Rutgers University: Algebra Written Qualifying Exam

August 2015: Problem 5 Solution

Exercise. Let $\zeta = \frac{1+\sqrt{-3}}{2}$. and R denote the subring $\mathbb{Z}[\zeta]$ of $\mathbb{C}$.

(a) Show that $R = \mathbb{Z} + \zeta \cdot \mathbb{Z}$

Solution.

Obviously $\mathbb{Z} + \zeta \cdot \mathbb{Z} \subseteq \mathbb{Z}[\zeta] = R$.
Now, suppose $P \in \mathbb{Z}[\zeta]$.
Then $P = a_n\zeta^n + \cdots + a_1\zeta + a_0$ for some $n \in \mathbb{Z}_{\geq 0}$ where $a_k \in \mathbb{Z}$ $\leftarrow$ so, check powers of ζ

<u>**Note:**</u>

$$\begin{aligned}
\zeta &= \frac{1+\sqrt{-3}}{2} \\
\zeta^2 &= \left(\frac{1+\sqrt{-3}}{2}\right)^2 \\
&= \frac{1-3+2\sqrt{-3}}{4} \\
&= \frac{-1+\sqrt{-3}}{2} \\
&= -1 + \frac{1+\sqrt{-3}}{2} \in \mathbb{Z} + \zeta \cdot \mathbb{Z} \\
\zeta^3 &= \left(\frac{1+\sqrt{-3}}{2}\right)\left(\frac{-1+\sqrt{-3}}{2}\right) \\
&= \frac{-1-3}{2} \\
&= -2 \in \mathbb{Z}
\end{aligned}$$

$$\begin{aligned}
\text{So, for } k &\equiv 0 \mod 3, & a_k\zeta^k &\in \mathbb{Z} \\
\text{For } k &\equiv 1 \mod 3, & a_k\zeta^k &\in \zeta \cdot \mathbb{Z} \\
\text{For } k &\equiv 2 \mod 3, & a_k\zeta^k &\in \mathbb{Z} + \zeta \cdot \mathbb{Z}
\end{aligned}$$

Thus, $p \in \mathbb{Z} + \zeta \cdot \mathbb{Z}$
$\implies \mathbb{Z}[\zeta] \subseteq \mathbb{Z} + \zeta \cdot \mathbb{Z}$.
So, $R = \mathbb{Z} + \zeta \cdot \mathbb{Z}$

(b) For $a \in R$, show that $|a|^2 = a\overline{a}$ is an integer, where $\overline{a}$ is the complex conjugate.

Solution.

$$a \in R \implies \qquad a = b + c\left(\frac{1+\sqrt{-3}}{2}\right) = \frac{2b+c+c\sqrt{-3}}{2} \qquad b, c, \in Z$$

$$\begin{aligned}
|a|^2 = a\overline{a} &= \left(\frac{2b+c+c\sqrt{-3}}{2}\right)\left(\frac{2b+c-c\sqrt{-3}}{2}\right) \\
&= \frac{(2b+c)^2+3c^2}{4} = \frac{4b^2+4bc+4c^2}{4} \\
&= b^2+bc+c^2 \in \mathbb{Z}, \text{ since } b, c \in \mathbb{Z}
\end{aligned}$$

(c) For $a \in \mathbb{C}$ show that there are $q \in R$, and $r \in \mathbb{C}$, with

$$a = q + r \text{ and } |r| < 1$$

Solution.

Since $a \in \mathbb{C}$, $a = a_0 + a_1 i$ for some $a_0, a_1 \in \mathbb{R}$.
Let $q \in R$, so $q = q_0 + q_1\left(\frac{1+i\sqrt{3}}{2}\right)$

Want q as close as possible to a. $\implies$ $\frac{q_1\sqrt{3}}{2}$ close to a_1 and $q_0 + \frac{q_1}{2}$ close to a_0

$$\text{where } q_1 \text{ is s.t.} \quad \left|\frac{q_1\sqrt{3}}{2} - a_1\right| < \left|\frac{(q_1-1)\sqrt{3}}{2} - a_1\right| \quad \text{and} \quad \left|\frac{q_1\sqrt{3}}{2} - a_1\right| < \left|\frac{(q_1+1)\sqrt{3}}{2} - a_1\right|$$

$$\implies \quad \left|\frac{q_1\sqrt{3}}{2} - a_1\right| < \frac{\sqrt{3}}{2}$$

$$\text{and } q_0 \text{ is s.t.} \quad \left|q_0 + \frac{q_1}{2} - a_0\right| < \left|q_0 \pm \frac{q_1}{2} - a_0\right|$$

$$\implies \quad \left|q_0 + \frac{q_1}{2} - a_0\right| < \frac{1}{2}$$

$$a = q + \underbrace{\left(a_0 - q_0 - \frac{q_1}{2}\right) + \left(a_1 - \frac{a_1}{2}\sqrt{3}\right)i}_{=:r}, \qquad r = \left(a_0 - q_0 - \frac{q_1}{2}\right) + \left(a_1 - \frac{q_1}{2}\sqrt{3}\right)i$$

$$|r| = \sqrt{\left(a_0 - q_0 - \frac{q_1}{2}\right)^2 + \left(a_1 - \frac{q_1}{2}\sqrt{3}\right)^2}$$

$$< \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2} = \sqrt{\frac{1}{4} + \frac{3}{4}} = 1$$

So, for $a \in \mathbb{C}$, $\exists q \in R$ and $r \in \mathbb{C}$ s.t.

$$a = q + r \text{ and } |r| < 1$$

(d) (Division algorithm) Show that for $a, b \in R$ with $b \neq 0$. there are $q, r \in R$ with

$$\underbrace{a = bq + r \text{ and } |r| < |b|}_{\text{This is similar to part (c). How can we use part (c)?}}$$

Solution.

Let $a, b \in R$. Then $\frac{a}{b} \in \mathbb{C}$.
By part (c), $\exists q \in R$ and $r_0 \in \mathbb{C}$ with $|r_0| < 1$ s.t.

$$\begin{aligned} \frac{a}{b} &= q + r_0 \\ \implies a &= bq + br_0 \\ &= bq + r \qquad \text{where } r := br_0 \\ |r| &= |b| \cdot |r_0| < |b| \end{aligned}$$

Moreover, since $r = a - bq$ and $a, b, q \in R$, it follows that $r \in R$.
Thus, the division algorithm holds.

(e) Show that R is a principal ideal domain.

Solution.

The division algorithm holds in R

$\implies$ R is a Euclidean domain

$\implies$ R is a principal ideal domain

More Details:

A **principal ideal domain** is an integral domain (i.e. commutative ring with multiplicative identity and no zero divisors) in which every proper ideal can be generated by a single element.

It is obviously an integral domain, so lets just prove it is a principal ideal.

$I = (0)$ is obviously a principal ideal

Suppose $I \neq (0)$ and let $a \in I$ be such that $|a| \leq |x|$ for all $x \in I$ $x \neq 0$ (assume minimality)

Then $(a) \subseteq I$

Let $b \in I$

By the division algorithm $\exists q, r \in R$ s.t.

$$b = aq + r \qquad \text{where } |r| < |a|$$

$$\implies \underbrace{b}_{\in I} - \underbrace{aq}_{\in I} = r \in I$$

$$|r| < |a| \text{ but } |a| \text{ has minimal value}$$

$$\implies |r| = 0$$

$$\implies b - aq = 0$$

$$\implies b = aq$$

$$\implies b \in (a)$$

$$\implies I \subseteq (a)$$

Thus $I = (a)$ and R is a principal ideal domain