MATH 5326-Algebraic Number Theory Final Exam

Orin Gotchey

December 11, 2022

Problem I

Let $m \equiv_4 1$ be a squarefree integer. Then the set of all elements $K = \mathbb{Q}(\sqrt{m})$ which are integral over $\mathbb{Z}[\sqrt{m}]$ is equal to $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$

Proof. First, let $\alpha = \frac{a+b\sqrt{m}}{2}$ for some integers $a, b \in \mathbb{Z}$ $a \equiv_2 b$. We demonstrate that α is algebraic over $\mathbb{Z}$:

$$\alpha^2 = \frac{a^2 + 2ab\sqrt{m} + b^2m}{4}$$
$$\alpha^2 - a\alpha = \frac{a^2 + 2ab\sqrt{m} + b^2m - 2ab\sqrt{m} - 2a^2}{4}$$
$$= \frac{-a^2 + b^2m}{4}$$

Now,

$$a \equiv_2 b \implies a^2 \equiv_4 b^2 \equiv_4 b^2m \implies \frac{-a^2 + b^2m}{4} \in \mathbb{Z}$$

Thus, α is a root of the monic integer polynomial

$$f(x) = x^2 - ax + \frac{a^2 - b^2m}{4} \in \mathbb{Z}[x]$$

Conversely, we assume that $\alpha = \frac{a}{b} + \frac{c}{d}\sqrt{m}$ is algebraic over $\mathbb{Z}$, with $b \neq 0 \neq d,\ \gcd(a, b) = 1,\ \gcd(c, d) = 1$. Thus, α is the root of some monic integer polynomial

$$f(x) = x^2 + \gamma_1 x + \gamma_0$$

for some $\gamma_1,\ \gamma_0 \in \mathbb{Z}$. Substituting α for x,

$$f(\alpha) = \frac{a^2}{b^2} + \frac{2ac}{bd}\sqrt{m} + m\frac{c^2}{d^2} + \gamma_1(\frac{a}{b} + \frac{c}{d}\sqrt{m}) + \gamma_0 = 0 \tag{1}$$

Now, 1 and $\sqrt{m}$ are linearly independent over $\mathbb{Z}$, so we separate:

$$\frac{2ac}{bd}\sqrt{m} + \gamma_1\frac{c}{d}\sqrt{m} = 0 \tag{2}$$
$$\frac{2ac}{bd} + \frac{\gamma_1 bc}{bd} = 0 \tag{3}$$
$$2ac + \gamma_1 bc = c(2a + \gamma_1 b) = 0 \tag{4}$$
$$\text{(and...)}\ \frac{a^2}{b^2} + m\frac{c^2}{d^2} + \gamma_1\frac{a}{b} + \gamma_0 = 0 \tag{5}$$

In view of (4), either $c = 0$ or $\gamma_1 = \frac{-2a}{b}$. In the former case, we get $\alpha \in \mathbb{Q}$ the root of some monic integer polynomial, so $\alpha \in \mathbb{Z} \subseteq \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ (in which case we'd be done). On the other hand, if $a = 0$, then $\frac{mc^2}{d^2} \in \mathbb{Z}$. However, m is squarefree, so $d \mid c$ and $\alpha \in \mathbb{Z}[\sqrt{m}]$, and we're done. Thus, we may assume that $c \neq 0 \neq a$ and $\gamma_1 = \frac{-2a}{b}$. This implies that $b|2a$.

Case 1 In the case that b is an odd integer, then $b|a$ since 2 is prime. b and a were chosen such that $\gcd(b, a) = 1$, thus $b = \pm 1$. Rewriting (5),

$$\frac{-a^2}{b^2} + m\frac{c^2}{d^2} \in \mathbb{Z}$$

$$-a^2 + m\frac{c^2}{d^2} \in \mathbb{Z}$$

$$\therefore (d^2)|(mc^2)$$

m is still squarefree, so $d|c$, and thus $\alpha \in \mathbb{Z}$, completing this case.

Case 2 If b is even:

$$(\exists x \in \mathbb{Z} \ : 2x = b) \therefore 2x|2a \therefore x|a \therefore x| \gcd(a, b)$$

Thus, x is a unit, so we can assume WLOG that $b = 2$.

So, a is an odd integer and $b = 2$.

$$\begin{aligned} \frac{a}{4}^2 + m\frac{c^2}{d^2} + \frac{-2a^2}{4} + \gamma_0 &= 0 \\ \frac{-a^2}{4} + m\frac{c^2}{d^2} &\in \mathbb{Z} \\ \frac{4mc^2}{d^2} &\in \mathbb{Z} \\ \frac{m(2c)^2}{d^2} &\in \mathbb{Z} \\ d^2 &| \, m(2c)^2 \\ \text{m squarefree} \therefore d^2 &| \, (2c)^2 \\ d &| \, 2c \end{aligned}$$

Arguing in a way symmetric to that above: if d were odd, then $d|c$. Since $\gcd(d, c) = 1$, $d = \pm 1$ In that case,

$$\frac{-a^2}{4} + mc^2 \in \mathbb{Z}$$

$$\frac{-a^2}{4} \in \mathbb{Z}$$

, which implies that $\alpha \in \mathbb{Z} \subseteq \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$, and so we may assume that d is even. An argument perfectly symmetric to that above shows that therefore $d = 2$, and with $\gcd(c, d) = 1$, we see that c is odd.

$$\alpha = \frac{a + c\sqrt{m}}{2} = \frac{a - c}{2} + c\frac{1 + \sqrt{m}}{2}$$

Recall that $a \equiv_2 c$, so $\alpha \in \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$, completing the proof. □

Problem II

Let $K = \mathbb{Q}(\theta)$ where θ is a root of $f(x) := x^6 + 2x^2 + 2 = 0$. Let $\alpha := \theta^4 + \theta^2 = \theta^2(1 + \theta^2)$. The minimal polynomial of α is $g(x) =$

Proof.

$$\begin{aligned}
\alpha &= \theta^4 + \theta^2 \\
\alpha^2 &= \theta^8 + 2\theta^6 + \theta^4 \\
&= (\theta^2 + 2)\theta^6 + \theta^4 \\
&= (\theta^2 + 2)(-2\theta^2 - 2) + \theta^4 \\
&= -2\theta^4 - 6\theta^2 - 4 + \theta^4 \\
&= -\theta^4 - 6\theta^2 - 4 \\
\alpha^3 &= (-\theta^4 - 6\theta^2 - 4)(\theta^4 + \theta^2) \\
&= -\theta^8 - \theta^6 - 6\theta^6 - 6\theta^4 - 4\theta^4 - 4\theta^2 \\
&= -\theta^8 - 7\theta^6 - 10\theta^4 - 4\theta^2 \\
&= -\theta^6(\theta^2 + 7) - 10\theta^4 - 4\theta^2 \\
&= (2\theta^2 + 2)(\theta^2 + 7) - 10\theta^4 - 4\theta^2 \\
&= (2\theta^4 + 16\theta^2 + 14) - 10\theta^4 - 4\theta^2 \\
&= -8\theta^4 + 12\theta^2 + 14
\end{aligned}$$

Observe: $\alpha,\ \alpha^2,\ \alpha^3$ are $\mathbb{Z}$-linear combinations of $\{\theta^2, \theta^4, 1\}$.

Namely,

$$\begin{bmatrix} 1 & 1 & 0 \\ -1 & -6 & -4 \\ -8 & 12 & 14 \end{bmatrix} \begin{bmatrix} \theta^4 \\ \theta^2 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \alpha^2 \\ \alpha^3 \end{bmatrix}$$

We are going to perform a kind of row reduction on the coefficient matrix, keeping track of the effects on the α^i's.

$$\left[\begin{array}{ccc|c} 1 & 1 & 0 & \alpha \\ 0 & -5 & -4 & \alpha^2 + \alpha \\ 0 & 20 & 14 & \alpha^3 + 8\alpha \end{array}\right]$$

$$\left[\begin{array}{ccc|c} 1 & 1 & 0 & \alpha \\ 0 & -5 & -4 & \alpha^2 + \alpha \\ 0 & 0 & -2 & \alpha^3 + 8\alpha + 4(\alpha^2 + \alpha) \end{array}\right]$$

Thus, we see that

$$\alpha^3 + 4\alpha^2 + 12\alpha = -2$$

, i.e.

$$\alpha^3 + 4\alpha^2 + 12\alpha + 2 = 0$$

. Thus, α is a root of $g(x) := x^3 + 4x^2 + 12x + 2$. This polynomial is monic, and is irreducible by Eisenstein. $\square$

Problem III

Let $p \equiv_4 3$ be a prime, and let $K = \mathbb{Q}(\sqrt{p})$. It is known that h_K is odd. As a result, there exist integers $a, b \in \mathbb{Z}$ such that $a^2 - pb^2 = (-1)^{\frac{p+1}{4}} 2$

Proof. Consider the ideal $< 2, 1 + \sqrt{p} >$ in K. Then $< 2, 1 + \sqrt{p} > = < 2, 1 + \sqrt{p} - 2\sqrt{p} > = < 2, 1 - \sqrt{p} >$

$$
\begin{aligned}
< 2, 1 + \sqrt{p} >^2 = & \\
& = < 2, 1 + \sqrt{p} >< 2, 1 - \sqrt{p} > \\
& = < 4, 1 - p > \\
& = < 2 >
\end{aligned}
$$

The last equality follows because $1 - p \equiv_4 2 \implies \exists m \in \mathbb{Z} : (1 - p) + 4m = 2$, and both 4 and $1 - p$ are generated by 2. Therefore, the ideal $< 2, 1 + \sqrt{p} >^2$ is principal. The order of the class $[< 2, 1 + \sqrt{p} >]$ then divides both two and h_K(odd), so it must be 1. Thus, $< 2, 1 + \sqrt{p} >$ is principal. This means that there exist $a, b \in \mathbb{Z}$ such that $< 2, 1 + \sqrt{p} > = < a + b\sqrt{p} >$. Then,

$$< 2 > = < 2, 1 + \sqrt{p} >^2 = < a + b\sqrt{p} >^2 = < a + b\sqrt{p} >< a - b\sqrt{p} > = < a^2 - pb^2 >$$

Since $a^2 - pb^2 \in \mathbb{Z}$ and 2 both generate the same ideal, they must differ by a unit in $\mathbb{Z}$. Thus,

$$a^2 - pb^2 = \pm 2$$

. We know that $a^2, b^2 \equiv_8 1$ or 4, and that $p \equiv_8 3 + 4(\frac{p+1}{4})$, so we break into cases:

$[a^2]_8$	$[b^2]_8$	$[p]_8$	$[a^2 - bp^2]_8$
1	1	3	6
1	1	7	2
1	4	3	5
1	4	7	5
4	1	3	1
4	1	7	5
4	4	3	0
4	4	7	0

To recap: if $p \equiv_8 3$, then $a^2 - bp^2 \equiv_8 6$, so $a^2 - bp^2 = (-2)$. Conversely, if $p \equiv_8 7$, then $a^2 - bp^2 \equiv_8 2$, so $a^2 - bp^2 = 2$. Combining these two cases into one equation, we see that

$$a^2 - pb^2 = (-1)^{\frac{p+1}{4}} 2$$

□