

Jacobson 2.1.1 *Proof.* Pick any functions $f, g, h \in C$.

$(C, +, 0)$ is an abelian group.

Closure: Clearly that $f + g$ is a function as well.

Associativity: For all $x \in \mathbb{R}$, $[f(x) + g(x)] + h(x) = f(x) + [g(x) + h(x)]$ by the additive associativity of \mathbb{R} . Thus, $(f + g) + h = f + (g + h)$.

Identity: Since the integer 0 is the identity in \mathbb{R} , $f(x) + 0 = f(x) = 0 + f(x)$ for all x , i.e., the zero function 0 is the identity here.

Inverse: Note that for all $x \in \mathbb{R}$, $f(x) + (-1)f(x) = x - x = 0$. Thus, the additive inverse of function f is $(-1)f$ or simply $-f$.

Commutative: The abelianess of C follows from that of \mathbb{R} . Note that for all $x \in \mathbb{R}$, $f(x) + g(x) = g(x) + f(x)$. Therefore, $f + g = g + f$.

* * *

$(C, \circ, \text{id}_{\mathbb{R}})$ is a monoid.

Closure: Clearly that $f \circ g$ is a function as well.

Associativity: For all $x \in \mathbb{R}$, $((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x)$. Thus, $f \circ (g \circ h) = (f \circ g) \circ h$.

Identity: For all $x \in \mathbb{R}$, $(f \circ \text{id}_{\mathbb{R}})(x) = f(\text{id}_{\mathbb{R}}(x)) = f(x) = \text{id}_{\mathbb{R}}(f(x)) = (\text{id}_{\mathbb{R}} \circ f)(x)$. Thus, $f \circ \text{id}_{\mathbb{R}} = \text{id}_{\mathbb{R}} \circ f$.

* * *

$(C, +, \circ)$ is not a ring as it violates the distributive law. Let $f(x) = |x|$, $g(x) = 2$, $h(x) = -2$ for all $x \in \mathbb{R}$. Then for all x ,

$$(f \circ (g + h))(x) = 0 \neq 4 = (f \circ g + f \circ h)(x).$$

■

Jacobson 2.1.4 *Proof.* Pick any $a + b\sqrt{-3}, c + d\sqrt{-3} \in I$.

First, I is a subgroup of the additive group of \mathbb{C} . Note that $(a + b\sqrt{-3}) - (c + d\sqrt{-3}) = (a - c) + (b - d)\sqrt{-3}$. Then,

Case 1: If all $a, b, c, d \in \mathbb{Z}$, then $a - c, b - d \in \mathbb{Z}$.

Case 2: If all a, b, c, d are halves of odd integers, i.e., $a = a' + 1/2, b = b' + 1/2, c = c' + 1/2, d = d' + 1/2$, for some $a', b', c', d' \in \mathbb{Z}$. So, $a - c = a' - c' \in \mathbb{Z}, b - d = b' - d' \in \mathbb{Z}$.

Case 3: If only $a, b \in \mathbb{Z}$ but c, d are halves of odd integers, i.e., $c = c' + 1/2, d = d' + 1/2$. Then $a - c = (a - c') - 1/2, b - d = (b - d') - 1/2$ where $a - c', b - d' \in \mathbb{Z}$. So, $a - c, b - d$ are halves of odd integers.

Case 4: If a, b are halves of odd integers but $c, d \in \mathbb{Z}$. Then similar as in case 3, both $a - c, b - d$ are halves of odd integers.

Therefore, in all four cases, $(a - c) + (b - d)\sqrt{-3} \in I$. Based on the subgroup criteria, I is an additive subgroup of \mathbb{C} .

Next, I is a submonoid of the multiplicative monoid of \mathbb{C} . First note that since $1, 0 \in \mathbb{Z}$, then $1 = 1 + 0\sqrt{-3} \in I$. It remains to check that I is closed under multiplication. Note that $(a + b\sqrt{-3})(c + d\sqrt{-3}) = (ac - 3bd) + (ad + bc)\sqrt{-3}$. Then,

Case 1: If all $a, b, c, d \in \mathbb{Z}$, then $ac - 3bd, ad + bc \in \mathbb{Z}$ as well.

Case 2: If all a, b, c, d are halves of odd integers as before. Then, $ac - 3bd = (a' + 1/2)(c' + 1/2) - 3(b' + 1/2)(d' + 1/2) = a'c' + a'/2 + c'/2 + 1/4 - 3(b'd' + b'/2 + d'/2 + 1/4) = a'c' - 3b'd' + 1/2(a' + c' - 3b' - 3d') - 1/2$, which is an integer if $a' + c' - 3b' - 3d'$ is odd, and is a half of an odd integer if $a' + c' - 3b' - 3d'$ is even. Similarly, $ad + bc = a'd' + a'/2 + d'/2 + 1/4 + b'c' + b'/2 + c'/2 + 1/4 = a'd' + b'c' + 1/2(a' + b' + c' + d') + 1/2$, which is either an integer or a half of an odd integer.

Case 3: If $a, b \in \mathbb{Z}$ but c, d are halves of odd integers. Then consider $2(ac - 3bd) = 2a(c' + 1/2) - 6b(d' + 1/2) = 2ac' + 1 - 6bd' - 3 \in \mathbb{Z}$, which means that $ac - 3bd$ is either itself an integer or a half of an odd integer. Similarly, consider $2(ad + bc) = 2a(d' + 1/2) + 2b(c' + 1/2) = 2ad' + a + 2bc' + b \in \mathbb{Z}$, which means that $ad + bc$ is either itself an integer or a half of an odd integer.

Case 4: If $c, d \in \mathbb{Z}$ but a, b are halves of odd integers. Then similar to case 3, it reaches the same conclusion.

Therefore, in all four cases, $(ac - 3bd) + (ad + bc)\sqrt{-3} \in I$, i.e., I is closed under multiplication. I is a subring of \mathbb{C} . ■

Jacobson 2.2.1 *Proof.* Let a finite domain R be given. Pick any nonzero element $a \in R$. We aim to show that there exists $a^{-1} \in R$ such that $a^{-1}a = 1 = aa^{-1}$. It is suffice to show that a has both a right inverse a_R^{-1} and a left inverse a_L^{-1} ; if so, we have,

$$a_R^{-1} = (a_L^{-1}a)a_R^{-1} = a_L^{-1}(aa_R^{-1}) = a_L^{-1},$$

i.e., the left inverse equals to the right inverse, which means the inverse a^{-1} exists.

First note that since R is a domain, then the left cancellation law holds. To see this, assume $ax = ay$ for some $x, y \in R$, then $ax - ay = 0$, which gives $a(x - y) = 0$. Since $a \neq 0$ and we are in a domain, a is thus not a zero-divisor, which means that $x - y = 0 \implies x = y$.

Now since R is finite, we can enumerate all elements of R as

$$r_1, r_2, \dots, r_k,$$

for some positive integer k . And we claim that the following is also an enumeration of all elements of R ,

$$ar_1, ar_2, \dots, ar_k,$$

as it contains k distinct elements of R . Note that they are distinct because if $ar_i = ar_j$, then by left cancellation law established above, $r_i = r_j$. Therefore, there exists $1 \leq s \leq k$ such that $ar_s = 1$, i.e., $a_R^{-1} = r_s$. And by a similar argument as above, a must also have a left inverse a_L^{-1} . This proves that a^{-1} exists, which concludes the proof. ■

Jacobson 2.2.4 *Proof.* We show that $1 - ba$ has both a left inverse and a right inverse, and they are equal.

We name the inverse of $1 - ab$ as c . Then, we see that

$$\begin{aligned}
 (1 - ab)c = 1 &\implies c - abc = 1 \implies bc - babc = b \implies bca - babca = ba \\
 &\implies (1 - ba)bca = ba \implies (1 - ba)bca - ba = 0 \\
 &\implies (1 - ba)bca + (1 - ba) = 1 \\
 &\implies (1 - ba)(bca + 1) = 1.
 \end{aligned}$$

Therefore, $(1 - ba)_R^{-1}$ exists. Similarly,

$$\begin{aligned}
 c(1 - ab) = 1 &\implies c - cab = 1 \implies ca - caba = a \implies bca - bcaba = ba \\
 &\implies bca(1 - ba) = ba \implies bca(1 - ba) - ba = 0 \\
 &\implies bca(1 - ba) + (1 - ba) = 1 \\
 &\implies (bca + 1)(1 - ba) = 1.
 \end{aligned}$$

Therefore, $(1 - ba)_L^{-1}$ exists. Since $(1 - ba)_L^{-1} = bca + 1 = (1 - ba)_R^{-1}$, this concludes the proof. ■

Jacobson 2.2.6 *Proof.*



Jacobson 2.2.7 Proof.

■