Math113Hw6

Trustin Nguyen

May 13, 2023

Homework 6

Exercise 1: Let $\omega = \frac{1}{2}(-1+\sqrt{-3}) \in \mathbb{C}$. Recall that we wrote $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ and similarly $\mathbb{Q}[\omega] = \{a + b\omega : a, b \in \mathbb{Q}\}$. Show that $\mathbb{Z}[\omega]$ is a subring of $\mathbb{C}$ while $\mathbb{Q}[\omega]$ is subfield. What are the units in $\mathbb{Z}[\omega]$?

Proof. Clearly, $\mathbb{Z}[\omega], \mathbb{Q}[\omega]$ are nonempty as they both have 0. Suppose that

$$a + \frac{b}{2}(-1+\sqrt{-3}),\ c + \frac{d}{2}(-1+\sqrt{-3}) \in \mathbb{Z}[\omega]$$

Observe that

$$a + \frac{b}{2}(-1+\sqrt{-3}) - c - \frac{d}{2}(-1+\sqrt{-3}) = (a-c) - \frac{b-d}{2}(-1-\sqrt{-3}) \in \mathbb{Z}[\omega]$$

Now for multiplicative closure:

$$\begin{gathered}(a + \frac{b}{2}(-1+\sqrt{-3}))(c + \frac{d}{2}(-1+\sqrt{-3})) = \\ ac + \frac{bc+ad}{2}(-1+\sqrt{-3}) + \frac{bd}{4}(-2-2\sqrt{-3}) = \\ ac - bd + \frac{ad - bd + ad}{2}(-1+\sqrt{-3}) \in \mathbb{Z}[\omega]\end{gathered}$$

The same argument works for $\mathbb{Q}[\omega]$. Also, $1 \in \mathbb{Z}[\omega], \mathbb{Q}[\omega]$ given by $1 + 0\omega$, so it has the identity elements $0, 1$. Suppose that $a + \frac{b}{2}(-1+\sqrt{-3}) \in \mathbb{Z}[\omega]$. Then to find its inverse, observe that it would be

$$\begin{aligned}\frac{1}{a + \frac{b}{2}(-1+\sqrt{-3})} &= \frac{1}{a - \frac{b}{2} + \frac{b}{2}\sqrt{-3}} \\ &= \frac{a - \frac{b}{2} - \frac{b}{2}\sqrt{-3}}{\left(a - \frac{b}{2}\right)^2 - \left(\frac{b}{2}\sqrt{-3}\right)^2} \\ &= \frac{a - \frac{b}{2}\left(1+\sqrt{-3}\right)}{\left(a - \frac{b}{2}\right)^2 - \left(\frac{b}{2}\sqrt{-3}\right)^2} \\ &= \frac{a - b - \frac{b}{2}(-1+\sqrt{-3})}{\left(a - \frac{b}{2}\right)^2 - \left(\frac{b}{2}\sqrt{-3}\right)^2} \in \mathbb{Q}[\omega]\end{aligned}$$

so all elements except 0 is a unit. So $\mathbb{Q}[\omega]$ is a subfield. $\square$

Exercise 2: Let R be a non-zero ring. An element $r \in R$ is called nilpotent if $r^n = 0$ for some positive integer n.

1. What are the nilpotent elements in $\mathbb{Z}/6\mathbb{Z}$?

   Proof. The elements of $\mathbb{Z}/6\mathbb{Z}$are

   $$\{[0], [1], [2], [3], [4], [5]\}$$

   Observe that [0] is naturally nilpotent. For [2], we have

   $$\begin{aligned} [2]^2 &= 4 \\ [2]^3 &= [8] = [2] \end{aligned}$$

   so no powers of [2] will be 0. For [3]

   $$[3]^2 = [9] = [3]$$

   which means [3] is not nilpotent. For [4],

   $$[4]^2 = [16] = [4]$$

   So [4] is not nilpotent. For [5], we have

   $$\begin{aligned} [5]^2 &= [25] = [1] \\ [5]^3 &= [5] \end{aligned}$$

   so [5] is not nilpotent. [0] is the only nilpotent element of the set. □

2. Show that if r is nilpotent, the it's not a unit but $1 + r$ and $1 - 4$ are units.

   Proof. If r is nilpotent, suppost that it is a unit, for contradiction. Then there is some r^{-1} such that $r^{-1}r = 1$. But notice that

   $$\begin{aligned} r^n &= 0 \\ r^n r^{-1} &= 0 \\ r^{n-1} r^{-1} &= 0 \\ &\vdots \\ r r^{-1} &= 1 = 0 \end{aligned}$$

   contradiction. So r is not a unit. Now to show that $1 - r$ and $1 + r$ are units, let $r^n = 0$ and observe that

   $$(1 - r)(1 + r)(1 + r^2)(1 + r^4) \cdots (1 + r^{2n}) = 1 - r^{2n} = 1$$

   So $1 - r$ has an inverse which is

   $$(1 + r)(1 + r^2)(1 + r^4) \cdots (1 + r^{2n})$$

   and for $1 + r$, it is

   $$(1 - r)(1 + r^2)(1 + r^4) \cdots (1 + r^{2n})$$

   □

3. Let N be the set of nilpotent elements. Show that it is an ideal in R. Describe the nilpotent elements in the quotient R/N.

Proof. To show that N is an ideal, we show that it is a group under addition, is non-empty, and is closed under multiplication by elements from R.

(a) $0 \in R$, $0^1 = 0$, therefore, $0 \in N$ and N is non-empty.

(b) Suppose $a, b \in N$. Then all terms of

$$(a-b)^{2n}$$

must have an $a^k b^j$ such that either $k \geq n$ or $j \geq n$. So

$$(a-b)^{2n} = 0$$

and N contains additive inverses closed under addition.

(c) Suppose $r \in R$, $n \in N$ with $n^k = 0$. Then we show that $rn \in N$.

$$(rn)^k = r^k n^k = 0$$

since rings in this class are assumed commutative. So $rn \in N$.

therefore, N is an ideal. Since we quotient out all nilpotent elements for R/N, the nilpotent elements in the quotient is the 0 elements or $0 + N$. $\square$

Exercise 3: Show that if I and J are ideals in R, then so is $I \cap J$ and $R(I \cap J)$ is isomorphic to a subring $R/I \times R/J$. Moreover, if there are $x \in I$ and $y \in J$ with $x + y = 1$, then $R/(I \cap J) \cong R/I \times R/J$.

Proof. (Part I) Consider the homomorphism $\varphi : R \to R/I \times R/J$

$$\varphi(r) = (r + I, r + J)$$

Observe that the kernel is $I \cap J$, since if

$$\varphi(r) = (r + I, r + J) = (I, J)$$

then $r \in I \cap J$ and vice versa. So since the kernel is an ideal, $I \cap J$ is an ideal also. So by isomorphism theorem, $R/(I \cap J) \cong R/I \times R/J$.

(Part II) If there is an $x \in I, y \in J$ such that $x + y = 1$, we will prove that the mapping given by φ is surjective. Suppose that $(a + I, b + j) \in R/I \times R/J$. The consider

$$\begin{aligned}
\varphi(ay + bx) &= (ay + I, bx + J) \\
&= ((a + I)(y + I), (b + J)(x + J)) \\
&= ((a + I)(R), (b + J)(R)) \\
&= ((a + I)(1 + I), (j + J)(1 + J)) \\
&= (a + I, b + J)
\end{aligned}$$

so the map is urjective. By the isomorphism theorem, the domain is isomorphic to the image of the maps, so it is isomorphic to the whole codomain. We are done. $\square$

Exercise 4: Let R be a ring. We say that $r \in R$ is idempotent if $r^2 = r$.

1. Describe the idempotents in $\mathbb{Z}/6\mathbb{Z}$.

Proof. The elements of $\mathbb{Z}/6\mathbb{Z}$ are

$$\{[0], [1], [2], [3], [4], [5]\}$$

We check each one.

$$\begin{aligned}
[0]^2 &= [0] \\
[1]^2 &= [1] \\
[2]^2 &= [4] \neq [2] \\
[3]^2 &= [9] \equiv [3] \\
[4]^2 &= [16] \equiv [4] \\
[5]^2 &= [25] \equiv [1] \neq [5]
\end{aligned}$$

So the idempotent elements of $\mathbb{Z}/6\mathbb{Z}$ are

$$\{[0], [1], [3], [4]\}$$

□

2. Show that if r is idempotent, then so is $r' = 1 - r$ and $rr' = 0$. Furthermore, prove that the ideal (r) is naturally a ring and that $R \cong (r) \times (r')$ as rings.

Proof. (Part I) If r is idempotent, then we have

$$rr' = (1 - r)r = r - r^2 = 0$$

since $r = r^2$. So rr' is idempotent also. For the second part, Observe that if we take any element of (r), λr^k, r is the identity of that ideal:

$$\lambda r^k \cdot r = \lambda r^{k+1} = \lambda r^k$$

so (r) is a ring.
(Part II) Consider the mapping $\varphi : R \to (r) \times (r')$

$$\varphi(r) = (r + (r), r + (r'))$$

Let $(a + (r), b + (r')) \in (r) \times (r')$ be arbitrary. We will show that φ is surjective. Then consider $ar' + br$. We have

$$\begin{aligned}
\varphi(ar' + br) &= (ar' + br + (r), ar' + br + (r')) \\
&= (ar' + (r), br + (r')) \\
&= (a - ar + (r), b(r' + 1) + (r')) \\
&= (a - ar + (r), br' + b + (r')) \\
&= (a + (r), b + (r'))
\end{aligned}$$

as desired. □