CHAPTER 1, QUESTION 21

21. Prove that $< 2, 1+\sqrt{-5} >$, $< 3, 1+\sqrt{-5} >$ and $< 3, 1-\sqrt{-5} >$ are prime ideals of $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Determine $< 2, 1+\sqrt{-5} > \cap \mathbb{Z}$, $< 3, 1+\sqrt{-5} > \cap \mathbb{Z}$ and $< 3, 1-\sqrt{-5} > \cap \mathbb{Z}$.

Solution. Let $\alpha = a + b\sqrt{-5} \in \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. We show first that

$$\alpha \in < 2, 1+\sqrt{-5} > \Longleftrightarrow a \equiv b \pmod 2. \tag{1}$$

If $a \equiv b \pmod 2$ then there exists $c \in \mathbb{Z}$ such that $a = b + 2c$. Then

$$\alpha = a + b\sqrt{-5} = b + 2c + b\sqrt{-5} = c2 + b(1+\sqrt{-5}) \in < 2, 1+\sqrt{-5} > .$$

Conversely suppose that $\alpha \in < 2, 1+\sqrt{-5} >$. Then there exist $x, y, z, w \in \mathbb{Z}$ such that

$$a + b\sqrt{-5} = (x + y\sqrt{-5})2 + (z + w\sqrt{-5})(1+\sqrt{-5}).$$

Hence

$$\begin{aligned} a &= 2x + z - 5w, \\ b &= 2y + z + w. \end{aligned}$$

Thus

$$a \equiv z - 5w \equiv z + w \equiv b \pmod 2.$$

We now show that $< 2, 1+\sqrt{-5} >$ is a prime ideal of $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Let $\alpha = a + b\sqrt{-5} \in \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ and $\beta = c + d\sqrt{-5} \in \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ be such that

$$\alpha\beta \in < 2, 1+\sqrt{-5} > .$$

Now

$$\alpha\beta = (ac - 5bd) + (ad + bc)\sqrt{-5}$$

so that by (1)

$$ac - 5bd \equiv ad + bc \pmod 2.$$

Thus

$$\begin{aligned}(a-b)(c-d) &= ac-bc-ad+bd\\ &\equiv (5bd+ad+bc)-bc-ad+bd \equiv 0 \pmod 2\end{aligned}$$

so that either $a-b \equiv 0 \pmod 2$ or $c-d \equiv 0 \pmod 2$. In the former case $\alpha = a+b\sqrt{-5} \in <2, 1+\sqrt{-5}>$ and in the latter case $\beta = c+d\sqrt{-5} \in <2, 1+\sqrt{-5}>$. This proves that $<2, 1+\sqrt{-5}>$ is a prime ideal.

Next we show that

$$<2, 1+\sqrt{-5}> \cap \mathbb{Z} = <2>.$$

We empasize that $<2, 1+\sqrt{-5}>$ is an ideal of $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ and $<2>$ is a principal ideal of $\mathbb{Z}$.

Let $\alpha \in <2, 1+\sqrt{-5}> \cap \mathbb{Z}$. Then $\alpha \in \mathbb{Z}$ and $\alpha \in <2, 1+\sqrt{-5}>$. By (1) we have $\alpha \equiv 0 \pmod 2$. Hence $\alpha \in <2>$. This proves that

$$<2, 1+\sqrt{-5}> \cap \mathbb{Z} \subseteq <2>.$$

Now let $\alpha \in <2>$. Then α is an even integer. Hence $\alpha \in \mathbb{Z}$ and by (1) we deduce that $\alpha \in <2, 1+\sqrt{-5}>$. Thus

$$\alpha \in <2, 1+\sqrt{-5}> \cap \mathbb{Z}.$$

This proves that

$$<2> \subseteq <2, 1+\sqrt{-5}> \cap \mathbb{Z}.$$

We have now shown that

$$<2, 1+\sqrt{-5}> \cap \mathbb{Z} = <2>.$$

We now turn to the ideals $<3, 1+\sqrt{-5}>$ and $<3, 1-\sqrt{-5}>$. By an argument similar to that used to prove (1) we can show that

$$a+b\sqrt{-5} \in <3, 1+\sqrt{-5}> \Leftrightarrow a \equiv b \pmod 3, \tag{2}$$
$$a+b\sqrt{-5} \in <3, 1-\sqrt{-5}> \Leftrightarrow a \equiv -b \pmod 3. \tag{3}$$

Using (2) and (3) it is easy to show as above that $<3, 1+\sqrt{-5}>$ and $<3, 1-\sqrt{-5}>$ are prime ideals of $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$.

Finally we show that

$$< 3, 1 + \sqrt{-5} > \cap \, \mathbb{Z} =< 3 > .$$

We have

$$\begin{aligned}
&< 3, 1 + \sqrt{-5} > \cap \, \mathbb{Z} \\
&= \left\{3(x + y\sqrt{-5}) + (1 + \sqrt{-5})(u + v\sqrt{-5}) \mid x, y, u, v \in \mathbb{Z},\ 3y + u + v = 0\right\} \\
&= \left\{3(x + y\sqrt{-5}) + (1 + \sqrt{-5})(-v - 3y + v\sqrt{-5}) \mid x, y, v \in \mathbb{Z}\right\} \\
&= \{3x - 3y - 6v \mid x, y, v \in \mathbb{Z}\} \\
&= \{3z \mid z \in \mathbb{Z}\} \\
&=< 3 > .
\end{aligned}$$

Similarly we can show that $< 3, 1 - \sqrt{-5} > \cap \, \mathbb{Z} =< 3 >$. ∎

June 19, 2004