x) = m_a(x) \cdot m_b(x)$, making it a homomorphism of additive groups. Let $a, b \in F$. Then, $m_{a+b}(x) = (a+b)\cdot x$. By the axioms of a field, we know that $(a+b)\cdot x = a\cdot x + b\cdot x$. Then, $a\cdot x = m_a(x)$ and $b\cdot x = m_b(x)$, so we have our equality $m_{a+b}(x) = (a+b)\cdot x = a\cdot x+b\cdot x = m_a(x) + m_b(x)$, showing that m_a is indeed a homomorphism of additive groups.

b) We show that $m_a \circ m_b = m_{ab}$. Write $m_a \circ m_b$ as $m_a(m_b(x))$. Then, we know that $m_b(x) = b \cdot x$, so $m_a(m_b(x)) = m_a(b \cdot x)$. Since F is a field, $\cdot$ is a binary operation on F, so since $b, x \in F$, we know that $b \cdot x \in F$. Then, $m_a(b \cdot x) = a \cdot (b \cdot x)$, which can be written as $(a \cdot b) \cdot x$ because once again $\cdot$ is a binary operation on F, and we know that $\cdot$ is associative on elements of F. $(a \cdot b) \cdot x = m_{ab}(x)$, so we have shown that $m_a \circ m_b = m_{ab}$.

c) $\Rightarrow$ We show that m_a is an isomorphism of additive groups if a $\neq 0$. We do this by contrapositive, and show that if $a = 0$, then m_a is not an isomorphism. If $a = 0$, then $m_0(1)$ and $m_0(2)$ (where $2 = 1 + 1$) will be $0 \cdot 1 = 0$ and $0 \cdot 2 = 0$, respectively. So, $m_0(1) = 0 = m_0(2)$, which violates injectivity, so $m_0(x)$ is not an isomorphism.
$\Leftarrow$ We show that if $a \neq 0$, then $m_a(x)$ is an isomorphism. For $m_a(x)$ to be an isomorphism, we must show injectivity and surjectivity. We show that $m_a(x)$ is injective. In other words, we must show that if $m_a(x_1) = m_a(x_2)$, then $x_1 = x_2$. If $m_a(x_1) = m_a(x_2)$, then $a \cdot x_1 = a \cdot x_2$. Because $(F - \{0\}, \cdot)$ is an abelian group, and by the left cancellation property of groups, we know that $a \cdot x_1 = a \cdot x_2 \to x_1 = x_2$, which means that $m_a(x)$ is indeed injective. Next, we show surjectivity. Let $z \in F$. We show that $\exists b \in F$ such that $m_a(b) = z$. $m_a(b) = a \cdot b$, so we need to show that $\exists b \in F$ such that $a \cdot b = z$. Multiply both sides on the left by a^{-1} to yield $b = a^{-1} \cdot z$. Since $a \neq 0$, a^{-1} is well defined, and in F. So, $\forall z \in F$, $\exists b \in F$ where $b = a^{-1}z$, so $m_a(b) = a \cdot b = a \cdot (a^{-1} \cdot z) = (a \cdot a^{-1}) \cdot z = z$, for any $z \in F$. So, $m_a(x)$ is surjective. So, since $m_a(x)$ is injective and surjective, it is bijective, and since we proved in part a that is a homomorphism, we have that $m_a(x)$ is an isomorphism.