Solution for Homework 9

Xiangcan Li

January 15, 2021

Exercise 1 Let $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, and define the operation $+$ in $\mathbb{Z}[i]$ as ordinary addition (as in $\mathbb{C}$).

(a) Prove that $(\mathbb{Z}, +)$ is a normal subgroup of $(\mathbb{Z}[i], +)$.

Let g be an arbitrary element in $(\mathbb{Z}[i], +)$. Then $g = a + bi$ for some $a, b \in \mathbb{Z}$. Let h be an arbitrary element in $(\mathbb{Z}, +)$, then $h = p$ for some $p \in \mathbb{Z}$.

We have

$$\begin{aligned} ghg^{-1} &= (a + bi) + p - (a + bi) \\ &= (a - a) + (bi - bi) + p \\ &= p \in \mathbb{Z} \end{aligned}$$

Since g, h are arbitrary, for all $g \in G$, $g(\mathbb{Z}, +)g^{-1} = (\mathbb{Z}, +)$. Then $(\mathbb{Z}, +)$ is a normal group of $(\mathbb{Z}[i], +)$.

(b) Prove that the quotient group $\mathbb{Z}[i]/\mathbb{Z}$ (with operation $+$) is an abelian group.

Let g, h be defined the same in (a). Then $gh = a + bi + p = (a + p) + bi$.

Note that $a + p \in \mathbb{Z}$ and $b \in \mathbb{Z}$.

Since h is an arbitrary element in $(\mathbb{Z}, +)$, we have $(\mathbb{Z}[i], +)/(\mathbb{Z}, +) = \{g(\mathbb{Z}, +) \mid g \in (\mathbb{Z}[i], +)\} = \{m + ni \mid m, n \in \mathbb{Z}\}$.

Let p, q be two arbitrary elements in $(\mathbb{Z}[i], +)/(\mathbb{Z}, +)$, then $p = s + ti$ and $q = k + li$ for some $s, t, k, l \in \mathbb{Z}$.

$$\begin{aligned} p + q &= s + ti + k + li = (s + k) + (t + l)i \\ q + p &= k + li + s + ti = (k + s) + (l + t)i = (s + k) + (t + l)i \end{aligned}$$

Hence, $p + q = q + p$. Since p and q are arbitrary, $(\mathbb{Z}[i], +)/(\mathbb{Z}, +)$ is an abelian group.

(c) Let (5) denote the set $(5) = \{5a + 5bi \mid a, g \in \mathbb{Z}\}$. Prove that (5) is a normal subgroup of $\mathbb{Z}[i]$.

Let g be an arbitrary element in $(\mathbb{Z}[i], +)$. Then $g = a + bi$ for some $a, b \in \mathbb{Z}$. Let h be an arbitrary element in $((5), +)$, then $h = 5m + 5ni$ for some $m, n \in \mathbb{Z}$.

We have

$$\begin{aligned} ghg^{-1} &= (a + bi) + 5m + 5ni - (a + bi) \\ &= (a - a) + (bi - bi) + 5m + 5ni \\ &= 5m + 5ni \in \mathbb{Z} \end{aligned}$$

Since g, h are arbitrary, for all $g \in G$, $g((5), +)g^{-1} = ((5), +)$. Then $((5), +)$ is a normal group of $(\mathbb{Z}[i], +)$.

(d) Prove that $\mathbb{Z}[i]/(5)$ is an abelian group (with operation $+$).

Let g, h be defined the same in (c). Then $gh = a + bi + 5m + 5ni = (a + 5m) + (b + 5n)i$.

Note that $a + 5m \in [a]_5$ and $b + 5n \in [b]_5$.

Since h is an arbitrary element in $((5), +)$, we have $\mathbb{Z}[i]/(5) = \{g(5) \mid g \in \mathbb{Z}[i]\} = \{[a]_5 + [b]_5 i \mid a, b \in \mathbb{Z}\}$.

Let p, q be two arbitrary elements in $\mathbb{Z}[i]/(5)$, then $p = [s]_5 + [t]_5 i$ and $q = [k]_5 + [l]_5 i$ for some $s, t, k, l \in \mathbb{Z}$.

$$\begin{aligned} p + q &= [s]_5 + [t]_5 i + [k]_5 + [l]_5 i = [s + k]_5 + [t + l]_5 i \\ q + p &= [k]_5 + [l]_5 i + [s]_5 + [t]_5 i = [k + s]_5 + [l + t]_5 i = [s + k]_5 + [t + l]_5 i \end{aligned}$$

Hence, $p + q = q + p$. Since p and q are arbitrary, $\mathbb{Z}[i]/(5)$ is an abelian group.

Exercise 2 Over the course of the parts of this exercise you will show that multiplication of cosets in $\mathbb{Z}[i]/\mathbb{Z}$ is not well-defined.

(a) Let $a, a', b, b' \in \mathbb{Z}$. Prove that $a + i$ and $a' + i$ represent the same coset in $\mathbb{Z}[i]/\mathbb{Z}$; that is, prove that

$$(a + i) + \mathbb{Z} = (a' + i) + \mathbb{Z}.$$

Note that $a + \mathbb{Z} = \{a + n \mid n \in \mathbb{Z}\}$.

Let $c \in \mathbb{Z}$, then $c = a + (c - a)$, where $c - a \in \mathbb{Z}$ since $a, c \in \mathbb{Z}$. Hence, $c \in a + \mathbb{Z}$. Then we have $\mathbb{Z} \subset a + \mathbb{Z}$.

Let $c \in \{a + n \mid n \in \mathbb{Z}\}$, then $c = a + c'$ for some $c' \in \mathbb{Z}$. Since $a, c' \in \mathbb{Z}$, $c = a + c' \in \mathbb{Z}$. Then we have $a + \mathbb{Z} \subset \mathbb{Z}$.

We conclude $a + \mathbb{Z} = \mathbb{Z}$.

Similarly, $a' + \mathbb{Z} = \mathbb{Z}$.

Hence, $(a + i) + \mathbb{Z} = (a + \mathbb{Z}) + i = \mathbb{Z} + i = (a' + \mathbb{Z}) + i = (a' + i) + \mathbb{Z}$.

(b) Prove that b and b' represent the same coset in $\mathbb{Z}[i]/\mathbb{Z}$; that is, prove that

$$b + \mathbb{Z} = b' + \mathbb{Z}.$$

Note that $b + \mathbb{Z} = \{b + n \mid n \in \mathbb{Z}\}$.

Let $c \in \mathbb{Z}$, then $c = b + (c - b)$, where $c - b \in \mathbb{Z}$ since $b, c \in \mathbb{Z}$. Hence, $c \in b + \mathbb{Z}$. Then we have $\mathbb{Z} \subset b + \mathbb{Z}$.

Let $c \in \{b + n \mid n \in \mathbb{Z}\}$, then $c = b + c'$ for some $c' \in \mathbb{Z}$. Since $b, c' \in \mathbb{Z}$, $c = b + c' \in \mathbb{Z}$. Then we have $b + \mathbb{Z} \subset \mathbb{Z}$.

We conclude $b + \mathbb{Z} = \mathbb{Z}$.

Similarly, $b' + \mathbb{Z} = \mathbb{Z}$.

Hence, $b + \mathbb{Z} = \mathbb{Z} + i = b' + \mathbb{Z}$.

(c) Determine the conditions under which $(a + i)b$ and $(a' + i)b'$ represent the same coset in $\mathbb{Z}[i] = \mathbb{Z}$. That is, determine what additionally must be assumed in order to ensure that

$$(a + i)b + \mathbb{Z} = (a' + 1)b' + \mathbb{Z}.$$

Be sure to prove your condition is the correct one.

$(a + i)b + \mathbb{Z} = (a' + i)b' + \mathbb{Z}$ if and only if $b = b'$.

- Note that $ab \in \mathbb{Z}$ since $a, b \in \mathbb{Z}$ and $ab + \mathbb{Z} = \{ab + n \mid n \in \mathbb{Z}\}$.
  Let $c \in \mathbb{Z}$, then $c = ab + (c - ab)$, where $c - ab \in \mathbb{Z}$ since $ab, c \in \mathbb{Z}$. Hence, $c \in ab + \mathbb{Z}$. Then we have $\mathbb{Z} \subset ab + \mathbb{Z}$.
  Let $c \in \{ab + n \mid n \in \mathbb{Z}\}$, then $c = ab + c'$ for some $c' \in \mathbb{Z}$. Since $ab, c' \in \mathbb{Z}$, $c = ab + c' \in \mathbb{Z}$. Then we have $ab + \mathbb{Z} \subset \mathbb{Z}$.
  We conclude $ab + \mathbb{Z} = \mathbb{Z}$.
  Similarly, $a'b' + \mathbb{Z} = \mathbb{Z}$.
  Then we have

$$\begin{aligned}(a + i)b + \mathbb{Z} &= (ab + \mathbb{Z}) + ib \\ &= \mathbb{Z} + ib \\ &= (a'b' + \mathbb{Z}) + ib.\end{aligned}$$

Then $(a'b' + \mathbb{Z}) + ib = (a' + i)b' + \mathbb{Z} = (a'b' + \mathbb{Z}) + ib'$. Therefore, $b = b'$.

- If $b = b'$, $(a+i)b + \mathbb{Z} = (a+i)b' + \mathbb{Z} = (ab' + \mathbb{Z}) + ib'$.
  Note that $ab' \in \mathbb{Z}$ since $a, b' \in \mathbb{Z}$ and $ab' + \mathbb{Z} = \{ab' + n \mid n \in \mathbb{Z}\}$.
  Let $c \in \mathbb{Z}$, then $c = ab' + (c - ab')$, where $c - ab' \in \mathbb{Z}$ since $ab', c \in \mathbb{Z}$. Hence, $c \in ab' + \mathbb{Z}$. Then we have $\mathbb{Z} \subset ab' + \mathbb{Z}$.
  Let $c \in \{ab' + n \mid n \in \mathbb{Z}\}$, then $c = ab' + c'$ for some $c' \in \mathbb{Z}$. Since $ab', c' \in \mathbb{Z}$, $c = ab' + c' \in \mathbb{Z}$. Then we have $ab' + \mathbb{Z} \subset \mathbb{Z}$.
  We conclude $ab' + \mathbb{Z} = \mathbb{Z}$.
  Then we have $(a+i)b + \mathbb{Z} = (ab' + \mathbb{Z}) + ib' = \mathbb{Z} + ib' = (a'b' + \mathbb{Z}) + ib' = (a' + i)b' + \mathbb{Z}$.

We conclude the condition is $b = b'$.

(d) Find specific values of $a, a', b, b' \in \mathbb{Z}$ for which $(a+i)b + \mathbb{Z} = (a'+i)b' + \mathbb{Z}$.

From (c), we know that If $(a+i)b + \mathbb{Z} = (a'+i)b' + \mathbb{Z}$, then $b = b'$. The contrapositive is If $b \neq b'$, then $(a+i)b + \mathbb{Z} \neq (a'+i)b' + \mathbb{Z}$.

Hence, a and a' can be any arbitrary value in $\mathbb{Z}$ and we need to ensure $b \neq b'$.

Hence, $a = a' = 1, b = 1, b' = 2$ satisfies what we need.

Exercise 3 In this exercise you will show that multiplication of cosets in $\mathbb{Z}[i]/(5)$ is well-defined.

(a) Prove that $a + bi$ and $a' + b'i$ represent the same cosets in $\mathbb{Z}[i]/(5)$ if and only if $a \equiv a' (\text{mod } 5)$ and $b \equiv b' (\text{mod } 5)$.

- $\implies$: Note that $a + bi + (5) = \{a + bi + 5m + 5ni \mid m, n \in \mathbb{Z}\}$ and $a' + b'i + (5) = \{a' + b'i + 5m + 5ni \mid m, n \in \mathbb{Z}\}$.
  Since $a + bi + (5) = a' + b'i + (5)$, for some arbitrary element $s = a + bi + 5p + 5qi \in a + bi + (5)$, $s \in a' + b'i + (5)$. We can then write s as $a' + b'i + 5p' + 5q'i$ for some $p', q' \in \mathbb{Z}$.
  Then we have

$$\begin{aligned} & a + bi + 5p + 5qi = a' + b'i + 5p' + 5q'i \\ \implies & (a + 5p) + (b + 5q)i = (a' + 5p') + (b' + 5q') \\ \implies & a + 5p = a' + 5p', b + 5p = b' + 5p' \\ \implies & a - a' = 5(p' - p), b - b' = 5(p' - p) \end{aligned}$$

  Since $p' - p \in \mathbb{Z}$, $a \equiv a' (\text{mod } 5)$ and $b \equiv b' (\text{mod } 5)$.
- $\impliedby$: Since $a \equiv a' (\text{mod } 5)$ and $b \equiv b' (\text{mod } 5)$, we have $a - a' = 5k$ and $b - b' = 5m$ for some $k, m \in \mathbb{Z}$. Then $a = a' + 5k, b = b' + 5m, a' = a - 5k$ and $b' = b - 5m$.
  Note that $a + bi + (5) = \{a + bi + 5m + 5ni \mid m, n \in \mathbb{Z}\}$ and $a' + b'i + (5) = \{a' + b'i + 5m + 5ni \mid m, n \in \mathbb{Z}\}$.
  Let $s = a + bi + 5p + 5qi \in a + bi + (5)$ for some $p, q \in \mathbb{Z}$. Then

$$\begin{aligned} s &= a' + 5k + (b' + 5m)i + 5p + 5qi \\ &= a' + 5k + b'i + 5mi + 5p + 5qi \\ &= a' + b'i + 5(k + p) + 5(m + q)i \in a' + b'i + (5) \end{aligned}$$

  Hence, $a + bi + (5) \subset a' + b'i + (5)$.
  Similarly, let $t = a' + b'i + 5p + 5qi \in a' + b'i + (5)$ for some $p, q \in \mathbb{Z}$. Then

$$\begin{aligned} t &= a - 5k + (b - 5m)i + 5p + 5qi \\ &= a - 5k + bi - 5mi + 5p + 5qi \\ &= a + bi + 5(p - k) + 5(q - m)i \in a + bi + (5) \end{aligned}$$

  Hence, $a' + b'i + (5) \subset a + bi + (5)$.
  We conclude $a + bi + (5) = a' + b'i + (5)$.

(b) Show that multiplication of cosets is well-defined for $\mathbb{Z}[i]/(5)$. In other words, prove that if $r, r', s, s' \in \mathbb{Z}[i]$ with $r + (5) = r' + (5)$ and $s + (5) = s' + (5)$ then $rs + (5) = r's' + (5)$.

Write $r = a + bi, r' = a' + b'i, s = m + ni, s' = m' + n'i$.

Since $r + (5) = r' + (5)$ and $s + (5) = s' + (5)$, by (a), $a \equiv a' (\text{mod } 5), b \equiv b' (\text{mod } 5), m \equiv m' (\text{mod } 5)$ and $n \equiv n' (\text{mod } 5)$. Hence, $a - a' = 5\alpha, b - b' = 5\beta, m - m' = 5\gamma$ and $n - n' = 5\xi$ for some $\alpha, \beta, \gamma, \xi \in \mathbb{Z}$.

We have

$$\begin{aligned}
rs &= (a + bi)(m + ni) \\
&= am + ani + bmi + bni^2 \\
&= am - bn + (an + bm)i \\
&= (a' + 5\alpha)(m' + 5\gamma) - (b' + 5\beta)(n' + 5\xi) + \big((a' + 5\alpha)(n' + 5\xi) + (b' + 5\beta)(m' + 5\gamma)\big)i \\
&= a'm' + 5a'\gamma + 5m'\alpha + 25\alpha\gamma - b'n' - 5b'\xi - 5n'\beta - 25\beta\xi + \\
&\quad a'n'i + 5a'\xi i + 5n'\alpha i + 25\beta\xi i + b'm'i + 5b'\gamma i + 5m'\beta i + 25\beta\gamma i \\
&= a'm' - b'n' + (a'n' + b'm')i + 5(a'\gamma + m'\alpha + 5\alpha\gamma - b'\xi - n'\beta - 5\beta\xi) + \\
&\quad 5(a'\xi + n'\alpha + 5\beta\xi + b'\gamma + m'\beta + 5\beta\gamma)i \\
r's' &= (a' + b'i)(m' + n'i) \\
&= a'm' - b'n' + (a'n' + b'm')i
\end{aligned}$$

Let $\sigma = a'\gamma + m'\alpha + 5\alpha\gamma - b'\xi - n'\beta - 5\beta\xi$ and $\tau = a'\xi + n'\alpha + 5\beta\xi + b'\gamma + m'\beta + 5\beta\gamma$, then

$$rs = a'm' - b'n' + (a'n' + b'm')i + 5\sigma + 5\tau i = r's' + 5\sigma + 5\tau i.$$

Note that $\sigma, \tau \in \mathbb{Z}$ since $\mathbb{Z}$ is closed under addition and multiplication.

Let $\mu = rs + (5p + 5qi) \in (5)$ for some $p, q \in \mathbb{Z}$. Then we have

$$\begin{aligned}
\mu &= r's' + 5\sigma + 5\tau i + (5p + 5qi) \\
&= r's' + 5(\sigma + p) + 5(\tau + q)i
\end{aligned}$$

Note that $\sigma + p, \tau + q \in \mathbb{Z}$ since $\sigma, p, \tau, q \in \mathbb{Z}$. Then $5(\sigma + p) + 5(\tau + q)i \in (5)$. Hence, $\mu \in r's' + (5)$.

Therefore, $rs + (5) \subset r's' + (5)$.

For $\varphi = r's' + 5p' + 5q'i \in r's' + (5)$, we have

$$\begin{aligned}
\varphi &= rs - (5\sigma + 5\tau i) + 5p' + 5q'i \\
&= rs + 5(p' - \sigma) + 5(q' - \tau)i
\end{aligned}$$

Note that $p' - \sigma, q' - \tau \in \mathbb{Z}$ since $p', \sigma, q', \tau \in \mathbb{Z}$. Then $5(p' - \sigma) + 5(q' - \tau)i \in (5)$. Hence, $\varphi \in rs + (5)$.

Therefore, $r's' + (5) \subset rs + (5)$.

We conclude $rs + (5) = r's' + (5)$.

Exercise 3.6.11 Suppose R is a ring and $\mathcal{J} \subset R$ is a (two-sided) ideal (see Exercise 3.3.13 for the definition of an ideal). The quotient additive group $R/\mathcal{J}$ is the set of cosets, which in the additive notation have the form $r + \mathcal{J}$, for $r \in R$.

(a) Prove that

$$(r + \mathcal{J})(s + \mathcal{J}) = rs + \mathcal{J}$$

well-defines an operation on $R/\mathcal{J}$. In other words, prove that if $r + \mathcal{J} = r' + \mathcal{J}$ and $s + \mathcal{J} = s' + \mathcal{J}$, then $rs + \mathcal{J} = r's' + \mathcal{J}$.

Let $j \in \mathcal{J}$ and $m = r + j \in r + \mathcal{J}$. Then $m \in r' + \mathcal{J}$. Hence, $m = r' + j'$ for some $j' \in \mathcal{J}$. Similarly, let $n = s + k = s' + k' \in \mathcal{J}$ for some $k, k' \in \mathcal{J}$.

We have $mn = (r+j)(s+k) = rs + rk + js + jk$. Since $r \in R, s \in \mathcal{J}$ and $\mathcal{J}$ is an ideal, $rk \in \mathcal{J}$. Similarly, $js \in \mathcal{J}$. Since $\mathcal{J}$ is a subring, $j, k \in \mathcal{J}$, $jk \in \mathcal{J}$. Then $rk + js + jk \in \mathcal{J}$. Hence, $mn \in rs + \mathcal{J}$.

We also have $mn = (r'+j')(s'+k') = r's' + r'k' + j's' + j'k'$. Similarly, $r'k' + j's' + j'k' \in \mathcal{J}$. Hence, $mn \in r's' + \mathcal{J}$.

Since $mn \in rs + \mathcal{J}$ and $mn \in r's' + \mathcal{J}$, we have $rs + \mathcal{J} \subset r's' + \mathcal{J}$ and $r's' + \mathcal{J} \subset rs + \mathcal{J}$. We conclude $rs + \mathcal{J} = r's' + \mathcal{J}$.

(b) Prove that the definition of coset multiplication in part (a) makes $R/\mathcal{J}$ into a ring.

- Note that $(R/\mathcal{J}, +)$ is a group. Then there is an additive identity and additive inverse in $R/\mathcal{J}$, we need to prove $(R/\mathcal{J}, +)$ is abelian.
  Let $m = r + j, n = s + k \in r + \mathcal{J}$ for some $r, s \in R$ and $j, k \in \mathcal{J} \subset R$.
  Note that $r, s, j, k \in R$ and R is a ring.
  Then we have $m + n = (r + j) + (s + k) = (s + k) + (r + j) = n + m$. Hence, $(R/\mathcal{J}, +)$ is an abelian group.
- Let $m = r+j, n = s+k \in r+\mathcal{J}$ for some $r, s \in R$ and $j, k \in \mathcal{J} \subset R$. Note that $r, s, j, k, rs, rk, js, jk \in R$ and R is a ring.
  Then we have

$$\begin{aligned} mn &= (r+j)(s+k) \\ &= rs + rk + js + jk \\ &= rs + js + rk + jk && (R,+) \text{ is an abelian group} \\ &= sr + sj + kr + kj && \text{Multiplication is associative in } R \\ &= (s+k)(r+j) \\ &= nm \end{aligned}$$

  Hence, multiplication is associative in $r + \mathcal{J}$.
- Let $m = r + j, n = s + k, p = t + l \in r + \mathcal{J}$ for some $r, s, t \in R$ and $j, k, l \in \mathcal{J} \subset R$. Note that $r, s, t, j, k, l, rs, rk, rt, rl, js, jk, jt, jl \in R$ and R is a ring.
  Then we have

$$\begin{aligned} m(n+p) &= (r+j)(s+k+t+l) \\ &= rs + rk + rt + rl + js + jk + jt + jl \\ &= (rs + rk + js + jk) + (rt + rl + jt + jl) && \text{Multiplication is associative in } R \\ &= (r+j)(s+k) + (r+j)(t+l) \\ &= mn + mp \end{aligned}$$

  Hence, multiplication distributes over addition in $r + \mathcal{J}$.

We conclude $R/\mathcal{J}$ is a ring.

(c) Prove that the quotient group homomorphism $\pi : R \to R/\mathcal{J}$ is also a ring homomorphism.

Note that $\mathcal{J} + \mathcal{J} = \mathcal{J}$ since $\mathcal{J}$ is a ring.

We have

$$\phi(sr) = sr + \mathcal{J} = (s + \mathcal{J})(r + \mathcal{J}) = \phi(s)\phi(r)$$

and

$$\phi(s + r) = s + r + \mathcal{J} = (s + \mathcal{J}) + (r + \mathcal{J}) = \phi(s) + \phi(r).$$

Hence, $\pi : R \to R/\mathcal{J}$ is also a ring homomorphism.

Exercise 3.6.12 Prove the *First Isomorphism Theorem of Rings*: If $\phi : R \to S$ is a surjective ring homomorphism, then there exists a unique ring isomorphism

$$\tilde{\phi} = R/\ker(\phi) \to S$$

such that $\tilde{\phi}\pi = \phi$.

Let $g, h \in R$ and $N = \ker(\phi)$.
Note that ϕ is ring homomorphism and π is homomorphism.
Then we have

$$\tilde{\phi}((gN)(hN)) = \tilde{\phi}(\pi(g)\pi(h)) = \tilde{\phi}(\pi(gh)) = \phi(gh) = \phi(g)\phi(h) = \tilde{\phi}(\pi(g))\tilde{\phi}(\pi(h)) = \tilde{\phi}(gN)\tilde{\phi}(hN)$$

$$\tilde{\phi}(gN + hN) = \tilde{\phi}((g+h)N) = \tilde{\phi}(\pi(g+h)) = \phi(g+h) = \phi(g) + \phi(h) = \tilde{\phi}(\pi(g)) + \tilde{\phi}(\pi(h)) = \tilde{\phi}(gN) + \tilde{\phi}(hN).$$

Hence, there exists a unique ring isomorphism $\tilde{\phi} = R/\ker(\phi) \to S$ such that $\tilde{\phi}\pi = \phi$.