Chapter 6, Question 13

---

13. Let m be a squarefree integer $\equiv 3 \pmod 4$. Prove that

$$< 2, 1+\sqrt{m} >= 2\mathbb{Z} + (1+\sqrt{m})\mathbb{Z}.$$

Solution. Let $\alpha \in 2\mathbb{Z} + (1+\sqrt{m})\mathbb{Z}$. Then there exist $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\alpha = 2x + (1+\sqrt{m})y$. Hence $\alpha \in < 2, 1+\sqrt{m} >$. Thus

$$2\mathbb{Z} + (1+\sqrt{m})\mathbb{Z} \subseteq < 2, 1+\sqrt{m} > .$$

Now let $\beta \in < 2, 1+\sqrt{m} >$. Then there exist $\theta \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ and $\phi \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ such that $\beta = 2\theta + (1+\sqrt{m})\phi$. As $\theta \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ there exist $r \in \mathbb{Z}$ and $s \in \mathbb{Z}$ such that $\theta = r + s\sqrt{m}$. Similarly there exist $t \in \mathbb{Z}$ and $u \in \mathbb{Z}$ such that $\phi = t + u\sqrt{m}$. Then

$$\begin{aligned}
\beta &= 2(r + s\sqrt{m}) + (1+\sqrt{m})(t + u\sqrt{m}) \\
&= (2r + t + mu) + (2s + t + u)\sqrt{m} \\
&= (2r - 2s + (m-1)u) + (2s + t + u)(1+\sqrt{m}) \\
&= 2(r - s + (\frac{m-1}{2})u) + (2s + t + u)(1+\sqrt{m}) \\
&\in 2\mathbb{Z} + (1+\sqrt{m})\mathbb{Z}.
\end{aligned}$$

Hence

$$< 1, 1+\sqrt{m} > \subseteq 2\mathbb{Z} + (1+\sqrt{m})\mathbb{Z}.$$

The two inclusions show that

$$< 2, 1+\sqrt{m} >= 2\mathbb{Z} + (1+\sqrt{m})\mathbb{Z}. \qquad \blacksquare$$

February 25, 2004