MATH 5362 Homework

Orin Gotchey

September 14, 2022

1 Homework 1

Lemma 1.1. *If $\alpha^n \in \mathscr{O}_K$ for some natural number $n \in \mathbb{N}$ and field K, then $\alpha \in \mathscr{O}_K$*

Proof. Let α, n , K be as stated. Then there exists some $g(x) \in \mathbb{Z}[x]$, written

$$g(x) = \Sigma_{i=0}^{deg(g)}(\beta_i x^i) \tag{1}$$

where $\beta_i \in \mathbb{Z}$, and such that $g(\alpha^n) = 0$. But α must be a root of:

$$h(x) := g(x^n) \in \mathbb{Z}[x] \tag{2}$$

□

Proposition 1.2. *Problem 1*
$\theta := \frac{10^{\frac{2}{3}}-1}{\sqrt{-3}}$ *is an algebraic integer.*

Proof.

$$\omega := (-3 \cdot \theta^2) + 1 = 10^{\frac{4}{3}} - 2 * 10^{\frac{2}{3}} \tag{3}$$

Since $\mathscr{O}$ is a ring, and since $10^{\frac{2}{3}}$ is a root of $f(x) = x^3 - 100$, and is therefore an algebraic integer, we get: $\omega \in \mathscr{O}$. That is, there exists some $f \in \mathbb{Z}[x]$ such that $f(\omega) = 0$. But then $f(-3 \cdot \theta^2) = 0$ gives rise to another $g(x) \in \mathbb{Z}[x]$ such that $g(\theta) = 0$. So $\theta \in \mathscr{O}$, as required; □

Lemma 1.3. *Let $m \in \mathbb{N}$. Then $\sqrt{m}$ is irrational or an integer.*

Proof. Assume $\sqrt{m}$ is a non-integer rational. Then there exist some $a \neq b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$ and $\sqrt{m} = \frac{a}{b}$. Thus, $m = \frac{a^2}{b^2}$, and we know from the Fundamental Theorem of Arithmetic that $\gcd(a^2, b^2) = 1$. This forces $a^2 = b^2$ or $a = b$, contradiction. □

Proposition 1.4. *Problem 2*
For a given $m \in \mathbb{N}$, the quantity $\alpha := \frac{\sqrt{m}+1}{\sqrt{2}}$ is an algebraic integer iff m is odd.

Proof. First note that m is odd iff the quantity $(m+1)^2 \equiv_4 0$, which in turn is true iff the polynomial

$$f(x) = x^4 - (m+1)x^2 - (\frac{3}{4}(m+1)^2 + 3m) = 0$$

is an element of $\mathbb{Z}[x]$. α is a root of $f(x)$ (check), completing the forward direction. Now assume that α is an algebraic integer. Then let $p(x) \in \mathbb{Z}[x]$ be the monic minimal polynomial for α. It holds that $p|f$ in $\mathbb{Q}[x]$. We will show that this forces $f(x) \in \mathbb{Z}[x]$, completing the proof.
We know that $1 \leq \deg(p) \leq 4$, so three cases for $\deg(p)$:

1. $\deg(p) = 1$ would imply that $\alpha \in \mathbb{Z}$, but the constant term of f must be $\alpha * p_0$ for some $p_0 \in \mathbb{Z}$, whence it follows $f(x) \in \mathbb{Z}[x]$.
2. $\deg(p) = 2$. Let $p(x) = x^2 + p_1 x + p_0$. Then there exist $a, b, c \in \mathbb{Q}$ such that
$$(x^2 + p_1 x + p_0)(ax^2 + bx + c) = f(x)$$
This implies that $a = 0$, and then $b = -p_1$ combined with the fact that $p_0 + c + pb_1 \in \mathbb{Z}$ grants us that $a, b, c \in \mathbb{Z}$, and thus $f(x) \in \mathbb{Z}[x]$
3. $\deg(p) = 3$. Let $p(x) = x^3 + p_2 x^2 + p_1 x + p_0$ with the $p_i \in \mathbb{Z}$, and then there is some $a \in \mathbb{Q}$ such that $p(x)(x + a) = f(x)$. But since f has no term of degree 3, $p_2 + a = 0$, but then $x - a \in \mathbb{Z}[x]$, so $f(x) \in \mathbb{Z}[x]$.
4. $\deg(p) = 4$. Then $p(x) = f(x)$, whence it follows $f(x) \in \mathbb{Z}[x]$.

□

Proposition 1.5. *Let* $\alpha := (\frac{1+\sqrt{2}}{9})^{\frac{1}{3}} + (\frac{1-\sqrt{2}}{9})^{\frac{1}{3}}$. *Then* $\alpha/729$ *is an algebraic integer*

Proof. α satisfies the equation $\alpha^3 + 3^{\frac{1}{3}}\alpha - \frac{2}{9} = 0$. That is,

$$3^{\frac{1}{3}}\alpha = -\alpha^3 + \frac{2}{9}$$
$$3\alpha^3 = -\alpha^9 + \frac{2}{3}\alpha^6 - \frac{4}{27}\alpha^3 + \frac{8}{729}$$
$$729\alpha^9 - 486\alpha^6 + 2305\alpha^3 - 8 = 0$$
$$729^{10}(\frac{\alpha}{729})^9 + ... = 0$$

Thus, $\frac{\alpha}{729}$ is an algebraic integer. □

Proposition 1.6. *The minimal polynomials of* $\alpha := \frac{1+i}{\sqrt{2}}$ *over* $\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$, *respectively, are:*

- $f(x) = x^4 + 1$

- $g(x) = x^2 - i$
- $h(x) = x^2 - \sqrt{2}x + 1$

Proof. Clearly, these are monic polynomials over their respective fields of which α is a root. Since α is a primitive 8th root of unity, and f is the 8-th cyclotomic polynomial, it is irreducible. g and h are irreducible because $\alpha \notin \mathbb{Q}(i)$ and $\alpha \notin \mathbb{Q}(\sqrt{2})$. $\square$

Proposition 1.7. *$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{6})$ and also $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) : \mathbb{Q}] = 8$.*

The minimal polynomials of $\sqrt{2}$ and $\sqrt{3}$ are $x^2 - 2$ and $x^2 - 3$, respectively. Since $\frac{-2\sqrt{2}}{-2\sqrt{3}} \notin \mathbb{Q}$, then any $c \in \mathbb{Q}$ gives us a primitive element, $\theta = c\sqrt{2} + \sqrt{3}$ generating $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let $c = 1$. Then $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Also, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, because $\sqrt{3}$ is not a $\mathbb{Q}$-linear combination of $\{1, \sqrt{2}\}$. The conjugates of $\sqrt{2} + \sqrt{3}$ are just $\pm\sqrt{2} \pm \sqrt{3}$, and the other conjugate of $\sqrt{5}$ is $-\sqrt{5}$. We need to find a $c \in \mathbb{Q}$ such that

$$c \neq \frac{(\sqrt{2} + \sqrt{3}) \pm \sqrt{2} \pm \sqrt{3}}{2\sqrt{5}}$$

again, $c = 1$ is suitable, so it follows that

$$\mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$$

Now, all we need to show is that $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$. This would require some $a, b, c \in \mathbb{Q}$ such that

$$\begin{aligned}
\sqrt{5} &= a\sqrt{2} + b\sqrt{3} + c\sqrt{6} \\
5 &= 2a^2 + 3b^3 + 6c^2 + ab\sqrt{6} + ac\sqrt{12} + bc\sqrt{18} \\
&ab\sqrt{6} + 2ac\sqrt{3} + 3bc\sqrt{2} \in \mathbb{Q}
\end{aligned}$$

But $\sqrt{2}$,$\sqrt{3}$,and $\sqrt{6}$ are linearly independent over $\mathbb{Q}$. If they weren't, then there would be $\alpha, \beta \in \mathbb{Q}$:

$$\sqrt{6} = \alpha\sqrt{2} + \beta\sqrt{3}$$

$$\begin{aligned}
6 &= 2\alpha^2 + 3\beta^2 + 2\alpha\beta\sqrt{6} \\
\sqrt{6} &\in \mathbb{Q}
\end{aligned}$$

(contradiction, see above). Thus: $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5} : \mathbb{Q})] = 8$