Problem 1 (Ch. 2.1)

Let C be the set of real-valued continuous functions on the real line $\mathbb{R}$. Show that C with the usual addition of functions and 0 is an abelian group, and that C with product $(f \cdot g)(x) = f(g(x))$ and 1 the identity map is a monoid. Is C with these compositions and 0 and 1 a ring?

Solution. Let $f, g, h \in C$.

We first show $(C, +, 0)$ is an abelian group. We have that $f + g$ is also a real-valued continuous function, and so $f+g \in C$. The associativity and commutativity of real addition gives $(f(x_0)+g(x_0))+h(x_0) = f(x_0)+(g(x_0)+h(x_0))$ and $f(x_0) + g(x_0) = g(x_0) + f(x_0)$ for all $x_0 \in \mathbb{R}$, hence $(f + g) + h = f + (g + h)$ and $f + g = g + h$. Furthermore, the zero function 0 is in C, and $0 + f = f + 0 = f$. Finally, if we consider $F = -f$, multiplying by a scalar does not change if a function is continuous or not, so $F \in C$, and $f + F = F + f = 0$. This satisfies all the conditions for an abelian group.

We now show that $(C, \circ, 1)$ is a monoid. Recall that the composition of two continuous functions is also continuous, so $f \circ g \in C$. Furthermore, $(f \circ g) \circ h(x) = f(g(h(x))) = f \circ (g \circ h)(x)$, which shows associativity. Finally, the identity map is continuous on $\mathbb{R}$, and $(1 \circ f)(x) = (f \circ 1)(x) = f(x)$. This satisfies all the conditions of a monoid.

It remains to consider the distributive laws, which will show that C is not a ring. Let $f(x) = x + 1$, $g(x) = 1$ and $h(x) = -1$. These are all obviously in C. We have $(f \circ (g + h))(x) = (f \circ 0)(x) = 1$ for all x, however $(f \circ g)(x) + (f \circ h)(x) = 2 + 0 = 2$ for all x. Thus $(f \circ (g + h))(x) \neq (f \circ g)(x) + (f \circ h)(x)$, and so C is not a ring.

Problem 4 (Ch. 2.1)

Let I be the set of complex numbers of the form $m + n\sqrt{-3}$ where either $m, n \in \mathbb{Z}$ or both m and n are halves of odd integers. Show that I is a subring of $\mathbb{C}$.

Solution. We first show that $(I, +, 0)$ form an abelian group. Since $\mathbb{C}$ is a ring, $+$ is associative and commutative, and $0 = 0 + 0\sqrt{-3} \in I$. Note that for any $m + n\sqrt{-3}$, $-m - n\sqrt{-3}$ is the additive inverse in $\mathbb{C}$, and if $m, n \in \mathbb{Z}$, so is $-m, -n$, or if m and n are halves of odd integers, say $2m$ and $2n$, then $-m, -n$ are halves of $-2m, -2n$ which are also odd integers; so additive inverses of elements in I are also in I. Finally, $(m + n\sqrt{-3}) + (m' + n'\sqrt{-3}) = (m + m') + (n + n')\sqrt{-3}$. If m, n and m', n' were all integers, then $m + m' \in \mathbb{Z}$ and $n + n' \in \mathbb{Z}$. If one of m, n and m', n' were integers, and so the others were half of odd integers, then $m + m'$ and $n + n'$ are also half of odd integers, namely $2m + 2m'$ and $2n + 2n'$ (which is odd, since WLOG $2m, 2n$ are even and $2m', 2n'$ are odd). If all of m, n, m', n' were half of odd integers, then $m + m' \in \mathbb{Z}$ and $n + n' \in \mathbb{Z}$. Hence, $(m + n\sqrt{-3}) + (m' + n'\sqrt{-3}) \in I$. This shows that $(I, +, 0)$ is an abelian group.

We now show that $(I, \cdot, 1)$ is a monoid. Since $\mathbb{C}$ is a ring, $\cdot$ is associative. Note that the multiplicative identity in $\mathbb{C}$, $1 + 0\sqrt{-3}$, is in I as well (both $m, n \in \mathbb{Z}$). Finally, we show that I is closed under multiplication. Note

$$(m + n\sqrt{-3}) \cdot (m' + n'\sqrt{3}) = (mm' - 3nn') + (mn' + nm')\sqrt{-3}$$

When $m, n, m', n' \in \mathbb{Z}$, then $mm' - 3nn'$ and $mn' + nm'$ are in $\mathbb{Z}$ as well. If one of the two, say WLOG $m, n \in \mathbb{Z}$, while m', n' are halves of odd integers, then let $l = 2m'$, $k = 2n'$ where l, k are odd, and we have $mm' - 3nn' = (ml - 3nk)/2$ which is an integer when $ml - 3nk$ is even and half an odd integer when $ml - 3nk$ is odd (and one of the two always happens, since $ml - 3nk \in \mathbb{Z}$); we also have $mn' + nm' = (mk + nl)/2$ which is an integer when $mk + nl$ is even and half an odd integer when $mk + nl$ is odd; it remains to show that $ml - 3nk$ and $mk + nl$ have the same parity: since $l, k, 3$ are odd, $ml \equiv mk \equiv m \pmod 2$ and $3nk \equiv nl \equiv n \pmod 2$, so

$$ml - 3nk \equiv m - n \equiv m - n + 2n \equiv m + n \equiv mk + nl \pmod 2$$

which confirms that they have the same parity. We now can turn to the final case, which is when m, n, m', n' are all halves of odd integers. Then denote $a = 2m, b = 2n, l = 2m', k = 2n'$ all of which are odd. See $mm' - 3nn' = \frac{al-3bk}{2}$ and $al - 3bk$ is even so $mm' - 3nn'$ is an integer, and $mn' + nm' = \frac{ak+bl}{2}$ and $ak + bl$ is even so $mn' + nm'$ is an integer. This exhausts all possible cases of m, n, m', n', showing that I is closed under multiplication.

It now remains to show the distributive laws hold. See

$$\begin{aligned}(m+n\sqrt{-3})\big((m'+n'\sqrt{-3})+(m''+n''\sqrt{-3})\big) &= (m+n\sqrt{-3})\big((m'+m'')+(n'+n'')\sqrt{-3}\big)\\ &= (m(m'+m'')-3n(n'+n''))+(m(n'+n'')+n(m'+m''))\sqrt{-3}\\ &= mm'+mm''-3nn'-3nn''+(mn'+mn''+nm'+nm'')\sqrt{-3}\\ &= mm'-3nn'+(mn'+nm')\sqrt{-3}\\ &\quad+mm''-3nn''+(mn''+nm'')\sqrt{-3}\\ &= (m+n\sqrt{-3})(m'+n'\sqrt{-3})+(m+n\sqrt{-3})(m''+n''\sqrt{-3})\end{aligned}$$

and

$$\begin{aligned}\big((m'+n'\sqrt{-3})+(m''+n''\sqrt{-3})\big)(m+n\sqrt{-3}) &= \big((m'+m'')+(n'+n'')\sqrt{-3}\big)(m+n\sqrt{-3})\\ &= ((m'+m'')m-3(n'+n'')n)+((n'+n'')m+(m'+m'')n)\sqrt{-3}\\ &= m'm+m''m-3n'n-3n''n+(n'm+n''m+m'n+m''n)\sqrt{-3}\\ &= m'm-3n'n+(n'm+m'n)\sqrt{-3}\\ &\quad+m''m-3n''n+(n''m+m''n)\sqrt{-3}\\ &= (m'+n'\sqrt{-3})(m+n\sqrt{-3})+(m''+n''\sqrt{-3})(m+n\sqrt{-3})\end{aligned}$$

Thus, we have proven that I is a ring, and so is a subring of $\mathbb{C}$.

Problem 1 (Ch. 2.2)

Show that any finite domain is a division ring.

Solution. For the sake of contradiction, assume that R is a finite domain that is not a division ring. Then, there exists some element $a \in R$, $a \neq 0$ that is not invertible. Let n denote the finite number of elements in $R^* = R \setminus \{0\}$.

We claim that for every $x, y' \in R$, if $xa = x'a$, then $x = x'$, since $xa = x'a \implies xa - x'a = 0 \implies (x-x')a = 0$, and since R is a domain and $a \neq 0$, $x - x' = 0 \implies x = x'$. Hence, $\{x_1a, x_2a, \ldots, x_na\}$ are distinct, non-zero elements, where x_i ranges over all the elements of R^* (the non-zeroness is because $x_i, a \neq 0 \implies x_ia \neq 0$ in a domain). Since all of $x_ia \in R^*$ (by the fact that $(R^*, \cdot)$ is a monoid when R is a domain) so $\{x_1a, x_2a, \ldots, x_na\} \subset R^*$, and there are the same number of elements (n) in both $\{x_1a, x_2a, \ldots, x_na\}$ and R^*, we have $\{x_1a, x_2a, \ldots, x_na\} = R^*$. Hence, there exists some $1 \leq j \leq n$ such that $x_ja = 1$. Thus, a has a left inverse. From now on, denote $l = x_j$.

We now do everything for right multiplication. So $ay = ay' \implies y = y'$ since $ay - ay' = 0 \implies a(y-y') = 0 \implies y - y' = 0 \implies y = y'$ as before. Hence, $\{ay_1, ay_2, \ldots, ay_n\}$ are distinct, non-zero elements, where y_i rangers over all the elements of R^*. Since $ay_i \in R^*$ and there are n elements in the set and R^*, we again have that there exists $1 \leq k \leq n$ such that $ay_k = 1$. Thus a has a right inverse, denoted $r = y_k$.

Now since we have $la = 1$, $ar = 1 \implies lar = l \implies r = l$. Hence, l is an inverse of a, contradicting our assumption that a was not invertible. Therefore, we have shown that any finite domain is also a division ring.

Problem 4 (Ch. 2.2)

Show that if $1 - ab$ is invertible in a ring then so is $1 - ba$.

Solution. Assume there exists c such that $c(1-ab) = (1-ab)c = 1$. Let $d = 1 + bca$. Using the distributive property of the ring, we see

$$d(1-ba) = (1-ba) + bca(1-ba) = 1 - ba + bc(a - aba) = 1 - ba + bc(1-ab)a = 1 - ba + ba = 1$$

and

$$(1-ba)d = (1-ba) + (1-ba)bca = 1 - ba + (b - bab)ca = 1 - ba + b(1-ab)ca = 1 - ba + ba = 1$$

hence, d is an inverse of $1 - ba$, so $1 - ba$ is invertible.

Problem 6 (Ch. 2.2)

Let u be an element of a ring that has a right inverse. Prove that the following conditions on u are equivalent: (1) u has more than one right inverse, (2) u is not a unit, (3) u is a left 0 divisor.

Solution. We first show (1) $\implies$ (2). We show the contrapositive. Let u be a unit, that is $\exists v$ such that $vu = uv = 1$. Now let v' be another right inverse of u. Then $uv' = 1$, so then $(vu)v' = v(uv') \implies v' = v$. Hence, any right inverse of u is just v, so there cannot be more than one right inverse.

Now we show (2) $\implies$ (3). Let v be the right inverse of u. Since u is not a unit, $uv = 1$ but $vu \neq 1$. See

$$0 = 1 - uv \implies 0u = (1 - uv)u \implies 0 = u - uvu \implies 0 = u(1 - vu)$$

And since $1 \neq vu \implies 1 - vu \neq 0$, we have that u is a left 0 divisor.

Now we show (3) $\implies$ (1). We have $\exists v$ such that $uv = 1$ and $\exists w \neq 0$ such that $uw = 0$. Then $uv + uw = 1 + 0 \implies u(v + w) = 1$. But since $w \neq 0 \implies v + w \neq v$, we have that $v + w$ is a distinct right inverse of u. Hence, u has more than one right inverse, v and $v + w$.

Problem 7 (Ch. 2.2)

(Kaplansky.) Prove that if an element of a ring has more than one right inverse then it has infinitely many. Construct a counterexample to show that this does not hold for monoids.

Solution. Let u be an element of a ring R that has more than one right inverse. So there is some $v \in R$ such that $uv = 1$. From Problem 6 above, u is not a unit, so $vu \neq 1$. This also means that $u^n \neq 1$ when $n > 0$, otherwise $uu^{n-1} = u^{n-1}u = 1$ making u a unit. Now, for all $n \in \mathbb{N}_0$, define $v_n = (1 - vu)u^n + v$. Note that $v_n \in R$. These v_n are all right inverses of u: $uv_n = u\,(1 - vu)u^n + v) = u(1-vu)u^n + uv = (u-uvu)u^n + 1 = (u-u)u^n + 1 = 0+1 = 1$. Furthermore, we claim that the map $\phi\colon \mathbb{N}_0 \to \{v_i\}_{i\in\mathbb{N}_0}$ defined by $\phi\colon n \mapsto v_n$ is injective. So assume that $n \neq m$ and we will show that $\phi(n) \neq \phi(m)$, i.e. $v_n \neq v_m$. WLOG assume that $n > m$. Since $n - m - 1 \geq 0$, $n - m - 1 \in \mathbb{N}_0$ so $uv_{n-m-1} = 1 \implies v_{n-m-1}u \neq 1$ (otherwise it would be a unit), hence $(1-vu)u^{n-m} + vu \neq 1 \implies (1-vu)u^{n-m} \neq 1 - vu$. Thus $(1 - vu)u^n \neq (1 - vu)u^m$, i.e. $v_n \neq v_m$ i.e. $\phi(n) \neq \phi(m)$. So $\{v_i\}_{i\in\mathbb{N}_0}$ is at least countable in size. Thus, there are infinitely many right inverses of u.

Counterexample: define the free monoid $M = \langle a, b, c\rangle$ such that $ab = ac = 1$ (operation is concatenation, 1 is the unit, where $1a = a1 = a$, etc.). Both b, c are right inverses of a, but by definition, no other distinct elements are right inverses of a.