Problem 9.6. Let $K \subseteq L \subseteq M$ be a chain of fields, with $[M : K] < \infty$.

(1) For $\theta \in M$, show that $T_{L/K}(T_{M/L}(\theta)) = T_{M/K}(\theta)$.
(2) For $\theta \in M$, show that $N_{L/K}(N_{M/L}(\theta)) = N_{M/K}(\theta)$.

Solution Let $\beta_1, \ldots \beta_m$ be an L-basis for M and let $\alpha_1, \ldots, \alpha_\ell$ be a K-basis for L. As we checked in class, $\alpha_i \beta_j$ is then a K-basis for M. For $\phi \in L$, let $\lambda(\phi)$ be the $\ell \times \ell$ matrix giving multiplication by ϕ in the α-basis. Note that λ is a map of rings from L to $\mathrm{Mat}_{\ell \times \ell}(K)$ and that, by definition, $\mathrm{Tr}\ \lambda(\phi) = T_{L/K}(\phi)$.

For $\theta \in M$, let $[\phi_{jj'}]_{1 \leq j, j' \leq m}$ be the matrix for multiplication by θ in the β-basis. Then multiplication by θ in the $\alpha_i \beta_j$ basis is given by the $(\ell m) \times (\ell m)$ matrix made up of the $\ell \times \ell$ blocks $\lambda(\phi_{jj'})$.

It is now straightforward to do part (1). To take the trace of a matrix in block form (with the same block sizes in rows and columns), we add up the traces of the diagonal matrices. So

$$T_{M/K}(\theta) = \sum_{j=1}^{m} \mathrm{Tr}\ \lambda(\phi_{jj}) = \mathrm{Tr}\ \lambda\left(\sum_{j=1}^{m} \phi_{jj}\right) = \mathrm{Tr}\ \lambda\big(T_{M/L}(\theta)\big) = T_{L/K}(T_{M/L}(\theta)).$$

The corresponding computation for determinants is messy, but isn't bad if we write m_θ in rational canonical form. To keep exposition simple, I'll assume that $M = L(\theta)$, so that the rational canonical form has only one block. Let the minimal polynomial of θ over L be $x^m - f_1 x^{m-1} + f_2 x^{m-2} - \cdots + (-1)^m f_m$; note that $f_m = N_{M/L}(\theta)$. So, if we choose the correct L-basis β_j for M, then multiplication by θ is given by the matrix

$$\begin{bmatrix} & & & & (-1)^{m+1} f_m \\ 1 & & \cdots & & (-1)^m f_{m-1} \\ & 1 & \cdots & & (-1)^{m-1} f_{m-2} \\ & & 1\ \cdots & & (-1)^{m-2} f_{m-3} \\ & & \ddots & & \vdots \\ & & & 1 & f_1 \end{bmatrix}.$$

If we then work in the $\alpha_i \beta_j$ basis for these β's, we get the block matrix

$$\begin{bmatrix} & & & & (-1)^{m+1} \lambda(f_m) \\ \mathrm{Id}_\ell & & \cdots & & (-1)^m \lambda(f_{m-1}) \\ & \mathrm{Id}_\ell & \cdots & & (-1)^{m-1} \lambda(f_{m-2}) \\ & & \mathrm{Id}_\ell\ \cdots & & (-1)^{m-2} \lambda(f_{m-3}) \\ & & \ddots & & \vdots \\ & & & \mathrm{Id}_\ell & \lambda(f_1) \end{bmatrix}.$$

The determinant of this is

$$\det \lambda(f_m) = N_{L/K}(f_m) = N_{L/K}(N_{M/L}(\theta)).$$

The reader may wonder if we dropped a sign; we did not. If we move the top row of the matrix to the bottom, we introduce $\ell(m-1) \times \ell = \ell^2(m-1)$ inversions. In the resulting matrix, the diagonal elements are $m-1$ identity matrices and one copy of $(-1)^{m+1}\lambda(f_m)$; we have $\det (-1)^{m+1}\lambda(f_m) = (-1)^{\ell(m+1)} \det \lambda(f_m)$. So our total sign is $(-1)^{\ell^2(m-1) + \ell(m+1)}$. We have $\ell^2(m-1) + \ell(m+1) \equiv \ell(m-1) + \ell(m+1) = 2\ell m \equiv 0 \bmod 2$.

Problem 9.8. Let ω be a primitive cube root of unity in $\mathbb{C}$. Let $K = \mathbb{Q}(\omega)$ and write $\alpha \mapsto \overline{\alpha}$ for the automorphism $\omega \mapsto \omega^{-1}$ of K. For a nonzero element α of K, let $L = K(\sqrt[3]{\alpha},\ \sqrt[3]{\overline{\alpha}})$.

(1) Show that $L/\mathbb{Q}$ is a Galois extension.
(2) Let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ show that either (1) there are integers b and c such that $\sigma(\omega^i \sqrt[3]{\alpha}) = \omega^{b+i} \sqrt[3]{\alpha}$ and $\sigma(\omega^j \sqrt[3]{\overline{\alpha}}) = \omega^{c+j} \sqrt[3]{\overline{\alpha}}$ or else (2) there are integers b and c such that $\sigma(\omega^i \sqrt[3]{\alpha}) = \omega^{b-i} \sqrt[3]{\overline{\alpha}}$ and $\sigma(\omega^j \sqrt[3]{\overline{\alpha}}) = \omega^{c-j} \sqrt[3]{\alpha}$ (for all integers i, j).
(3) If $\alpha\overline{\alpha}^2$ is a cube in K, show that $\mathrm{Gal}(L/\mathbb{Q})$ is abelian.

Solution To make the solution more readable, we assume $\alpha \neq \overline{\alpha}$. Note that the polynomial $(x-\alpha)(x-\overline{\alpha})$ has coefficients in $\mathbb{Q}$. The field L is the splitting polynomial of $(x^3-\alpha)(x^3-\overline{\alpha})$, so $L/\mathbb{Q}$ is Galois.

For part (2), we must either have $\sigma(\omega) = \omega$ or $\sigma(\omega) = \omega^{-1}$.

In the first case, σ acts trivially on K, so $\sigma(\alpha) = \alpha$ and σ must take $\sqrt[3]{\alpha}$ to $\omega^b \sqrt[3]{\alpha}$ for some b. We then have $\sigma(\omega^i \sqrt[3]{\alpha}) = \sigma(\omega)^i \sigma(\sqrt[3]{\alpha}) = \omega^i \omega^b \sqrt[3]{\alpha}$. We similarly have $\sigma(\omega^j \sqrt[3]{\overline{\alpha}}) = \omega^j \omega^c \sqrt[3]{\overline{\alpha}}$ for some c.

In the second case, we have $\sigma(\omega) = \overline{\omega}$ so $\sigma(\alpha) = \overline{\alpha}$. So $\sigma(\sqrt[3]{\alpha})$ must be a cube root of $\overline{\alpha}$, say $\omega^b \sqrt[3]{\overline{\alpha}}$. So $\sigma(\omega^i \sqrt[3]{\alpha}) = \sigma(\omega)^i \sigma(\sqrt[3]{\alpha}) = \omega^{-i} \omega^b \sqrt[3]{\overline{\alpha}}$. Similarly, $\sigma(\omega^j \sqrt[3]{\overline{\alpha}}) = \omega^{-j} \omega^c \sqrt[3]{\alpha}$ for some c.

We now more to part (3). Let $\alpha\overline{\alpha}^2 = \beta^3$ so $\sqrt[3]{\alpha}\sqrt[3]{\overline{\alpha}}^2 = \omega^k \beta$ for some k. Thus, for any $\sigma \in \mathrm{Gal}(L/K)$, we must have $\sigma\left(\sqrt[3]{\alpha}\sqrt[3]{\overline{\alpha}}^2\right) = \sqrt[3]{\alpha}\sqrt[3]{\overline{\alpha}}^2$. We have $\sigma \in \mathrm{Gal}(L/K)$ if and only if σ is in the first case where $\sigma(\omega^i \sqrt[3]{\alpha}) = \omega^{b+i} \sqrt[3]{\alpha}$ and $\sigma(\omega^j \sqrt[3]{\overline{\alpha}}) = \omega^{c+j} \sqrt[3]{\overline{\alpha}}$. So $\sigma\left(\sqrt[3]{\alpha}\sqrt[3]{\overline{\alpha}}^2\right) = \sqrt[3]{\alpha}\sqrt[3]{\overline{\alpha}}^2$ gives $b + 2c \equiv 0 \bmod 3$ or, in other words, $b \equiv c \bmod 3$.

What about σ which are not in $\mathrm{Gal}(L/K)$? I think the simplest route is to think about σ^2. If $\sigma(\omega^i \sqrt[3]{\alpha}) = \omega^{b-i} \sqrt[3]{\overline{\alpha}}$ and $\sigma(\omega^j \sqrt[3]{\overline{\alpha}}) = \omega^{c-j} \sqrt[3]{\alpha}$ then

$$\sigma^2(\sqrt[3]{\alpha}) = \sigma(\omega^b \sqrt[3]{\overline{\alpha}}) = \omega^{-b+c} \sqrt[3]{\alpha} \text{ and } \sigma^2(\sqrt[3]{\overline{\alpha}}) = \sigma(\omega^c \sqrt[3]{\alpha}) = \omega^{-c+b} \sqrt[3]{\overline{\alpha}}.$$

Using our previous result, we get that $-b + c \equiv b - c \bmod 3$, which implies that $b \equiv c \bmod 3$.

So we have now reduced to the group to the smaller group of maps of the form $(\sqrt[3]{\alpha},\ \sqrt[3]{\overline{\alpha}}) \mapsto (\omega^b \sqrt[3]{\alpha},\ \omega^b \sqrt[3]{\overline{\alpha}})$ and $(\sqrt[3]{\alpha},\ \sqrt[3]{\overline{\alpha}}) \mapsto (\omega^b \sqrt[3]{\overline{\alpha}},\ \omega^b \sqrt[3]{\alpha})$, and this group is easily checked to be abelian.