Solution for Homework 3

Xiangcan Li

March 22, 2021

Exercise 2.1.1 Prove that multiplication of complex numbers is associative. More precisely, let $z = a + bi$, $w = c + di$, and $v = g + hi$, and prove that $z(wv) = (zw)v$.

$$\begin{aligned}
z(wv) &= (a+bi)\big((c+di)(g+hi)\big) \\
&= (a+bi)\big(cg - dh + (ch+dg)i\big) \\
&= a(cg-dh) - b(ch+dg) + \big(a(ch+dg) + b(cg-dh)\big)i \\
&= acg - adh - bch - bdg + (ach + adg + bcg - bdh)i \\
(zw)v &= \big(ac - bd + (ad+bc)i\big)(g+hi) \\
&= (ac-bd)g - (ad+bc)h + \big((ac-bd)h + (ad+bc)g\big)i \\
&= acg - bdg - adh - bch + (ach - bdh + adg + bcg)i
\end{aligned}$$

Hence, $z(wv) = (zw)v$.
Since z, w, v are arbitrary, we conclude multiplication of complex numbers is associative.

Exercise 2.1.2 Let $z = a + bi$, $w = c + di \in \mathbb{C}$ and prove each of the following statements:
(i) $z + \overline{z}$ is real and $z - \overline{z}$ is imaginary.

$\overline{z} = a - bi$. Then $z + \overline{z} = a + bi + a - bi = 2a \in \mathbb{R}$.
$z - \overline{z} = a + bi - (a - bi) = 2bi = 0 + 2bi$. The real part is zero.
Hence, $z + \overline{z}$ is real and $z - \overline{z}$ is imaginary.

(ii) $\overline{z + w} = \overline{z} + \overline{w}$.

$z + w = a + bi + c + di = (a + c) + (b + d)i$. Then $\overline{z + w} = (a + c) - (b + d)i$.
$\overline{z} + \overline{w} = a - bi + c - di = a + c - (b + d)i$.
Hence, $\overline{z + w} = \overline{z} + \overline{w}$.

(iii) $\overline{zw} = \overline{z}\,\overline{w}$.

$zw = (a + bi)(c + di) = ac - bd + (ad + bc)i$. Then $\overline{zw} = ac - bd - (ad + bc)i$.
$\overline{z}\,\overline{w} = (a - bi)(c - di) = ac - adi - bci + bdi^2 = ac - bd - (ad + bc)i$.
Hence, $\overline{zw} = \overline{z}\,\overline{w}$.

Exercise 2.2.1 Prove that if $\mathbb{F}$ is a is a field and $a, b \in \mathbb{F}$ with $ab = 0$, then either $a = 0$ or $b = 0$.

Suppose $b = 0$, then done. Suppose $b \neq 0$, then there exists $b^{-1} \in \mathbb{F}$ such that $bb^{-1} = 1$.
Then we have $abb^{-1} = 0b^{-1} \implies a1 = 0 \implies a = 0$.
We conclude if $\mathbb{F}$ is a is a field and $a, b \in \mathbb{F}$ with $ab = 0$, then either $a = 0$ or $b = 0$.

Exercise 2.2.2 Prove that $\mathbb{Q}(\sqrt{2})$ is a field. Hint: you should use the fact that $\sqrt{2} \notin \mathbb{Q}$.

Let $z = a + b\sqrt{2}, w = c + d\sqrt{2}, v = g + h\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, where $a, b, c, d, g.h \in \mathbb{Q}$.
Since $\mathbb{Q} \subset \mathbb{R}$, $a, b, c, d, g, h, \sqrt{2} \in \mathbb{R}$.

(i)

$$\begin{aligned}
z + w &= a + b\sqrt{2} + c + d\sqrt{2} \\
&= (a + c) + (b + d)\sqrt{2} \\
w + z &= c + d\sqrt{2} + a + b\sqrt{2} \\
&= (a + c) + (b + d)\sqrt{2}
\end{aligned}$$

Then $z + w = w + c$.

$$\begin{aligned}
(z + w) + v &= (a + b\sqrt{2} + c + d\sqrt{2}) + g + h\sqrt{2} \\
&= (a + c + g) + (b\sqrt{2} + d\sqrt{2} + h\sqrt{2}) \\
z + (w + v) &= a + b\sqrt{2} + (c + d\sqrt{2} + g + h\sqrt{2}) \\
&= (a + c + g) + (b\sqrt{2} + d\sqrt{2} + h\sqrt{2})
\end{aligned}$$

Then $(z + w) + v = z + (w + v)$.

$$\begin{aligned}
zw &= (a + b\sqrt{2})(c + d\sqrt{2}) \\
&= ac + ad\sqrt{2} + bc\sqrt{2} + 2bd \\
wz &= (c + d\sqrt{2}(a + b\sqrt{2}) \\
&= ac + ad\sqrt{2} + bc\sqrt{2} + 2bd
\end{aligned}$$

Then $zw = wz$.

$$\begin{aligned}
z(wv) &= (a + b\sqrt{2})\big((c + d\sqrt{2})(g + h\sqrt{2})\big) \\
&= (a + b\sqrt{2})(cg + ch\sqrt{2} + dg\sqrt{2} + 2dh) \\
&= acg + ach\sqrt{2} + adg\sqrt{2} + bcg\sqrt{2} + 2adh + 2bch + 2bdg + 2\sqrt{2}bdh \\
(zw)v &= \big((a + b\sqrt{2})(c + d\sqrt{2})\big)(g + h\sqrt{2}) \\
&= (ac + ad\sqrt{2} + bc\sqrt{2} + 2bd)(g + h\sqrt{2}) \\
&= acg + ach\sqrt{2} + adg\sqrt{2} + bcg\sqrt{2} + 2adh + 2bch + 2bdg + 2\sqrt{2}bdh
\end{aligned}$$

Then $z(wv) = (zw)v$.

We conclude addition and multiplication are commutative, associative operations.

(ii)

$$\begin{aligned}
z(w + v) &= (a + b\sqrt{2})\big((c + d\sqrt{2}) + (g + h\sqrt{2})\big) \\
&= (a + b\sqrt{2})(c + g + d\sqrt{2} + h\sqrt{2}) \\
&= ac + ag + ad\sqrt{2} + ah\sqrt{2} + cd\sqrt{2} + bg\sqrt{2} + 2bd + 2bh \\
zw + zv &= (a + b\sqrt{2})(c + d\sqrt{2}) + (a + b\sqrt{2})(g + h\sqrt{2}) \\
&= ac + ad\sqrt{2} + cd\sqrt{2} + 2bd + ag + ah\sqrt{2} + bg\sqrt{2} + 2bh \\
&= ac + ag + ad\sqrt{2} + ah\sqrt{2} + cd\sqrt{2} + bg\sqrt{2} + 2bd + 2bh
\end{aligned}$$

Then $z(w+v) = zw + zv$.

We conclude multiplication distributes over addition.

(iii) Since $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, let $a, b = 0 \in \mathbb{Q}$, then $0 + 0\sqrt{2} = 0 \in \mathbb{Q}(\sqrt{2})$. Hence, there exists an additive identity denoted $0 \in \mathbb{Q}(\sqrt{2})$.

(iv) For all $\alpha = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, there exists an additive inverse denoted $-\alpha = -a - b\sqrt{2}$, such that $-\alpha + \alpha = 0$.

(v) Since $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, let $a = 1, b = 0 \in \mathbb{Q}$, then $1 + 0\sqrt{2} = 1 \in \mathbb{Q}(\sqrt{2})$. Hence, there exists a multiplicative identity denoted $1 \in \mathbb{Q}(\sqrt{2})$ with $1 \neq 0$: $1a = a$ for all $a \in \mathbb{Q}(\sqrt{2})$.

(vi) We first prove the following proposition: the product of a non-zero rational number and an irrational number is irrational.

Proof. Suppose a is a non-zero rational number and x is an irrational number. Then we can write a as $a = b/c$ for some non-zero integers b and c.

Suppose for contradiction, the product of a non-zero rational number and an irrational number is rational, then ax is rational. We can write ax as $ax = m/n$ for some non-zero integers m and n. Therefore, $x = m/an = cm/bn$. Note that both cm and bn are non-zero integers. Then x is rational, which is a contradiction.

We conclude that the product of a non-zero rational number and an irrational number is irrational. $\square$

Suppose $z = a + b\sqrt{2} \neq 0$, we will discuss in two cases.

Suppose $b = 0$, then $a \neq 0$. Then $z = a$ and $z^{-1} = a^{-1} \in \mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$.

Suppose $b \neq 0$, then b is a non-zero rational number by definition. Since $\sqrt{2}$ is an irrational number, by the proposition above, we have $b\sqrt{2}$ is irrational. Then $a \neq b\sqrt{2}$. Hence, $a - b\sqrt{2} \neq 0$.

Then we have

$$\begin{aligned} z^{-1} &= \frac{1}{a + b\sqrt{2}} \\ &= \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} \\ &= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\ &= \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}. \end{aligned}$$

Since $a, b \in \mathbb{Q}$, by the axioms of the field, we have $\frac{a}{a^2 - 2b^2}, \frac{-b}{a^2 - 2b^2} \in \mathbb{Q}$. Therefore, $z^{-1} \in \mathbb{Q}(\sqrt{2})$.

Therefore, for every nonzero element $z \in \mathbb{Q}(\sqrt{2}) - \{0\}$ has a multiplicative inverse z^{-1}, such that $zz^{-1} = 1$.

We conclude $\mathbb{Q}(\sqrt{2})$ is a field.

Exercise 2.3.1 Prove parts (iii)-(v) of Proposition 2.3.2:
Suppose $\mathbb{F}$ is a field.
(i) Addition and multiplication are commutative, associative operations on $\mathbb{F}[x]$ which restrict to the operations of addition and multiplication on $\mathbb{F} \subset \mathbb{F}[x]$.
(ii) Multiplication distributes over addition: $f(g + h) = fg + gh$ for all $f, g, h \in \mathbb{F}[x]$.
(iii) $0 \in \mathbb{F}$ is an additive identity in $\mathbb{F}[x]$: $f + 0 = f$ for all $f \in \mathbb{F}[x]$.

We have

$$f = \sum_{k=0}^{n} a_k x^k \text{ and } 0 = \sum_{j=0}^{n} b_j x^j,$$

then

$$f + 0 = \sum_{k=0}^{n} (a_k + 0)x^k = \sum_{k=0}^{n} (a_k)x^k = f.$$

We conclude $0 \in \mathbb{F}$ is an additive identity in $\mathbb{F}[x] : f + 0 = f$ for all $f \in \mathbb{F}[x]$.

(iv) Every $f \in \mathbb{F}[x]$ has an additive inverse given by $-f = (-1)f$ with $f + (-f) = 0$.

We have

$$-f = (-1)f = (-1)\sum_{k=0}^{n} a_k x^k = \sum_{k=0}^{n} (-a_k)x^k,$$

then

$$f + (-f) = \sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{n} (-a_k)x^k = \sum_{k=0}^{n} (a_k - a_k)x^k = \sum_{k=0}^{n} 0x^k = 0.$$

We conclude every $f \in \mathbb{F}[x]$ has an additive inverse given by $-f = (-1)f$ with $f + (-f) = 0$.

(v) $1 \in \mathbb{F}$ is the multiplicative identity in $\mathbb{F}[x] : 1f = f$ for all $f \in \mathbb{F}[x]$.

We have

$$1f = 1\sum_{k=0}^{n} a_k x^k = \sum_{k=0}^{n} (1a_k)x^k = \sum_{k=0}^{n} a_k x^k = f.$$

We conclude $1 \in \mathbb{F}$ is the multiplicative identity in $\mathbb{F}[x] : 1f = f$ for all $f \in \mathbb{F}[x]$.