Homework

Ding Yaoyao, 516030910572

2017-12-01

Exercise 3-1

1

(1)

Beacuse the operation $\oplus$ does not satisfy $(a \oplus b) \oplus c = a \oplus (b \oplus c)$, S does not form a ring.

(2)

Beacuse the operations $\oplus$ and $*$ do not satisfy $(a \oplus b) * c = (a * c) \oplus (b * c)$, S does not form a ring.

(3)

S does not form a ring by the same reason of (2).

4

Let $u, v, w \in Z[\sqrt{3}]$ and $u = a_1 + b_1\sqrt{3}$, $v = a_2 + b_2\sqrt{3}$, $w = a_3 + b_3\sqrt{3}$.

- closure: $u+v = (a_1+b_1\sqrt{3})+(a_2+b_2\sqrt{3}),= (a_1+a_2)+(b_1+b_2)\sqrt{3} \in Z[\sqrt{3}]$.
- associativity: $(u+v)+w = (a_1+a_2+a_3)+(b_1+b_2+b_3)\sqrt{3} = u+(v+w)$.
- identity: $0 + u = u + 0 = u$, so 0 is an identity.
- inverse: Let $u^{-1} = (-a_1) + (-b_1)\sqrt{3}$, then $uu^{-1} = u^{-1}u = 0$.
- abelian: $u + v = (a_1 + b_1\sqrt{3}) + (a_2 + b_2\sqrt{3}) = v + u$.

Then $(Z[\sqrt{3}], +)$ is an abelian group.

- closure: $uv = (a_1a_2 + 3b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{3} \in Z[\sqrt{3}]$.
- associativity: $(uv)w = (a_1a_2a_3 + 3a_1b_2b_3 + 3a_2b_1b_2 + 3a_3b_1b_2) + (b_1a_2a_3 + b_2a_1a_3 + b_3a_1a_2)\sqrt{3} = u(vw)$.

- identity: $1u = u1 = u$, so 1 is an identity.
- abelian: $uv = vu$.

Then $(Z[\sqrt{3}], \cdot)$ is an abelian monoid. Also

$$\begin{aligned}(u+v)w &= [(a_1+a_2)+(b_1+b_2)\sqrt{3}](a_3+b_3\sqrt{3}) \\ &= (a_1+b_1\sqrt{3})(a_3+b_3\sqrt{3})+(b_1+b_2\sqrt{3})(a_3+b_3\sqrt{3}) \\ &= uw+vw\end{aligned}$$

Similarly, $w(u+v) = wu + wv$. So $+$ and $\cdot$ satisfy distributive laws.
Above all, $(Z[\sqrt{3}, +, \cdot)$ is an abelian ring with identity.

17

(2)(3)(4).

18

(1)(4).

Exercise 3-2

2

Let $u, v, w \in Z[\theta]$ and $u = a_1 + b_1\theta, v = a_2 + b_2\theta, w = a_3 + b_3\theta$.

- closure: $u + v = (a_1 + a_2) + (b_1 + b_2)\theta \in Z[\theta]$.
- associativity: $(u + v) + w = u + (v + w)$(For all $u, v, w \in \mathbb{C}$).
- identity: $0 \in Z[\theta]$ and $0 + u = u + 0 = u$, so 0 is the identity.
- inverse: Let $(-u) = (-a_1)+(-b_1)\theta \in Z[\theta]$, then $u+(-u) = (-u)+u = 0$.
- abelian: $uv = vu$(For all $u, v \in \mathbb{C}$).

Then $(Z[\theta], +)$ is an abelian group.

- closure: $uv = (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1 + b_1b_2)\theta \in Z[\theta]$.
- associativity: $(uv)w = u(vw)$(For all $u, v \in \mathbb{C}$).
- identity: Let $e = 1 \in Z[\theta]$ and e satisfy $eu = ue = u$, so e is the identity.
- abelian: $uv = vu$(For all $u, v \in \mathbb{C}$).
- no zeros: If $u \neq 0$ and $v \neq 0$, then $uv \neq 0$(For all $u, v \in \mathbb{C}$).

$(u+v)w = uw + vw$ and $w(u+v) = wu + wv$ are true for all $u, v \in \mathbb{C}$.

Above all, $(Z[\theta], +, \cdot)$ is an integral domain.

If u is a unit, then

$$\frac{1}{u} = \frac{1}{a+b\theta} = \frac{a+b-b\theta}{a^2+b^2+ab}$$

then we have

$$a^2 + b^2 + ab \mid a + b$$

Then we have $u = 1, -1, \theta, -\theta, 1-\theta, \theta-1$.

9

The zeros:

$$\{(a,b,c) \mid abc = 0 \text{ and } (a,b,c) \neq (0,0,0)\}$$

The units:

$$\{(a,b,c) \mid |a| = |c| = 1, b \neq 0\}$$

Supplement

If I is an ideal of ring $\mathbb{Z}_N$, I must also be a subgroup of $\mathbb{Z}_N$ under the $+$ operation. Thus $I = d\mathbb{Z}_N$, where $d = 0$ or $d \mid N$.

For any $d = 0$ or $d \mid N$, we can get an subring $I = d\mathbb{Z}_N$. For any $a \in \mathbb{Z}_N$, we have $aI = (ad)\mathbb{Z}_N \subseteq d\mathbb{Z}_N$, thus subring I is an ideal of $\mathbb{Z}_N$.