# TRACE AND NORM

KEITH CONRAD

## 1. Introduction

Let $L/K$ be a finite extension of fields, with $n = [L : K]$. We will associate to this extension two important functions $L \to K$, called the trace and the norm. They are related to the trace and determinant of matrices and have many important applications in the study of fields (and rings). Among elementary applications, the trace can be used to show certain numbers are not in certain fields and the norm can be used to show some number in $L$ is not a perfect power in $L$. The math behind the definitions of the trace and norm also leads to a systematic way of finding the minimal polynomial over $K$ of any element of $L$.

## 2. Basic Definitions

Our starting point is the process by which an abstract linear transformation $\varphi\colon V \to V$ from an $n$-dimensional $K$-vector space $V$ to itself is turned into a matrix: for a basis $\{e_1, \ldots, e_n\}$ of $V$, write $\varphi(e_j) = \sum_{i=1}^n a_{ij}e_i$, with $a_{ij} \in K$.[1] We declare the *matrix* of $\varphi$ with respect to that basis, also called the *matrix representation* of $\varphi$, to be $[\varphi] := (a_{ij})$. This definition is motivated by the way entries of a square matrix $A = (a_{ij})$ can be recovered from the effect of $A$ on the standard basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ of $K^n$: $A\mathbf{e}_j = \sum_{i=1}^n a_{ij}\mathbf{e}_i$ (the $j$th column of $A$).

**Example 2.1.** Let $\varphi\colon \mathbf{C} \to \mathbf{C}$ be complex conjugation: $\varphi(z) = \overline{z}$. This is $\mathbf{R}$-linear: $\overline{z + z'} = \overline{z} + \overline{z'}$ and $\overline{cz} = c\overline{z}$ for $c \in \mathbf{R}$. Using the basis $\{1, i\}$, we compute the complex conjugate of each number in the basis and write the answer in terms of the basis:

$$\begin{aligned} \varphi(1) &= 1 = 1 \cdot 1 + 0 \cdot i, \\ \varphi(i) &= -i = 0 \cdot 1 + (-1) \cdot i. \end{aligned}$$

From the coefficients in the first equation, the first column of $[\varphi]$ is $\binom{1}{0}$, and from the coefficients in the second equation, the second column is $\binom{0}{-1}$, so $[\varphi]$ is

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

If instead we use the basis $\{1 + i, 1 + 2i\}$, then

$$\begin{aligned} \varphi(1 + i) &= 1 - i = 3 \cdot (1 + i) - 2 \cdot (1 + 2i), \\ \varphi(1 + 2i) &= 1 - 2i = 4 \cdot (1 + i) + (-3) \cdot (1 + 2i). \end{aligned}$$

Now the first column of $[\varphi]$ is $\binom{3}{-2}$ and the second column is $\binom{4}{-3}$, so $[\varphi]$ is

$$\begin{pmatrix} 3 & 4 \\ -2 & -3 \end{pmatrix}.$$

[1] Watch the indices! It is not $\varphi(e_i) = \sum_{j=1}^n a_{ij}e_j$. The point is that $a_{ij}$ appears in the formula for $\varphi(e_j)$, not $\varphi(e_i)$.

If the basis of $V$ changes, or even the order of the terms in the basis changes, then the matrix usually changes, but it will be a conjugate of the first matrix. (Two squares matrices $M$ and $N$ are called conjugate if $N = UMU^{-1}$ for an invertible matrix $U$.) Conjugate matrices have the same trace (trace = sum of main diagonal entries) and determinant, so we declare $\mathrm{Tr}(\varphi) = \mathrm{Tr}([\varphi])$ and $\det(\varphi) = \det([\varphi])$, using *any* matrix representation of $\varphi$. For instance, both matrix representations we computed for complex conjugation on $\mathbf{C}$, treated as an $\mathbf{R}$-linear map, have trace 0 and determinant $-1$.

We turn now to field extensions. For a finite extension of fields $L/K$, we associate to each element $\alpha$ of $L$ the $K$-linear transformation $m_\alpha\colon L \to L$, where $m_\alpha$ is multiplication by $\alpha$: $m_\alpha(x) = \alpha x$ for $x \in L$. Each $m_\alpha$ is a $K$-linear function from $L$ to $L$:

$$m_\alpha(x+y) = \alpha(x+y) = \alpha x + \alpha y = m_\alpha(x) + m_\alpha(y), \quad m_\alpha(cx) = \alpha(cx) = c(\alpha x) = cm_\alpha(x)$$

for $x$ and $y$ in $L$ and $c \in K$. By choosing a $K$-basis of $L$ we can create a matrix representation for $m_\alpha$, which is denoted $[m_\alpha]$. (We need to put an ordering on the basis to get a matrix, but we will often just refer to picking a basis and listing it in a definite way instead of saying "pick an ordered basis".)

**Example 2.2.** Let $K = \mathbf{R}$, $L = \mathbf{C}$, and use basis $\{1, i\}$. For $\alpha = a + bi$ with real $a$ and $b$, when we multiply the basis 1 and $i$ by $\alpha$ and write the answer in terms of the basis we have

$$\begin{aligned} \alpha \cdot 1 &= a \cdot 1 + bi, \\ \alpha \cdot i &= -b \cdot 1 + ai. \end{aligned}$$

Therefore the first column of $[m_\alpha]$ is $\binom{a}{b}$ and the second column is $\binom{-b}{a}$: $[m_\alpha]$ equals

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Using the basis $\{i, 1\}$, which is the same basis listed in the opposite order, we compute

$$\begin{aligned} \alpha \cdot i &= ai + (-b) \cdot 1, \\ \alpha \cdot 1 &= bi + a \cdot 1 \end{aligned}$$

and $[m_\alpha]$ changes to

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

which serves as a reminder that $[m_\alpha]$ depends on the ordering of the $K$-basis of $L$.

**Example 2.3.** Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt{2})$. Use the basis $\{1, \sqrt{2}\}$. For $\alpha = a + b\sqrt{2}$ with rational $a$ and $b$, we multiply it by 1 and $\sqrt{2}$:

$$\begin{aligned} \alpha \cdot 1 &= a \cdot 1 + b\sqrt{2}, \\ \alpha \cdot \sqrt{2} &= 2b \cdot 1 + a\sqrt{2}. \end{aligned}$$

Therefore $[m_\alpha]$ equals

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}.$$

**Example 2.4.** Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt[3]{2})$. Using the basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$, the matrix representation for multiplication by $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ on $L$, where $a$, $b$, and $c$ are rational,

is obtained by multiplying $\alpha$ by 1, $\sqrt[3]{2}$, and $\sqrt[3]{4}$:

$$\begin{aligned} \alpha \cdot 1 &= a + b\sqrt[3]{2} + c\sqrt[3]{4}, \\ \alpha \cdot \sqrt[3]{2} &= 2c + a\sqrt[3]{2} + b\sqrt[3]{4}, \\ \alpha \cdot \sqrt[3]{4} &= 2b + 2c\sqrt[3]{2} + a\sqrt[3]{4}. \end{aligned}$$

From these calculations, $[m_\alpha]$ is

$$\begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix}.$$

**Example 2.5.** Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\gamma)$ for $\gamma$ a root of $X^3 - X - 1$. Then $\gamma^3 = 1 + \gamma$. Use the basis $\{1, \gamma, \gamma^2\}$. For $\alpha = a + b\gamma + c\gamma^2$ with rational $a$, $b$, and $c$, multiply $\alpha$ by 1, $\gamma$, and $\gamma^2$:

$$\begin{aligned} \alpha \cdot 1 &= a + b\gamma + c\gamma^2, \\ \alpha \cdot \gamma &= a\gamma + b\gamma^2 + c\gamma^3 = c + (a+c)\gamma + b\gamma^2, \\ \alpha \cdot \gamma^2 &= c\gamma + (a+c)\gamma^2 + b\gamma^3 = b + (b+c)\gamma + (a+c)\gamma^2. \end{aligned}$$

Therefore $[m_\alpha]$ equals

$$\begin{pmatrix} a & c & b \\ b & a+c & b+c \\ c & b & a+c \end{pmatrix}.$$

**Example 2.6.** Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\gamma)$ for $\gamma$ a root of $X^4 - X - 1$ (which is irreducible over $\mathbf{Q}$ since it's irreducible mod 2). Use the basis $\{1, \gamma, \gamma^2, \gamma^3\}$. For $\alpha = a + b\gamma + c\gamma^2 + d\gamma^3$ with rational $a$, $b$, $c$, and $d$, verify that $[m_\alpha]$ equals

$$\begin{pmatrix} a & d & c & b \\ b & a+d & c+d & b+c \\ c & b & a+d & c+d \\ d & c & b & a+d \end{pmatrix}.$$

**Example 2.7.** If $c \in K$, then with respect to any $K$-basis of $L$, $[m_c]$ is the scalar diagonal matrix $cI_n$, where $n$ is the dimension of $L$ over $K$: if $\{e_1, \ldots, e_n\}$ is a $K$-basis then $m_c(e_j) = ce_j$, so $[m_c]$ has $j$th column with a $c$ in the $j$th row and 0 elsewhere.

Here, finally, are the trace and norm mappings that we want to study.

**Definition 2.8.** The *trace* and *norm* of $\alpha$ from $L$ to $K$ are the trace and determinant of any matrix representation for $m_\alpha$ as a $K$-linear map:

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}([m_\alpha]) \in K, \quad \mathrm{N}_{L/K}(\alpha) = \det([m_\alpha]) \in K.$$

Let's use matrices in our previous examples to calculate some trace and norm formulas. By Example 2.2,

$$\mathrm{Tr}_{\mathbf{C}/\mathbf{R}}(a + bi) = 2a, \quad \mathrm{N}_{\mathbf{C}/\mathbf{R}}(a + bi) = a^2 + b^2.$$

By Example 2.3,

$$\mathrm{Tr}_{\mathbf{Q}(\sqrt{2})/\mathbf{Q}}(a + b\sqrt{2}) = 2a, \quad \mathrm{N}_{\mathbf{Q}(\sqrt{2})/\mathbf{Q}}(a + b\sqrt{2}) = a^2 - 2b^2.$$

By Example 2.4,

$$\mathrm{Tr}_{\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = 3a, \quad \mathrm{N}_{\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc.$$

By Example 2.5, $\mathrm{Tr}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(a+b\gamma+c\gamma^2) = 3a+2c$ and

$$\mathrm{N}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(a+b\gamma+c\gamma^2) = a^3+b^3+c^3-ab^2+ac^2-bc^2+2a^2c-3abc.$$

By Example 2.6, $\mathrm{Tr}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(a+b\gamma+c\gamma^2+d\gamma^3) = 4a+3d$ and

$$\begin{aligned}\mathrm{N}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(a+b\gamma+c\gamma^2+d\gamma^3) &= a^4-b^4+c^4-d^4+3a^3d-2a^2c^2+3a^2d^2+ab^3+ac^3\\ &\quad +ad^3+2b^2d^2-bc^3-bd^3+cd^3-3a^2bc+4ab^2c-4a^2bd\\ &\quad -5abd^2+ac^2d+4acd^2+3b^2cd-4bc^2d-3abcd.\end{aligned}$$

By Example 2.7, for any $c \in K$ the matrix $[m_c]$ is $cI_n$, where $n = [L:K]$, so

$$\mathrm{Tr}_{L/K}(c) = nc, \quad \mathrm{N}_{L/K}(c) = c^n.$$

In particular, $\mathrm{Tr}_{L/K}(1) = [L:K]$ and $\mathrm{N}_{L/K}(1) = 1$.

**Remark 2.9.** In the literature you might see S or Sp used in place of Tr since Spur is the German word for trace (not because S is the first letter in the word "sum").

**Remark 2.10.** The word "norm" has another meaning in algebra besides the one above: a method of measuring the size of elements in a vector space is called a norm. For instance, when $\mathbf{v} = (a_1, \ldots, a_n)$ is in $\mathbf{R}^n$, its squared length $||\mathbf{v}|| = \mathbf{v} \cdot \mathbf{v} = a_1^2 + \cdots + a_n^2$ is called the norm of $\mathbf{v}$. This concept, suitably axiomatized, leads to normed vector spaces, which occur throughout analysis, but vector space norms have essentially nothing to do with the field norm we are using.

**Remark 2.11.** There is an alternate definition of $\mathrm{Tr}_{L/K}(\alpha)$ and $\mathrm{N}_{L/K}(\alpha)$ in terms of a sum and product running over the field embeddings of $L$ into an algebraic closure of $K$. See, for instance, [1, Chap. VI, Sec. 5]. That alternate definition is a bit clunky to work with when $L/K$ is not separable.

## 3. Initial Properties of the Trace and Norm

The most basic properties of the trace and norm follow from the way $m_\alpha$ depends on $\alpha$.

**Lemma 3.1.** *Let $\alpha$ and $\beta$ belong to $L$.*

1) *If $\alpha \neq \beta$ then $m_\alpha \neq m_\beta$,*
2) *As functions $L \to L$,*

$$m_{\alpha+\beta} = m_\alpha + m_\beta \quad \text{and} \quad m_{\alpha\beta} = m_\alpha \circ m_\beta,$$

*and $m_1$ is the identity map $L \to L$.*

Concretely, this says the matrices in the previous examples are embeddings of $L$ into the $n \times n$ matrices over $K$, where $n = [L:K]$. For instance, from Example 2.2 the $2 \times 2$ real matrices of the special form $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ add and multiply in the same way as complex numbers add and multiply. Compare multiplication:

$$(a+bi)(c+di) = (ac-bd)+(ad+bc)i, \quad \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix}.$$

*Proof.* Since $m_\alpha(1) = \alpha$, we can recover the number $\alpha$ from the mapping $m_\alpha$, so $\alpha \mapsto m_\alpha$ is injective.

For $\alpha$, $\beta$, and $x$ in $L$,

$$m_{\alpha+\beta}(x) = (\alpha+\beta)(x) = \alpha x + \beta x = m_\alpha(x) + m_\beta(x) = (m_\alpha + m_\beta)(x)$$

and

$$(m_\alpha \circ m_\beta)(x) = m_\alpha(\beta x) = \alpha(\beta x) = (\alpha\beta)x = m_{\alpha\beta}(x),$$

so $m_{\alpha+\beta} = m_\alpha + m_\beta$ and $m_{\alpha\beta} = m_\alpha \circ m_\beta$. Easily $m_1$ is the identity map on $L$: $m_1(x) = 1 \cdot x = x$ for all $x \in L$. □

**Theorem 3.2.** *The trace* $\mathrm{Tr}_{L/K}\colon L \to K$ *is* $K$*-linear and the norm* $\mathrm{N}_{L/K}\colon L \to K$ *is multiplicative. Moreover,* $\mathrm{N}_{L/K}(L^\times) \subset K^\times$.

*Proof.* We have equations $m_{\alpha+\beta} = m_\alpha + m_\beta$ and $m_{\alpha\beta} = m_\alpha \circ m_\beta$. Picking a basis of $L/K$ and passing to matrix representations in these equations, $[m_{\alpha+\beta}] = [m_\alpha + m_\beta] = [m_\alpha] + [m_\beta]$ and $[m_{\alpha\beta}] = [m_\alpha \circ m_\beta] = [m_\alpha][m_\beta]$. Therefore

$$\mathrm{Tr}_{L/K}(\alpha+\beta) = \mathrm{Tr}([m_{\alpha+\beta}]) = \mathrm{Tr}([m_\alpha]+[m_\beta]) = \mathrm{Tr}([m_\alpha])+\mathrm{Tr}([m_\beta]) = \mathrm{Tr}_{L/K}(\alpha)+\mathrm{Tr}_{L/K}(\beta)$$

and

$$\mathrm{N}_{L/K}(\alpha\beta) = \det([m_{\alpha\beta}]) = \det([m_\alpha][m_\beta]) = \det([m_\alpha])\det([m_\beta]) = \mathrm{N}_{L/K}(\alpha)\mathrm{N}_{L/K}(\beta).$$

So $\mathrm{Tr}_{L/K}\colon L \to K$ is additive and $\mathrm{N}_{L/K}\colon L \to K$ is multiplicative.

To show $\mathrm{Tr}_{L/K}$ is $K$-linear, not just additive, for $c \in K$ and $\alpha \in L$ we have $m_{c\alpha} = cm_\alpha$ as mappings $L \to L$ (check that), so $[m_{c\alpha}] = [cm_\alpha] = c[m_\alpha]$. Therefore $\mathrm{Tr}_{L/K}(c\alpha) = \mathrm{Tr}_{L/K}(c[m_\alpha]) = c\mathrm{Tr}_{L/K}(\alpha)$.

Since $\mathrm{N}_{L/K}(1) = \det([m_1]) = 1$, for nonzero $\alpha$ in $L$ taking norms of both sides of $\alpha \cdot (1/\alpha) = 1$ implies $\mathrm{N}_{L/K}(\alpha)\mathrm{N}_{L/K}(1/\alpha) = 1$, so $\mathrm{N}_{L/K}(\alpha) \neq 0$. □

The linearity of $\mathrm{Tr}_{L/K}$ means calculating it on all elements is reduced to finding its values on a basis.

**Example 3.3.** Consider the extension $\mathbf{Q}(\gamma)/\mathbf{Q}$ where $\gamma^3 - \gamma - 1 = 0$. For $a, b, c \in \mathbf{Q}$, we saw before that $\mathrm{Tr}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(a + b\gamma + c\gamma^2) = 3a + 2c$ by using the matrix for multiplication by $a + b\gamma + c\gamma^2$ from Example 2.5. Because the trace is $\mathbf{Q}$-linear, we can calculate this trace in another way:

$$\mathrm{Tr}(a + b\gamma + c\gamma^2) = a\mathrm{Tr}(1) + b\mathrm{Tr}(\gamma) + c\mathrm{Tr}(\gamma^2),$$

where $\mathrm{Tr} = \mathrm{Tr}_{\mathbf{Q}(\gamma)/\mathbf{Q}}$. Therefore finding the trace down to $\mathbf{Q}$ of a general element of $\mathbf{Q}(\gamma)$ is reduced to finding the traces of just three numbers: 1, $\gamma$, and $\gamma^2$.

- $\mathrm{Tr}(1) = [\mathbf{Q}(\gamma) : \mathbf{Q}] = 3$.
- To compute $\mathrm{Tr}(\gamma)$ we will compute $[m_\gamma]$ using the basis $\{1, \gamma, \gamma^2\}$: $\gamma \cdot 1 = \gamma$, $\gamma \cdot \gamma = \gamma^2$, and $\gamma \cdot \gamma^2 = \gamma^3 = 1 + \gamma$, so
$$[m_\gamma] = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$
Therefore $\mathrm{Tr}(\gamma) = 0$.
- To compute $\mathrm{Tr}(\gamma^2)$ we want to find the matrix $[m_{\gamma^2}]$, which can be found either directly by multiplying $\gamma^2$ on the basis $\{1, \gamma, \gamma^2\}$ or by squaring the matrix $[m_\gamma]$ just above, since $[m_{\gamma^2}] = [m_\gamma m_\gamma] = [m_\gamma]^2$. Either way,
$$[m_{\gamma^2}] = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \tag{3.1}$$
so $\mathrm{Tr}(\gamma^2) = 2$.

Therefore $\mathrm{Tr}(a+b\gamma+c\gamma^2) = a\mathrm{Tr}(1)+b\mathrm{Tr}(\gamma)+c\mathrm{Tr}(\gamma^2) = 3a+2c$, which agrees with our calculation of this trace earlier.

## 4. Applications of the Trace and Norm

Here are two negative results about $\mathbf{Q}(\sqrt[3]{2})$ that will be settled with the trace and norm.
Task 1: Show $\sqrt[3]{3} \notin \mathbf{Q}(\sqrt[3]{2})$.
Task 2: Show $1+\sqrt[3]{2}$ is not a perfect square in $\mathbf{Q}(\sqrt[3]{2})$.

Solution to Task 1: We argue by contradiction: assume $\sqrt[3]{3} \in \mathbf{Q}(\sqrt[3]{2})$, so

$$\sqrt[3]{3} = a + b\sqrt[3]{2} + c\sqrt[3]{4} \tag{4.1}$$

for some rational $a$, $b$, and $c$. Our goal is to show such an equation is impossible. The *awful* way to do this is to cube both sides to get

$$\begin{aligned} 3 &= (a+b\sqrt[3]{2}+c\sqrt[3]{4})^3 \\ &= (a^3+2b^3+4c^3+12abc) + (3a^2b+6ac^2+6b^2c)\sqrt[3]{2} + (3a^2c+3ab^2+6bc^2)\sqrt[3]{4} \end{aligned}$$

and then set the rational term on the right to be 3 and the coefficients of $\sqrt[3]{2}$ and $\sqrt[3]{4}$ to be 0. This is a system of 3 cubic equations in $a$, $b$, and $c$, and we want to show it has no rational solution. What a mess.

A better approach is to tackle the problem "linearly" using traces.

From the assumption that $\sqrt[3]{3}$ is in the cubic field $\mathbf{Q}(\sqrt[3]{2})$ we have

$$\mathbf{Q}(\sqrt[3]{2}) = \mathbf{Q}(\sqrt[3]{3}).$$

Call this common cubic field $K$. The two primitive elements $\sqrt[3]{2}$ and $\sqrt[3]{3}$ for $K/\mathbf{Q}$ suggest different bases over $\mathbf{Q}$: $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ and $\{1, \sqrt[3]{3}, \sqrt[3]{9}\}$. Using the first basis, the matrix for multiplication by $\sqrt[3]{2}$ is

$$\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

so $\mathrm{Tr}_{K/\mathbf{Q}}(\sqrt[3]{2}) = 0$. In a similar way we get $\mathrm{Tr}_{K/\mathbf{Q}}(\sqrt[3]{3}) = 0$ using the second basis. The matrix for multiplication by $\sqrt[3]{4}$ with respect to the basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ is

$$\begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{pmatrix},$$

so $\mathrm{Tr}_{K/\mathbf{Q}}(\sqrt[3]{4}) = 0$. Applying $\mathrm{Tr}_{K/\mathbf{Q}}$ to both sides of (4.1), we get

$$0 = a\mathrm{Tr}_{K/\mathbf{Q}}(1) + b\mathrm{Tr}_{K/\mathbf{Q}}(\sqrt[3]{2}) + c\mathrm{Tr}_{K/\mathbf{Q}}(\sqrt[3]{4}) = 3a,$$

so $a = 0$. Now multiply both sides of (4.1) by $\sqrt[3]{2}$:

$$\sqrt[3]{6} = a\sqrt[3]{2} + b\sqrt[3]{4} + 2c. \tag{4.2}$$

The number $\sqrt[3]{6}$ has degree 3 over $\mathbf{Q}$, so it has to be a primitive element of $K$, and using the basis $\{1, \sqrt[3]{6}, \sqrt[3]{36}\}$ for $K/\mathbf{Q}$ gives us $\mathrm{Tr}_{K/\mathbf{Q}}(\sqrt[3]{6}) = 0$. Therefore if we apply $\mathrm{Tr}_{K/\mathbf{Q}}$ to both sides of (4.2) we get $0 = 6c$, so $c = 0$.

Returning to (4.1), it now reads $\sqrt[3]{3} = b\sqrt[3]{2}$, so $3/2 = b^3$, which clearly has no rational solution. We have a contradiction, so $\sqrt[3]{3} \notin \mathbf{Q}(\sqrt[3]{2})$.

Solution to Task 2: If $1+\sqrt[3]{2} = \alpha^2$ for $\alpha$ in $K = \mathbf{Q}(\sqrt[3]{2})$, then $\mathrm{N}_{K/\mathbf{Q}}(1+\sqrt[3]{2}) = (\mathrm{N}_{K/\mathbf{Q}}(\alpha))^2$ in $\mathbf{Q}$. To compute $\mathrm{N}_{K/\mathbf{Q}}(1+\sqrt[3]{2})$, use the basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ for $K/\mathbf{Q}$: the matrix for multiplication by $1+\sqrt[3]{2}$ is

$$\begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix},$$

whose determinant is 3, so $\mathrm{N}_{K/\mathbf{Q}}(1+\sqrt[3]{2}) = 3$. Therefore $3 = (\mathrm{N}_{K/\mathbf{Q}}(\alpha))^2$ in $\mathbf{Q}$, but this is impossible because $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ would be a rational square root of 3.

While this idea suffices to prove a number in a field is not a square (or other power) by showing its norm down to a subfield we know better is not a square there, if the norm turns out to be a square in the smaller field that does *not* usually mean the original number is a square in the larger field.

Another application of the trace and norm is an algebraic analogue of volume for any basis of a field extension.

In $\mathbf{R}^n$, if $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is a basis then the parellelepiped spanned by the $\mathbf{v}_i$'s is the set $\{\sum_{i=1}^n c_i\mathbf{v}_i : 0 \leq c_i \leq 1\}$ and its volume in $\mathbf{R}^n$ is $\sqrt{|\det(\mathbf{v}_i \cdot \mathbf{v}_j)|}$, so its squared volume is $|\det(\mathbf{v}_i \cdot \mathbf{v}_j)|$. The trace product $\mathrm{Tr}_{L/K}(\alpha\beta)$ for $\alpha$ and $\beta$ in $L$ is the right analogue of the dot product $\mathbf{v} \cdot \mathbf{w}$ for $\mathbf{v}$ and $\mathbf{w}$ in $\mathbf{R}^n$, so if we drop the absolute value (which makes no sense in general fields) and replace the dot product with the trace product, then we are led to consider the determinant $\det(\mathrm{Tr}_{L/K}(e_ie_j)) \in K$ for any basis $e_1, \ldots, e_n$ of $L/K$ to be something like a "squared volume". This is called the *discriminant* of the basis and is denoted $\mathrm{disc}_{L/K}(e_1, \ldots, e_n)$. The next example explains the name.

**Example 4.1.** Let $[L : K] = 2$ and pick $\alpha \in L - K$, so $L = K(\alpha)$. Let the minimal polynomial of $\alpha$ over $K$ be $X^2 + bX + c$. Then $\mathrm{Tr}_{L/K}(1) = 2$, $\mathrm{Tr}_{L/K}(\alpha) = -b$, and $\mathrm{Tr}_{L/K}(\alpha^2) = \mathrm{Tr}_{L/K}(-b\alpha - c) = b^2 - 2c$. Therefore $\mathrm{disc}_{L/K}(1, \alpha)$ equals

$$\det \begin{pmatrix} \mathrm{Tr}_{L/K}(1 \cdot 1) & \mathrm{Tr}_{L/K}(1 \cdot \alpha) \\ \mathrm{Tr}_{L/K}(\alpha \cdot 1) & \mathrm{Tr}_{L/K}(\alpha \cdot \alpha) \end{pmatrix} = \det \begin{pmatrix} 2 & -b \\ -b & b^2 - 2c \end{pmatrix} = 2b^2 - 4c - b^2 = b^2 - 4c,$$

which is the familiar discriminant of $X^2 + bX + c$.

When $L = K(\alpha)$, there are two formulas for the discriminant of the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ of $K(\alpha)/K$ in terms of the minimal polynomial $f(X)$ for $\alpha$ over $K$, which we state here without proof:[2]

- If $f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$ over a splitting field, then
$$\mathrm{disc}_{K(\alpha)/K}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{i<j} (\alpha_j - \alpha_i)^2.$$
- The discriminant is the norm of a derivative, up to a sign:
$$\mathrm{disc}_{K(\alpha)/K}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2}\mathrm{N}_{K(\alpha)/K}(f'(\alpha)).$$

**Example 4.2.** In the notation of Example 4.1, $f(X) = X^2 + bX + c$. Factoring $f(X)$ over a splitting field as $(X - \alpha_1)(X - \alpha_2)$, we have $\alpha_1 + \alpha_2 = -b$ and $\alpha_1\alpha_2 = c$ by equating coefficients, so $(\alpha_2 - \alpha_1)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = b^2 - 4c$.

[2]Proofs are given in the second handout on trace and norm.

Alternatively, $(-1)^{n(n-1)/2}\mathrm{N}_{K(\alpha)/K}(f'(\alpha)) = -\mathrm{N}_{K(\alpha)/K}(2\alpha+b)$. The matrix for multiplication by $2\alpha+b$ in the basis $\{1,\alpha\}$ is $\left(\begin{smallmatrix} b & -2c \\ 2 & -b \end{smallmatrix}\right)$, whose determinant is $-b^2+4c$, so $-\mathrm{N}_{K(\alpha)/K}(2\alpha+b) = b^2-4c$.

## 5. The Trace and Norm in terms of Roots

The numbers $\mathrm{Tr}_{L/K}(\alpha)$ and $\mathrm{N}_{L/K}(\alpha)$ can be expressed in terms of the coefficients or the roots of the minimal polynomial of $\alpha$ over $K$. To explain this we need another polynomial in $K[X]$ related to $\alpha$ besides its minimal polynomial over $K$, inspired by more linear algebra.

**Definition 5.1.** For $\alpha \in L$, its *characteristic polynomial* relative to the extension $L/K$ is the characteristic polynomial of a matrix representation $[m_\alpha]$:

$$\chi_{\alpha,L/K}(X) = \det(X \cdot I_n - [m_\alpha]) \in K[X],$$

where $n = [L:K]$.

Note that we are defining the characteristic polynomial of a matrix $A$ to be $\det(XI_n - A)$, not $\det(A - XI_n)$. This is because we like our polynomials to be monic; if we used the second way then the leading coefficient would be $(-1)^n$.

**Example 5.2.** For the extension $\mathbf{C}/\mathbf{R}$, the characteristic polynomial of the matrix in Example 2.2 is $\chi_{a+bi,\mathbf{C}/\mathbf{R}}(X) = X^2 - 2aX + a^2 + b^2$.

**Example 5.3.** For the extension $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$, the characteristic polynomial of the matrix in Example 2.3 is $\chi_{a+b\sqrt{2},\mathbf{Q}(\sqrt{2})/\mathbf{Q}}(X) = X^2 - 2aX + a^2 - 2b^2$.

**Example 5.4.** For the extension $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$, from Example 2.4 $\chi_{a+b\sqrt[3]{2}+c\sqrt[3]{4},\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}}(X) = X^3 - 3aX^2 + (3a^2-6bc)X - (a^3+2b^3+4c^3-6abc)$.

**Example 5.5.** For $c \in K$, $m_c\colon L \to L$ has matrix representation $cI_n$, so $\chi_{c,L/K}(X) = \det(XI_n - cI_n) = (X-c)^n = X^n - ncX^{n-1} + \cdots + (-1)^n c^n$.

For any $n \times n$ square matrix $A$, its trace and determinant appear up to sign as coefficients in its characteristic polynomial:

$$\det(XI_n - A) = X^n - \mathrm{Tr}(A)X^{n-1} + \cdots + (-1)^n \det A,$$

so

$$\chi_{\alpha,L/K}(X) = X^n - \mathrm{Tr}_{L/K}(\alpha)X^{n-1} + \cdots + (-1)^n \mathrm{N}_{L/K}(\alpha). \tag{5.1}$$

This tells us the trace and norm of $\alpha$ are, up to sign, coefficients of the characteristic polynomial of $\alpha$, which can be seen in the above examples. Unlike the minimal polynomial of $\alpha$ over $K$, whose degree $[K(\alpha):K]$ varies with $K$, the degree of $\chi_{\alpha,L/K}(X)$ is always $n$, which is independent of the choice of $\alpha$ in $L$.

**Theorem 5.6.** *Every $\alpha$ in $L$ is a root of its characteristic polynomial $\chi_{\alpha,L/K}(X)$.*

*Proof.* This will be a consequence of the Cayley-Hamilton theorem in linear algebra, which says any linear operator is killed by its characteristic polynomial: if a square matrix $A$ has characteristic polynomial $\chi(X) = \det(XI_n - A) \in K[X]$, then $\chi(A) = O$.

For any polynomial $f(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$ in $K[X]$,

$$\begin{aligned} f([m_\alpha]) &= [m_\alpha]^n + c_{n-1}[m_\alpha]^{n-1} + \cdots + c_1[m_\alpha] + c_0 I_n \\ &= [m_{\alpha^n}] + c_{n-1}[m_{\alpha^{n-1}}] + \cdots + c_1[m_\alpha] + c_0[m_1] \quad \text{since } [m_x][m_y] = [m_{xy}] \\ &= [m_{\alpha^n}] + [m_{c_{n-1}\alpha^{n-1}}] + \cdots + [m_{c_1\alpha}] + [m_{c_0}] \quad \text{since } c[m_x] = [m_{cx}] \\ &= [m_{\alpha^n} + m_{c_{n-1}\alpha^{n-1}} + \cdots + m_{c_1\alpha} + m_{c_0}] \quad \text{since } [m_x] + [m_y] = [m_x + m_y] \\ &= [m_{\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0}] \quad \text{since } m_x + m_y = m_{x+y} \\ &= [m_{f(\alpha)}]. \end{aligned}$$

In words, the value $f(X)$ at a matrix for multiplication by $\alpha$ on $L$ is a matrix for multiplication by $f(\alpha)$ on $L$. Taking for $f(X)$ the polynomial $\chi_{\alpha,L/K}(X)$, we have $\chi_{\alpha,L/K}([m_\alpha]) = O$ by Cayley–Hamilton, so $[m_{\chi_{\alpha,L/K}(\alpha)}] = O$. The only $\beta$ in $L$ such that $[m_\beta] = O$ is 0, so $\chi_{\alpha,L/K}(\alpha) = 0$. □

**Example 5.7.** The complex number $a+bi$ is a root of $\chi_{a+bi,\mathbf{C}/\mathbf{R}}(X) = X^2 - 2aX + a^2 + b^2$, which can be seen by direct substitution of $a + bi$ into this polynomial.

**Example 5.8.** Let $\gamma^3 - \gamma - 1 = 0$ over $\mathbf{Q}$. Since $[\mathbf{Q}(\gamma) : \mathbf{Q}] = 3$ and $\gamma^2$ is irrational (otherwise $\gamma$ can't have degree 3 over $\mathbf{Q}$), $\mathbf{Q}(\gamma^2) = \mathbf{Q}(\gamma)$, so $\gamma^2$ has a minimal polynomial of degree 3 over $\mathbf{Q}$. What is that minimal polynomial? A tedious way to find it is to solve

$$(\gamma^2)^3 + a(\gamma^2)^2 + b\gamma^2 + c = 0$$

for unknown rational coefficients $a, b, c$ by expressing $\gamma^6$ and $\gamma^4$ as $\mathbf{Q}$-linear combinations of $1, \gamma, \gamma^2$ to get a system of 3 linear equations in the three unknowns $a, b, c$, and solve for $a, b, c$. Ugh. A more direct method is to calculate the characteristic polynomial of $[m_{\gamma^2}]$ in (3.1), which is $X^3 - 2X^2 + X - 1$ (check!). This has $\gamma^2$ as a root by Theorem 5.6 and it has the right degree, so $X^3 - 2X^2 + X - 1$ is the minimal polynomial of $\gamma^2$ over $\mathbf{Q}$. Isn't that nice?

If $L = K(\alpha)$, then $\chi_{\alpha,L/K}(X)$ is the minimal polynomial of $\alpha$ over $K$ since this polynomial is monic in $K[X]$, has $\alpha$ as a root, and its degree is $[L : K] = [K(\alpha) : K]$. If $\alpha$ doesn't generate $L$ over $K$ then $\chi_{\alpha,L/K}(X)$ is not the minimal polynomial of $\alpha$ in $K[X]$ since the degree of $\chi_{\alpha,L/K}(X)$ is $n = [L : K]$, which is too big. However, the characteristic polynomial tells us the minimal polynomial in principle, since it is a power of the minimal polynomial.

**Theorem 5.9.** *For $\alpha \in L$, let $\pi_{\alpha,K}(X)$ be the minimal polynomial of $\alpha$ in $K[X]$. If $L = K(\alpha)$ then $\chi_{\alpha,L/K}(\alpha) = \pi_{\alpha,K}(X)$. More generally, $\chi_{\alpha,L/K}(X) = \pi_{\alpha,K}(X)^{n/d}$ where $d = \deg \pi_{\alpha,K}(X) = [K(\alpha) : K]$.*

In words, $\chi_{\alpha,L/K}(X)$ is the power of the minimal polynomial of $\alpha$ over $K$ that has degree $n$. For example, if $c \in K$ its minimal polynomial in $K[X]$ is $X - c$ while its characteristic polynomial for $L/K$ is $(X - c)^n$.

*Proof.* A $K$-basis of $K(\alpha)$ is $\{1, \alpha, \ldots, \alpha^{d-1}\}$. Let $m = [L : K(\alpha)]$ and $\beta_1, \ldots, \beta_m$ be a $K(\alpha)$-basis of $L$. Then a $K$-basis of $L$ is

$$\{\beta_1, \alpha\beta_1, \ldots, \alpha^{d-1}\beta_1, \ldots, \beta_m, \alpha\beta_m, \ldots, \alpha^{d-1}\beta_m\}.$$

Let $\alpha \cdot \alpha^j = \sum_{i=0}^{d-1} c_{ij}\alpha^i$ for $0 \le j \le d-1$, where $c_{ij} \in K$. The matrix for multiplication by $\alpha$ on $K(\alpha)$ with respect to $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is $(c_{ij})$, so $\chi_{\alpha,K(\alpha)/K}(X) = \det(X \cdot I_d - (c_{ij}))$. This polynomial has $\alpha$ as a root by Theorem 5.6 (using $K(\alpha)$ in place of $L$) and it has degree $d$.

Therefore $\det(X \cdot I_d - (c_{ij})) = \pi_{\alpha,K}(X)$ because $\pi_{\alpha,K}(X)$ is the only monic polynomial in $K[X]$ of degree $d = [K(\alpha) : K]$ with $\alpha$ as a root.

Since $\alpha \cdot \alpha^j\beta_k = \sum_{i=0}^{d-1} c_{ij}\alpha^i\beta_k$, with respect to the above $K$-basis of $L$ the matrix for $m_\alpha$ is a block diagonal matrix with $m$ repeated $d \times d$ diagonal blocks $(c_{ij})$, so $\chi_{\alpha,L/K}(X) = \det(X \cdot I_d - (c_{ij}))^m = \pi_{\alpha,K}(X)^m = \pi_{\alpha,K}(X)^{n/d}$.

If $L = K(\alpha)$ then $n/d = 1$, so the characteristic and minimal polynomials of $\alpha$ coincide. □

**Corollary 5.10.** *Let the minimal polynomial for $\alpha$ over $K$ be $X^d + c_{d-1}X^{d-1} + \cdots + c_1X + c_0$. Then*

$$\mathrm{Tr}_{K(\alpha)/K}(\alpha) = -c_{d-1}, \quad \mathrm{N}_{K(\alpha)/K}(\alpha) = (-1)^d c_0,$$

*and more generally*

$$\mathrm{Tr}_{L/K}(\alpha) = -\frac{n}{d}c_{d-1}, \quad \mathrm{N}_{L/K}(\alpha) = (-1)^n c_0^{n/d}.$$

*Proof.* We will prove the general formula at the end. The special case $L = K(\alpha)$ then arises from setting $n = d$.

Write $\pi_{\alpha,K}(X)$ for the minimal polynomial of $\alpha$ over $K$. By Theorem 5.9,

$$\begin{aligned} \chi_{\alpha,L/K}(X) &= \pi_{\alpha,K}(X)^{n/d} \\ &= (X^d + c_{d-1}X^{d-1} + \cdots + c_1X + c_0)^{n/d} \\ &= X^n + \frac{n}{d}c_{d-1}X^{n-1} + \cdots + c_0^{n/d}. \end{aligned}$$

From this formula and (5.1), $\mathrm{Tr}_{L/K}(\alpha) = -\frac{n}{d}c_{d-1}$ and $\mathrm{N}_{L/K}(\alpha) = (-1)^n c_0^{n/d}$. □

**Example 5.11.** If $\gamma$ is a root of $X^3 - X - 1$, then

$$\mathrm{Tr}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(\gamma) = 0, \quad \mathrm{N}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(\gamma) = 1.$$

**Example 5.12.** If $\gamma$ is a root of $X^4 - X - 1$, then

$$\mathrm{Tr}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(\gamma) = 0, \quad \mathrm{N}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(\gamma) = -1.$$

**Example 5.13.** If $\gamma$ is a root of $X^5 + 6X^4 + X^3 + 5$ (which is irreducible over $\mathbf{Q}$, since it's irreducible mod 2), then

$$\mathrm{Tr}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(\gamma) = -6, \quad \mathrm{N}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(\gamma) = -5.$$

In the notation of Corollary 5.10, $n/d$ equals $[L : K(\alpha)]$, so we can rewrite the formulas for $\mathrm{Tr}_{L/K}(\alpha)$ and $\mathrm{N}_{L/K}(\alpha)$ at the end of Corollary 5.10 in terms of $\mathrm{Tr}_{K(\alpha)/K}(\alpha)$ and $\mathrm{N}_{K(\alpha)/K}(\alpha)$, as follows:

$$\mathrm{Tr}_{L/K}(\alpha) = [L : K(\alpha)]\mathrm{Tr}_{K(\alpha)/K}(\alpha), \quad \mathrm{N}_{L/K}(\alpha) = \mathrm{N}_{K(\alpha)/K}(\alpha)^{[L:K(\alpha)]}. \tag{5.2}$$

**Example 5.14.** If $\gamma$ is a root of $X^3 + X^2 + 7X + 2$, which is irreducible over $\mathbf{Q}$, then

$$\mathrm{Tr}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(\gamma) = -1, \quad \mathrm{N}_{\mathbf{Q}(\gamma)/\mathbf{Q}}(\gamma) = -2.$$

If $L$ is an extension of $\mathbf{Q}$ containing $\gamma$ such that $[L : \mathbf{Q}] = 12$, then we make a field diagram

$$\begin{array}{c} L \\ | \\ {\scriptstyle 4} \\ | \\ \mathbf{Q}(\gamma) \\ | \\ {\scriptstyle 3} \\ | \\ \mathbf{Q} \end{array}$$

and see that

$$\mathrm{Tr}_{L/\mathbf{Q}}(\gamma) = 4(-1) = -4, \quad \mathrm{N}_{L/\mathbf{Q}}(\gamma) = (-2)^4 = 16.$$

**Corollary 5.15.** *Let the minimal polynomial for $\alpha$ over $K$ split completely over a large enough field extension of $K$ as $(X - \alpha_1) \cdots (X - \alpha_d)$ Then*

$$\mathrm{Tr}_{K(\alpha)/K}(\alpha) = \alpha_1 + \cdots + \alpha_d, \quad \mathrm{N}_{K(\alpha)/K}(\alpha) = \alpha_1 \cdots \alpha_d,$$

*and more generally*

$$\mathrm{Tr}_{L/K}(\alpha) = \frac{n}{d}(\alpha_1 + \cdots + \alpha_d), \quad \mathrm{N}_{L/K}(\alpha) = (\alpha_1 \cdots \alpha_d)^{n/d},$$

*where $[L : K] = n$ and $d = [K(\alpha) : K]$.*

*Proof.* The factorization of the minimal polynomial $X^d + c_{d-1}X^{d-1} + \cdots + c_1X + c_0$ into linear factors implies $c_{d-1} = -\sum_{i=1}^d \alpha_i$ and $c_0 = (-1)^d \prod_{i=1}^d \alpha_i$. Substituting these into the formulas from Corollary 5.10 expresses the trace and norm of $\alpha$ in terms of the roots of the minimal polynomial. □

The roots $\alpha_1, \ldots, \alpha_d$ of the minimal polynomial of $\alpha$ over $K$ do not have to be in $L$ for the trace and norm formulas in Corollary 5.15 to work: those formulas use numbers that may be outside of $L$. When $L \neq K(\alpha)$, the formulas say that the $\alpha_i$'s have to be repeated $n/d$ times in the sum and product, which makes a total of $n$ terms in the sum and product. This is already evident in the special case of elements in $K$: for $c \in K$, $\mathrm{Tr}_{L/K}(c) = nc$ and $\mathrm{N}_{L/K}(c) = c^n$.

**Example 5.16.** If $c \in K$ then $\chi_{\alpha+c,L/K}(X) = \chi_{\alpha,L/K}(X - c)$ from the definition of the characteristic polynomial. Since $\mathrm{N}_{L/K}(\alpha) = (-1)^n \chi_{\alpha,L/K}(0)$, replacing $\alpha$ with $\alpha + c$ tells us that $\mathrm{N}_{L/K}(\alpha + c) = (-1)^n \chi_{\alpha,L/K}(-c)$. If we use $-c$ in place of $c$, then

$$\mathrm{N}_{L/K}(\alpha - c) = (-1)^n \chi_{\alpha,L/K}(c).$$

For instance, in $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ the number $\sqrt[3]{2}$ has characteristic polynomial $X^3 - 2$, so the characteristic polynomial of $c + \sqrt[3]{2}$ for $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$, where $c \in \mathbf{Q}$, is $(X - c)^3 - 2$. Thus

$$\mathrm{N}_{\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}}(c + \sqrt[3]{2}) = -((-c)^3 - 2) = c^3 + 2.$$

The norm is *not* $c^3 - 2$. And this is only for $c \in \mathbf{Q}$. To find $\mathrm{N}_{\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}}(1 + \sqrt[3]{4} + \sqrt[3]{2})$ you can't use the above formula with $c = 1 + \sqrt[3]{4}$: the number wouldn't even be rational.

## References

[1] S. Lang, "Algebra," 3rd ed., Addison-Wesley, New York, 1993.