1. Let A be a ring (i.e., a commutative ring) which is a domain and has finitely many elements. In this problem we will show that A is a field. Let $a \in A$, $a \neq 0$ be an element.

(a) Consider the map $\varphi_a \colon A \longrightarrow A$ given by multiplying by a (i.e, $\varphi_a(b) = ab$ for all $b \in A$), and show that this map is injective.

(b) Since A is finite, explain why φ_a must also be surjective.

(c) Explain why there must be an element $b \in A$ such that $ab = 1$.

(d) Explain why A is a field.

Solution.

(a) Suppose that $b_1, b_2 \in A$ and that $\varphi_a(b_1) = \varphi_a(b_2)$, i.e, that $ab_1 = ab_2$. Subtracting, this is the same as $a(b_1 - b_2) = 0$. Since A is a domain, and $a \neq 0$, this implies that $b_1 - b_2 = 0$, or that $b_1 = b_2$. Therefore φ_a is injective.

(b) Since φ is injective, $|\operatorname{Im}(\varphi_a)| = |A|$ (i.e., the size of the image of φ_a is the size of A). Together with the facts that $\operatorname{Im}(\varphi_a) \subseteq A$ and that $|A|$ is finite, we conclude that $\operatorname{Im}(\varphi_a) = A$, i.e., that φ_a is surjective.

(c) Since $1 \in A$, and φ_a is surjective, there must be some $b \in A$ such that $\varphi_a(b) = 1$. By definition $\varphi_a(b) = ab$, so we have found a b such that $ab = 1$.

(d) By parts (a)–(c), for any $a \in A$, $a \neq 0$, there exists $b \in A$ such that $ab = 1$. Since A is a (commutative) ring in which every nonzero element has a multiplicative inverse, A is a field.

2. Let $K \subseteq L$ be fields, and S_1 and S_2 two subsets of L. If we adjoin S_1 to K we get the field $K(S_1)$, and we could then adjoin S_2 to get the field $(K(S_1))(S_2)$. Show that this field is the same as $K(S_1 \cup S_2)$, obtained by adjoining the union of S_1 and S_2.

Suggestion: Use the defining properties of "field obtained by adjoining elements" to show that each of the fields is contained in the other.

Solution. The field $(K(S_1))(S_2)$ is a field which contains K, S_1 and S_2, and therefore also contains $S_1 \cup S_2$. By the defining property of $K(S_1 \cup S_2)$, this means that $K(S_1 \cup S_2) \subseteq (K(S_1))(S_2)$.

On the other hand, $K(S_1 \cup S_2)$ contains K and S_1, so by the defining property of $K(S_1)$ we have the containment $K(S_1) \subseteq K(S_1 \cup S_2)$. Since $K(S_1 \cup S_2)$ contains $K(S_1)$ and

S_2, by the defining property of $(K(S_1))(S_2)$ we have the containment $(K(S_1))(S_2) \subseteq K(S_1 \cup S_2)$.

Thus $(K(S_1))(S_2) = K(S_1 \cup S_2)$. $\square$

3. Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. (HINT: One inclusion should be obvious, and the other should follow after a little algebra.)

Solution. The field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ contains $\mathbb{Q}$ and contains $\sqrt{2} + \sqrt{3}$, thus we must have $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ by the defining property of $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.

On the other hand, since

$$(\sqrt{2} + \sqrt{3})^3 = \left(\sqrt{2}\right)^3 + 3\left(\sqrt{2}\right)^2 \sqrt{3} + 3\sqrt{2}\left(\sqrt{3}\right)^2 + \left(\sqrt{3}\right)^3 = 11\sqrt{2} + 9\sqrt{3}$$

we see that

$$-\tfrac{9}{2}(\sqrt{2} + \sqrt{3}) + \tfrac{1}{2}(\sqrt{2} + \sqrt{3})^3 = -\tfrac{9}{2}(\sqrt{2} + \sqrt{3}) + \tfrac{1}{2}(11\sqrt{2} + 9\sqrt{3}) = \sqrt{2}$$

and

$$\tfrac{11}{2}(\sqrt{2} + \sqrt{3}) - \tfrac{1}{2}(\sqrt{2} + \sqrt{3})^3 = \tfrac{11}{2}(\sqrt{2} + \sqrt{3}) - \tfrac{1}{2}(11\sqrt{2} + 9\sqrt{3}) = \sqrt{3}.$$

Therefore both $\sqrt{2}$ and $\sqrt{3}$ are in $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. Since $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ also contains $\mathbb{Q}$, the defining property of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ shows us that we have the inclusion $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Combining both inclusions gives $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. $\square$

4. In our argument that $\left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \,\middle|\, a, b, c \in \mathbb{Q}\right\}$ is a field we needed to use the identity

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4}) \cdot \left((a^2 - 2bc) + (2c^2 - ab)\sqrt[3]{2} + (b^2 - ac)\sqrt[3]{4}\right) = a^3 + 2b^3 + 4c^3 - 6abc$$

to "get the cube roots out of the denominator". There is a gap in this argument not addressed in class : if a, b, and c are such that $a + b\sqrt[3]{2} + c\sqrt[3]{4} \neq 0$, how do we know that $a^3 + 2b^3 + 4c^3 - 6abc \neq 0$? (That's something we can't allow in a denominator.)

In this question we will justify that assertion, although we will assume something that we haven't proven yet : that 1, $\sqrt[3]{2}$ and $\sqrt[3]{4}$ are linearly independent over $\mathbb{Q}$. You may assume this for the question.

Let $\gamma = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ be an element of $\mathbb{Q}(\sqrt[3]{2})$, with $a, b, c \in \mathbb{Q}$, and consider the map $\varphi\colon \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q}(\sqrt[3]{2})$ given by multiplication by γ.

(a) Prove that φ is a $\mathbb{Q}$-linear map.

(b) Write out the matrix for this map in the $\mathbb{Q}$-basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.

(c) Compute the determinant of this matrix.

(d) If $\gamma \neq 0$, explain why $a^3 + 2b^3 + 4c^3 - 6abc \neq 0$.

NOTE: We will soon have a different way of showing that the set $\left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \,\middle|\, a, b, c \in \mathbb{Q}\right\}$ is a field, without needing the identity above, and without needing to prove that $a^3 + 2b^3 + 4c^3 - 6abc \neq 0$ whenever $\gamma \neq 0$. The computation is still useful however, and we will come back to the meaning of the determinant later in the course.

Solution.

(a) Let $M = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \,\middle|\, a, b, c \in \mathbb{Q}\right\}$. It is easy to see that M is closed under multiplication (and this was in fact an implicit assumption in the problem). By definition the map φ is $\varphi(\alpha) = \gamma \cdot \alpha$ for any $\alpha \in M$. Let us now check that this map is $\mathbb{Q}$-linear.

For any $\alpha_1, \alpha_2 \in M$ we have $\varphi(\alpha_1+\alpha_2) = \gamma\cdot(\alpha_1+\alpha_2) = \gamma\cdot\alpha_1+\gamma\cdot\alpha_2 = \varphi(\alpha_1)+\varphi(\alpha_2)$. Therefore the map φ is compatible with addition.

For any $\alpha \in M$ and $c \in \mathbb{Q}$ we have $\varphi(c\alpha) = \gamma \cdot (c\alpha) = c(\gamma \cdot \alpha) = c\varphi(\alpha)$, so φ is compatible with multiplication by elements of $\mathbb{Q}$ (or indeed of any subfield of M).

Therefore φ is a $\mathbb{Q}$-linear transformation.

(b) We have :

$$\begin{array}{rcccl} \varphi(1) & = & \gamma \cdot 1 & = & a + b\sqrt[3]{2} + c\sqrt[3]{4}; \\ \varphi(\sqrt[3]{2}) & = & \gamma \cdot \sqrt[3]{2} & = & 2c + a\sqrt[3]{2} + b\sqrt[3]{4}; \text{ and} \\ \varphi(\sqrt[3]{4}) & = & \gamma \cdot \sqrt[3]{4} & = & 2b + 2c\sqrt[3]{2} + a\sqrt[3]{4}. \end{array}$$

Therefore in the $\mathbb{Q}$-basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ the matrix for φ is

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

(c) This matrix has determinant

$$\begin{vmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{vmatrix} = a \cdot a \cdot a + (2c) \cdot (2c) \cdot (2c) + (2b) \cdot b \cdot b - a \cdot (2b) \cdot c - a \cdot b \cdot (2c) - a \cdot b \cdot (2c)$$
$$= a^3 + 2b^3 + 4c^3 - 6abc.$$

(d) The linear transformation φ is a map from the 3-dimensional $\mathbb{Q}$-vector space M to itself. For any nonzero γ the map φ is also an injective linear transformation, i.e., $\text{Ker}(\varphi) = \{0\}$. The reason is that if $\alpha \in M$ and $\varphi(\alpha) = \gamma \cdot \alpha = 0$, then we must have $\alpha = 0$ since we are multiplying in the domain $\mathbb{R}$.

Since φ is an injective linear transformation from a finite-dimensional vector space to itself, it is an invertible linear transformation, and hence its determinant, $a^3 + 2b^3 + 4c^3 - 6abc$ is nonzero.

REMARK: If $\gamma \neq 0$ the argument in (d) shows that φ is injective, and hence surjective since φ is a map from the finite dimensional $\mathbb{Q}$-vector space M to itself. In particular, there must be $\alpha \in M$ so that $\varphi(\alpha) = 1$, or (using the definition of φ) so that $\gamma \cdot \alpha = 1$. Thus, following the argument in Question 1, for every nonzero $\gamma \in M$, there exists $\alpha \in M$ such that $\gamma\alpha = 1$. We already know that M is a commutative ring, and hence M is a field. In other words, we now have a third argument that M is a field.

This argument works more generally:

Lemma : If M is a commutative domain which is a finite dimensional vector space over a field K, such that multiplication is K-linear, then M is a field.

Proof. As above, for any $\gamma \neq 0$ in M, consider the map $\varphi : M \longrightarrow M$ which is multiplication by γ. As above, we deduce that φ is K-linear, that φ is injective [this uses that M is a domain], and therefore that φ is surjective since φ is an injective linear map from a finite-dimensional vector space to itself. Thus there is an $\alpha \in M$ such that $\gamma \cdot \alpha = \varphi(\alpha) = 1$, and so every nonzero element of M has a multiplicative inverse. Thus M is a field. $\square$