CHAPTER 5, QUESTION 19

19. Let m be a squarefree integer $\equiv 1 \pmod 4$. Let $A = \mathbb{Z} + \mathbb{Z}\sqrt{m}$ and $B = \mathbb{Q}(\sqrt{m})$. Prove that

$$A^B = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right).$$

Solution. Let $\alpha \in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$. Then $\alpha = r + s\left(\frac{1+\sqrt{m}}{2}\right)$ for some $r, s \in \mathbb{Z}$. Clearly $\alpha \in B$. As α is a root of the monic polynomial

$$x^2 - (2r+s)x + \left(r^2 + rs + (\frac{1-m}{4}s^2)\right) \in A[x],$$

α is integral over A and thus belongs to A^B. Hence $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right) \subseteq A^B$.

We now show that $A^B \subseteq \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$. Let $\alpha \in A^B$. Clearly $\alpha \in B$ so that $\alpha = a + b\sqrt{m}$ for some $a, b \in \mathbb{Q}$. Thus α is a root of the monic polynomial

$$x^2 - 2ax + (a^2 - mb^2) \in \mathbb{Q}[x].$$

The discriminant of this polynomial is

$$(2a)^2 - 4(a^2 - mb^2) = 4mb^2.$$

As m is squarefree, the polynomial is reducible in $\mathbb{Q}[x]$ if $b = 0$ and irreducible in $\mathbb{Q}[x]$ if $b \neq 0$. Hence

$$\mathrm{irr}_{\mathbb{Q}}(\alpha) = \begin{cases} x - a & , \text{ if } b = 0, \\ x^2 - 2ax + (a^2 - mb^2) & , \text{ if } b \neq 0. \end{cases}$$

As $\alpha \in A^B$, α is integral over A and thus is a root of a monic polynomial

$$x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n \in A[x].$$

For $j = 1, 2, \ldots, n$ we have $\alpha_j \in A$ so that $\alpha_j = a_j + b_j\sqrt{m}$ for some $a_j, b_j \in \mathbb{Z}$. Now

$$\alpha^n + (a_1 + b_1\sqrt{m})\alpha^{n-1} + \cdots + (a_n + b_n\sqrt{m}) = 0$$

so that

$$(\alpha^n + a_1\alpha^{n-1} + \cdots + a_n) + \sqrt{m}(b_1\alpha^{n-1} + \cdots + b_n) = 0$$

and thus

$$(\alpha^n + a_1\alpha^{n-1} + \cdots + a_n)^2 - m(b_1\alpha^{n-1} + \cdots + b_n)^2 = 0.$$

Thus α is a root of the monic polynomial

$$(x^n + a_1x^{n-1} + \cdots + a_n)^2 - m(b_1x^{n-1} + \cdots + b_n)^2 \in \mathbb{Z}[x].$$

Hence α is an algebraic integer and so, by Theorem 5.1.2, $\mathrm{irr}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$, that is

$$\begin{cases} a \in \mathbb{Z} & , \text{ if } b = 0, \\ 2a,\ a^2 - mb^2 & , \text{ if } b \neq 0. \end{cases}$$

In the former case $\alpha = a + b\sqrt{m} = a = a + 0\left(\frac{1+\sqrt{m}}{2}\right) \in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$. In the latter case we have $a = r/2$ for some $r \in \mathbb{Z}$. If $r \in 2\mathbb{Z}$ then $a \in \mathbb{Z}$ and $mb^2 \in \mathbb{Z}$. As $b \neq 0$ and m is square free, we deduce that $b \in \mathbb{Z}$. Thus

$$\alpha = a + b\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m} \subset \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right).$$

If $r \in 2\mathbb{Z} + 1$ then $2a \in 2\mathbb{Z} + 1$ so $m(2b)^2 = (2a)^2 - 4(a^2 - mb^2) \in \mathbb{Z}$. ∎

June 23, 2004