

**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,

$$\begin{aligned} ac - 3bd &= (a' + 1/2)(c' + 1/2) - 3(b' + 1/2)(d' + 1/2) \\ &= a'c' + a'/2 + c'/2 + 1/4 - 3(b'd' + b'/2 + d'/2 + 1/4) \\ &= a'c' - 3b'd' + 1/2(a' + c' - 3b' - 3d') - 1/2, \end{aligned}$$

which is either an integer or a half of an odd integer. Note that  $ac - 3bd \in \mathbb{Z}$  iff  $a' + c' - 3b' - 3d'$  is odd, and  $ac - 3bd$  is a half of an odd integer iff  $a' + c' - 3b' - 3d'$  is even.

Similarly,

$$\begin{aligned} ad + bc &= a'd' + a'/2 + d'/2 + 1/4 + b'c' + b'/2 + c'/2 + 1/4 \\ &= a'd' + b'c' + 1/2(a' + b' + c' + d') + 1/2 \end{aligned}$$

which is either an integer or a half of an odd integer. Note that  $ad + bc \in \mathbb{Z}$  iff  $a' + b' + c' + d'$  is odd, and  $ad + bc$  is a half of an odd integer iff  $a' + b' + c' + d'$  is even.

Now, if  $(ad + bc) \in \mathbb{Z}$ , then  $a' + b' + c' + d'$  is odd. This means that either one or three of  $a', b', c', d'$  are odd. This gives that  $a' + c' - 3b' - 3d'$  is also odd, as multiplying by  $-3$  does not change the parity of an integer, which in turn gives that  $(ac - 3bd) \in \mathbb{Z}$ . And by a similar argument,  $(ac - 3bd) \in \mathbb{Z} \implies (ad + bc) \in \mathbb{Z}$ .

**Case 3:** If  $a, b \in \mathbb{Z}$  but  $c, d$  are halves of odd integers. Then,

$$\begin{aligned} ac - 3bd &= a(c' + 1/2) - 3b(d' + 1/2) \\ &= ac' + a/2 - 3bd' - 3b/2 \\ &= (ac' - 3bd') - (a - 3b)/2, \end{aligned}$$

which means that  $ac - 3bd$  is either an integer or a half of an integer. Note that  $ac - 3bd \in \mathbb{Z}$  iff  $a - 3b$  is even, and  $ac - 3bd$  a half of an odd integer iff  $a - 3b$  is odd.

Similarly,

$$\begin{aligned} ad + bc &= a(d' + 1/2) + b(c' + 1/2) \\ &= (ad' + bc') + (a + b)/2, \end{aligned}$$

which means that  $ad + bc$  is either an integer or a half on odd integer. Note that  $ad + bc \in \mathbb{Z}$  iff  $a + b$  is even, and  $ad + bc$  is half of an odd integer iff  $a + b$  is odd.

Now, if  $ac - 3bd \in \mathbb{Z}$ , then  $a - 3b$  is even. So  $a, b$  have the same parity, which means that  $a + b$  is even as well. This gives that  $ad + bc$  is an integer as well. And by a similar reasoning on parity,  $ad + bc \in \mathbb{Z} \implies ac - 3bd \in \mathbb{Z}$ .

**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,  $ac - 3bd$  and  $ad + bc$  are either both integers or both halves of odd integers. This means that  $(ac - 3bd) + (ad + bc)\sqrt{-3} \in I$ , 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.* We show equivalence by proving  $(1) \implies (3), (3) \implies (2)$ , and  $(2) \implies (1)$ .

$(1) \implies (3)$  : Suppose  $u$  has two distinct right inverses,  $x_1, x_2$ . Then  $ux_1 = 1 = ux_2$ , which gives that  $ux_1 - ux_2 = 0$ . Then by distributive law,  $u(x_1 - x_2) = 0$ . Since  $x_1 \neq x_2$ ,  $x_1 - x_2 \neq 0$ , which means that  $u$  is a left zero-divisor.

$(3) \implies (2)$  : Suppose  $u$  is a left zero-divisor, then there exists  $x \neq 0$  such that  $ux = 0$ . Now for the sake of contradiction, suppose that  $u$  is a unit, then  $u^{-1}$  exists. Therefore,

$$x = 1 \cdot x = (u^{-1}u)x = u^{-1}(ux) = u^{-1} \cdot 0 = 0.$$

This contradicts  $x \neq 0$ . Hence,  $u$  is not a unit.

$(2) \implies (1)$  : We do proof by contraposition. Suppose that  $u$  has a unique right inverse,  $x$ . Then  $ux = 1$ , and  $uxu = u$ , or  $uxu - u = 0$ . Therefore,  $uxu - u + ux = 1$ , i.e.,  $u(xu - 1 + x) = 1$ . Since  $u$  has a unique right inverse, then  $xu - 1 + x = x$ , which gives that  $xu = 1$ . So,  $x$  is also a left inverse  $u$ , which proves that  $u$  is a unit. ■

**Jacobson 2.2.7 Proof.** Suppose that element  $u$  in a ring  $R$  has one right inverse  $x$ . We then claim that the  $\{x_n\}_{n \in \mathbb{N}}$  is an infinite collection of distinct right inverses of  $u$ , where,

$$x_n = x + (1 - xu)u^n.$$

We first see that each  $x_n$  is a right inverse of  $u$ . Note that

$$\begin{aligned} ux_n &= u(x + (1 - xu)u^n) = ux + u(1 - xu)u^n = ux + (u - (ux)u)u^n \\ &= ux + (u - u)u^n = ux + 0 \cdot u^n \\ &= ux \\ &= 1. \end{aligned}$$

We next see that  $x_n \neq x_m$  if  $n \neq m$ . Suppose the contrary that  $n \neq m$  but  $x_n = x_m$  (WLOG assume  $n > m$ ). First notice that since  $u$  has a right inverse, then  $u$  is not a right zero-divisor, meaning that  $u$  obeys the right cancellation law. To see this, suppose  $au = bu$  for some  $a, b \in R$ . Then  $(a - b)u = 0$ . Note then that

$$0 = 0 \cdot x = [(a - b)u]x = (a - b)[ux] = a - b.$$

Therefore,  $a = b$ , i.e., we can cancel  $u$  on the right.

Going back the proof, if  $x_n = x_m$ , then

$$\begin{aligned} x + (1 - xu)u^n &= x + (1 - xu)u^m \implies (1 - xu)u^n = (1 - xu)u^m \\ &\implies (1 - xu)u^{n-m} = 1 - xu \quad (\text{cancel } u \text{ on the right}) \\ &\implies (1 - xu)u^{n-m} + xu = 1 \\ &\implies ((1 - xu)u^{n-m-1} + x)u = 1, \end{aligned}$$

i.e.,  $u$  has a left inverse, which means that  $u$  is a unit. However, we have established in the previous exercise that  $u$  is not a unit since  $u$  has more than one right inverse. Therefore,  $x_n \neq x_m$ , i.e., all  $x_n$ 's are distinct.

\* \* \*

Consider the following counter-example. Let  $R$  be the set of continuous functions on  $[0, +\infty)$ . Then as in Ex 2.1.1, we see that  $(R, \circ, \text{id})$  is a monoid. Consider the function  $f \in R$  where  $f(x) = x^2$  for all  $x \in [0, +\infty)$ . Suppose  $g$  is a right inverse of  $f$ , then we must have

$$\begin{aligned} (f \circ g)(x) &= x \implies f(g(x)) = x \\ &\implies g(x)^2 = x \\ &\implies g(x) = \pm\sqrt{x}. \end{aligned}$$

Since  $g$  has to be continuous, then either  $g(x) = +\sqrt{x}$  or  $g(x) = -\sqrt{x}$ , and only those two options. So  $f$  has exactly two right inverses, not infinitely many. ■