ABSTRACT ALGEBRA — FIRST MIDTERM EXAM

ARDEN RASMUSSEN

OCTOBER 8, 2019

Problem 1

Let $\omega \in \mathbb{C}$ be a solution of the equation

$$\omega^2 + \omega + 1 = 0.$$

Consider the set $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$. Show that the set $\mathbb{Z}[\omega]$ is closed under the ordinary addition and under the ordinary multiplication. Conclude that $\mathbb{Z}[\omega]$ is a ring which is a subring of the field of complex numbers.

Proof. Consider the set $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$. Let $a_1 + b_1\omega, a_2 + b_2\omega \in \mathbb{Z}[\omega]$, then we compute

$$(a_1 + b_1\omega) + (a_2 + b_2\omega) = (a_1 + a_2) + (b_1 + b_2)\omega.$$

It is clear that $a_1 + a_2 \in \mathbb{Z}$ and $b_1 + b_2 \in \mathbb{Z}$, so we can conclude that $\mathbb{Z}[\omega]$ is closed under ordinary addition. Now we compute

$$(a_1 + b_1\omega) \cdot (a_2 + b_2\omega) = a_1a_2 + a_1b_2\omega + a_2b_1\omega + b_1b_2\omega^2.$$

Since $\omega^2 + \omega + 1 = 0$, then we know that $\omega^2 = -\omega - 1$, so we can rewrite this to be

$$\begin{aligned} &a_1a_2 + a_1b_2\omega + a_2b_1\omega - b_1b_2(\omega + 1) \\ &\qquad = (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1 - b_1b_2)\,\omega. \end{aligned}$$

Again, we can see that $a_1a_2 - b_1b_2 \in \mathbb{Z}$ and $a_1b_2 + a_2b_1 - b_1b_2 \in \mathbb{Z}$, thus we conclude that $\mathbb{Z}[\omega]$ is closed under ordinary addition.

Since $\mathbb{Z}[\omega] \subset \mathbb{C}$ and it is closed under addition and multiplication, then we are able to conclude that $(\mathbb{Z}[\omega], +, \cdot)$ is a ring, and is a subring of $\mathbb{C}$. $\square$

Problem 2

Consider the set $\mathbb{Z}[2i] = \{a + 2bi | a, b \in \mathbb{Z}\}$. Standard number addition and multiplication turn $\mathbb{Z}[2i]$ into a commutative integral domain with identity.

(a). Prove that 2 is irreducible in this ring.

Proof. Assmume that 2 is reducible, that is that there exists some $a, b \in \mathbb{Z}[2i]$ such that $2 = ab$, where a, b are non-unit and non-zero. Then we compute

$$\begin{aligned} 2 &= ab \\ N(2) &= N(a)N(b) \\ 4 &= N(a)N(b). \end{aligned}$$

Since a, b are not unit, then $N(a), N(b) \neq 1$, so that means

$$N(a) = N(b) = 2.$$

If $a = \alpha + 2\beta$, with $\alpha, \beta \in \mathbb{Z}$, then $N(a) = \alpha^2 + 4\beta^2 = 2$. There can be no α, β that satisfy this equation. Thus we conclude that a must be unit. However, this is a contradiction of our assumption, thus 2 must be irreducible in $\mathbb{Z}[2i]$. $\square$

(b). Prove that $2i$ is irreducible in this ring.

Proof. Assmume that $2i$ is reducible, that is that there exists some $a, b \in \mathbb{Z}[2i]$ such that $2i = ab$, where a, b are non-unit and non-zero. Then we compute

$$\begin{aligned} 2i &= ab \\ N(2i) &= N(a)N(b) \\ 4 &= N(a)N(b). \end{aligned}$$

Since a, b are not unit, then $N(a), N(b) \neq 1$, so that means

$$N(a) = N(b) = 2.$$

If $a = \alpha + 2\beta$, with $\alpha, \beta \in \mathbb{Z}$, then $N(a) = \alpha^2 + 4\beta^2 = 2$. There can be no α, β that satisfy this equation. Thus we conclude that a must be unit. However, this is a contradiction of our assumption, thus $2i$ must be irreducible in $\mathbb{Z}[2i]$. $\square$

(c). Is it true that $2|2i$ in this ring?

Proof. Assume $2|2i$, this implies that there exists some $q \in \mathbb{Z}[2i]$ such that $2i = 2 \cdot q$. However, the only q that would satisfy this statement would be i, and $i \notin \mathbb{Z}[2i]$. Thus $2 \nmid 2i$ $\square$

(d). Are 2 and $2i$ associates in this ring?

Proof. Units in this ring are ± 1. Thus 2 and $2i$ are not associates, as they are not off by a unit of one another. $\square$

(e). Can you provide two factorizations of 4 into irreducible?

$$\begin{aligned} 4 &= 2 \cdot 2 \\ 4 &= 2i \cdot (-2i) \end{aligned}$$

(f). Is 2 prime in this ring? Justify your claim.
No 2 is not prime. Consider $2|4 \to 2|2i \cdot -2i$, but $2 \nmid 2i$ and $2 \nmid -2i$.

(g). Is $2i$ prime in this ring?
No $2i$ is not prime. Consider $2i|4 \to 2|2 \cdot 2$, but $2i \nmid 2$.

(g). Is $\mathbb{Z}[2i]$ a Euclidean domain? Is it a PID?
It is neither. It is not a Euclidean domain, because primes $\neq$ irreducibles, and it is not a PID, with a counter example of $(2, 2i)$.

Problem 3

Let I be an ideal of a commutative ring R with identity. Define the following set:

$$\operatorname{rad}(I) = \{r \in R | r^n \in I \text{ for some } n \in \mathbb{N}\}.$$

Note: $\mathbb{N}$ is the set of positive integers only. In particular, $0 \notin \mathbb{N}$.

(a). Suppose temporarily that $R = \mathbb{Z}$. Find $\operatorname{rad}(I)$ for the following choices of I:

(i). $I = (9)$

$$\begin{aligned}\operatorname{rad}(I) &= \{\pm 3, \pm 6, \pm 9, \ldots\} \\ &= \{k \cdot 3 | k \in \mathbb{Z}\} \\ &= (3)\end{aligned}$$

(i). $I = (43)$

$$\begin{aligned}\operatorname{rad}(I) &= \{\pm 43, \pm 86, \pm 129, \ldots\} \\ &= \{k \cdot 43 | k \in \mathbb{Z}\} \\ &= (43)\end{aligned}$$

(iii). $I = (72)$

$$\begin{aligned}\operatorname{rad}(I) &= \{\pm 6, \pm 12, \pm 18, \ldots\} \\ &= \{k \cdot 6 | k \in \mathbb{Z}\} \\ &= (6) \\ &= (2 \cdot 3) \\ &= (2) \cap (3)\end{aligned}$$

(b). Going back to the general situation, show $\operatorname{rad}(I)$ is an ideal. Hint: Look at your very first homework assignment.

Proof. To prove that $\operatorname{rad}(I)$ is an ideal, we show that $\operatorname{rad}(I)$ is closed under addition and multiplication, by some other element in R. Consider $a, b \in \operatorname{rad}(I)$, thus there exists some $n, m \in \mathbb{N}$ such that

$$a^m, b^n \in I.$$

Consider the expression

$$\sum_{k=0}^{k=m+n} \binom{m+n}{k} a^k b^{m+n-k}.$$

We consider the general element of this sumation, for some k. If $k < m$ then we can express this as

$$\begin{aligned}&\binom{m+n}{k} a^k b^{n+\delta} \qquad \delta = m - k > 0 \\ &= \left(\binom{m+n}{k} a^k b^\delta\right) b^n \\ &= rb^n.\end{aligned}$$

Then by the definition of an ideal, and $b^n \in I$, then $rb^n \in I$. Thus any element with $k < m$ is an element of I. If $k \geq m$ then we can express this as

$$\begin{aligned} &\binom{m+n}{k} a^{m+\delta} b^{\gamma} \qquad \delta = k - m > 0, \gamma = m + n - k > 0 \\ &= \left(\binom{m+n}{k} a^{\delta} b^{\gamma} \right) a^m \\ &= r a^m. \end{aligned}$$

Thus again by the definition of an ideal, and $a^m \in I$, then this $ra^m \in I$. Thus any element with $k \geq m$ is an element of I.

So we conclude that all elements of this sum is an element of the ideal I, and since ideals are closed under addition, then

$$\sum_{k=0}^{k=m+n} \binom{m+n}{k} a^k b^{m+n-k} \in I.$$

By the Binomial theorem, we know that

$$\sum_{k=0}^{k=m+n} \binom{m+n}{k} a^k b^{m+n-k} = (a+b)^{m+n} \in I.$$

and thus we can conclude that $a + b \in \operatorname{rad}(I)$.

Now we show that $\operatorname{rad}(I)$ is closed under multiplication. Consider $a \in \operatorname{rad}(I)$, and $r \in R$. We know that there exists some $n \in \mathbb{N}$ such that $a^n \in I$. Then there is some $b \in R$ such that $b = r^n$, and by definiton of an ideal, $ba^n \in I$ which implies that $r^n a^n \in I$. So we conclude that $(ra)^n \in I$, and thus $ra \in \operatorname{rad}(I)$.

Since $\operatorname{rad}(I)$ is closed under addition and multiplication, we can conclude that it is indeed a ring. $\square$