MATH 7230 Homework 2

Andrea Bourque

January 2021

1 Problem 2.1 1

If $E = \mathbb{Q}(\theta)$ where θ is a root of $X^3 - 3X + 1$, find the norm and trace of θ^2.

Proof. We begin by analyzing how θ^2 acts on the basis $\{1, \theta, \theta^2\}$ of $E/\mathbb{Q}$. First, $\theta^2 \cdot 1 = \theta^2$. Next, $\theta^2 \cdot \theta = \theta^3 = 3\theta - 1$. Finally, $\theta^2 \cdot \theta^2 = \theta^4 = 3\theta^2 - \theta$. Thus over this basis, the map given by multiplication by θ^2 is

$$\begin{pmatrix} 0 & -1 & 0 \\ 0 & 3 & -1 \\ 1 & 0 & 3 \end{pmatrix}.$$

Thus the trace of θ^2 is 6, and the norm of θ^2 is 1. □

2 Problem 2.1 2

Find the trace of the primitive 6^{th} root of unity ω in the cyclotomic extension $\mathbb{Q}_6 = \mathbb{Q}(\omega)$.

Proof. Note that in this case, the characteristic polynomial of ω is equal to the minimal polynomial, which is $\omega^2 - \omega + 1 = 0$. Then the trace is 1, and the norm is also 1. □

3 Problem 2.1 4

Let θ be a root of $X^4 - 2$ over $\mathbb{Q}$. Show that $\sqrt{3}$ cannot belong to $\mathbb{Q}[\theta]$.

Proof. Note to Dr. Long: I'm not sure how to prove this using the machinery developed so far. I tried using some field theory but got nowhere. So I stuck to my competition math roots and made this dirty.

We have a basis for $\mathbb{Q}[\theta]$ given by $\{1, \theta, \theta^2, \theta^3\}$. Thus suppose $\sqrt{3} = a + b\theta + c\theta^2 + d\theta^3$ with $a, b, c, d \in \mathbb{Q}$. Squaring both sides gives

$$3 = (a^2 + 2c^2 + 4bd) + (2ab + 4cd)\theta + (b^2 + 2d^2 + 2ac)\theta^2 + (2ad + 2bc)\theta^3.$$

By equating the θ and θ^3 coefficients on the left and right hand sides, we get $ab = -2cd$ and $ad = -bc$. Then $a^2bd = 2c^2bd$, and $b^2ac = 2d^2ac$.

First, if we suppose $bd \neq 0$, we get that $a^2 = 2c^2$. We know that $\sqrt{2} \notin \mathbb{Q}$, so $a = c = 0$. Equating the θ^2 coefficients then gives $b^2 + 2d^2 = 0$, which is only possible if $b = d = 0$, a contradiction.

Next, if we suppose $ac \neq 0$, we get that $b^2 = 2d^2$. Then $b = d = 0$. Once again looking at the θ^2 coefficients, we get $ac = 0$, a contradiction.

Thus, $ac = bd = 0$. Looking at the θ^2 equation gives $b^2 + 2d^2 = 0$, which implies $b = d = 0$. Looking at the 1 coefficient, we have $a^2 + 2c^2 = 3$. Since $ac = 0$, we have $a = 0$ or $c = 0$. If $a = 0$, then $2c^2 = 3$, which is not solvable in $\mathbb{Q}$. If $c = 0$, we have $a^2 = 3$, which is also not solvable in $\mathbb{Q}$. Thus we have arrived at a final contradiction from the assumption that $\sqrt{3} \in \mathbb{Q}[\theta]$. $\square$

4 Problem 2.2 1

Let $L = \mathbb{Q}(\alpha)$, where α is a root of the irreducible quadratic $X^2+bX+c \in \mathbb{Q}[X]$. Show that $L = \mathbb{Q}(\sqrt{m})$ for some square-free integer m.

Proof. By the quadratic formula, the roots are $\frac{-b \pm \sqrt{b^2-4c}}{2}$. Let $b = \frac{s}{t}, c = \frac{p}{q}$, where $s, t, p, q \in \mathbb{Z}$. Then $\sqrt{b^2-4c} = \sqrt{\frac{s^2q^2-4t^2pq}{t^2q^2}} = \frac{\sqrt{s^2q^2-4t^2pq}}{tq}$. Then let m be the product of the unique prime divisors of $s^2q^2 - 4t^2pq$, so that $n\sqrt{m} = \sqrt{s^2q^2-4t^2pq}$ for some $n \in \mathbb{N}$, and, m is by definition square-free. Then $\alpha \in \{\frac{-b}{2} \pm \frac{n\sqrt{m}}{2tq}\} \subseteq \mathbb{Q}(\sqrt{m})$. Furthermore, $\sqrt{m} \in \{\pm\frac{tq}{n}(2\alpha+b)\} \subseteq \mathbb{Q}(\alpha)$. Thus the extensions are equal, as desired. □

5 Problem 2.2 2

Show that the quadratic extensions $\mathbb{Q}(\sqrt{m})$, m square-free, are all distinct.

Proof. Suppose $\sqrt{n} = a + b\sqrt{m}$, where n, m are square-free integers, and $a, b \in \mathbb{Q}$. Then $n = (a^2 + b^2 m) + 2ab\sqrt{m}$. Then $ab = 0$, so $a = 0$ or $b = 0$. If $b = 0$, then $\sqrt{n} = a \in \mathbb{Q}$, so $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}$ is not a quadratic extension. Thus $a = 0$, so $n = b^2 m$. Let $b = \frac{s}{t}$, where $s, t \in \mathbb{Z}$ are in reduced form. Then $t^2 n = s^2 m$. Both m, n are square-free, but both sides have square integer terms, implying that they must cancel out, giving $n = m$. □

6 Problem 2.2 5

Give an example of a quadratic extension of $\mathbb{Q}$ that is also a cyclotomic extension.

Proof. $\mathbb{Q}(\sqrt{-3})$ is the cyclotomic extension given by $\zeta_3 = e^{2\pi i/3} = \frac{-1}{2} + \frac{\sqrt{-3}}{2}$. □

7 Problem 2.3 1

Let $x_1, ..., x_n$ be arbitrary algebraic integers in a number field, and consider the direct expansion of the determinant of the matrix $(\sigma_i(x_j))$. Let P be the sum of those terms prefixed by plus signs, and N the sum of those terms prefixed by minus signs. Then the discriminant D of $(x_1, ..., x_n)$ is $(P-N)^2$. Show that $P+N$ and PN are fixed by each σ_i, and deduce that they are rational numbers.

Proof. Each term in the expansion is of the form $\prod_{i=1}^{n} \sigma_i(x_{\tau(i)})$, where $\tau \in S_n$. P is the sum of the terms where τ is an even permutation, and N is the sum of the terms where τ is an odd permutation. Furthermore, each σ_i induces a permutation on the set of σ_j, say $\sigma_i \circ \sigma_j = \sigma_{\rho(j)}$. Thus if ρ is even, σ_i will preserve the even and odd permutations. If ρ is odd, then σ_i will reverse the permutations. That is to say, either $\sigma_i(P) = P$, $\sigma_i(N) = N$, or $\sigma_i(P) = N$, $\sigma_i(N) = P$. In either case, $\sigma_i(P + N) = P + N$ and $\sigma_i(PN) = PN$. Thus $P + N$ and PN are rational since they are fixed by each embedding. □

8 Problem 2.3 2

Show that $P + N$ and PN are rational integers.

Proof. Since the x_i were given to be algebraic, so are the $\sigma_i(x_j)$, and therefore so are the sums of products of the $\sigma_i(x_j)$. Thus $P + N$ and PN are algebraic, and they are rational, so they are rational integers. □

9 Problem 2.3 3

Show that $D \equiv 0$ or $1 \bmod 4$.

Proof. $D = (P-N)^2 = (P+N)^2 - 4PN$, so D is a square mod 4. The only squares are $0, 1$, so we get the desired result. □