**Problem 1.** Let \( M \) be a \( \mathbb{Z} \)-module in which every element is torsion (i.e., for every \( m \in M \) there is a nonzero \( n \in \mathbb{Z} \) such that \( n \cdot m = 0 \)). Show that \( M \otimes \mathbb{Q} = 0 \).

*Solution.* Let \( G \) be an abelian group and let \( B : M \times \mathbb{Q} \to G \) be a bilinear map of \( \mathbb{Z} \)-modules. For \( m, n \) as in the problem, and any \( q \in \mathbb{Q} \), we have \( B(m, q) = B(nm, q/n) = B(0, q/n) = 0 \), so \( B \) is identically zero. Thus the universal property defining the tensor product is satisfied by the trivial module and the zero bilinear map, so \( M \otimes \mathbb{Q} = 0 \).

**Problem 2.** Let \( f(x) = x^8 - 1 \). Find the Galois group of \( f(x) \) over each of the following fields:

(a) The rational field \( \mathbb{Q} \).
(b) The field \( \mathbb{Q}(i) \).
(c) The field \( \mathbb{F}_3 \) of three elements.

*Solution.* (a) The splitting field of \( f(x) \) over \( \mathbb{Q} \) is \( K = \mathbb{Q}(\zeta) \), where \( \zeta \) is a fixed primitive eighth root of unity. Any automorphism of \( K \) maps \( \zeta \) to another primitive eighth root of unity, namely \( \zeta^i \) with \( i \in \{1, 3, 5, 7\} \), and conversely these are roots of the minimal polynomial of \( \zeta \) over \( \mathbb{Q} \) so they are images of \( \zeta \) under \( \text{Gal}(K/\mathbb{Q}) \). Finally, each automorphism \( \zeta \mapsto \zeta^i \) has order 1 or 2, so \( \text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2)^2 \).

(b) The splitting field is again \( K = \mathbb{Q}(\zeta) \), but \( \zeta^2 = \pm i \) so \( K \) contains \( \mathbb{Q}(i) \). Hence \( [K : \mathbb{Q}(i)] = [K : \mathbb{Q}]/[\mathbb{Q}(i) : \mathbb{Q}] = 4/2 = 2 \), so \( \text{Gal}(K/\mathbb{Q}(i)) \cong (\mathbb{Z}/2) \) (and consists of the maps \( \zeta \mapsto \pm \zeta \)).

(c) The eighth roots of unity in the algebraic closure of \( \mathbb{F}_3 \) are precisely the nonzero elements of \( \mathbb{F}_9 \), so the splitting field of \( f \) is \( \mathbb{F}_9 \), and \( \text{Gal}(\mathbb{F}_9/\mathbb{F}_3) \cong (\mathbb{Z}/2) \) (and is generated by the cubing map).

**Problem 3.** Let \( V \) be the vector space \( \mathbb{C}[X]/(X^4 + X^2) \oplus \mathbb{C}[X]/(X^2 + 1) \), and let \( L : V \to V \) be the linear map given by multiplication by \( X \). Find the Jordan canonical form of \( L \).

*Solution.* Decompose \( \mathbb{C}[X]/(X^4 + X^2) \) into \( \mathbb{C}[X]/(X^2) \oplus \mathbb{C}[X]/(X^2 + 1) \), and \( \mathbb{C}[X]/(X^2 + 1) \) into \( \mathbb{C}[X]/(X - i) \oplus \mathbb{C}[X]/(X + i) \), so \( V \) is isomorphic to the \( \mathbb{C}[X] \)-module

\[
\mathbb{C}[X]/(X^2) \oplus \mathbb{C}[X]/(X - i) \oplus \mathbb{C}[X]/(X - i) \oplus \mathbb{C}[X]/(X + i) \oplus \mathbb{C}[X]/(X + i).
\]

The correspondence between \( \mathbb{C}[X] \)-modules and vector spaces with endomorphisms gives the Jordan canonical form

\[
\begin{pmatrix}
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & i & 0 & 0 & 0 \\
0 & 0 & i & 0 & 0 \\
0 & 0 & 0 & -i & 0 \\
0 & 0 & 0 & 0 & -i
\end{pmatrix}.
\]
Problem 4. What are the sizes of the subfields of the field with $2^{12}$ elements?

Solution. For any prime power $q$, and any positive integer $n$, the finite field with $q$ elements has a unique extension of degree $n$, which is the finite field with $q^n$ elements. The subfields of this field therefore have $2^m$ elements, where $mn = 12$ for some positive $n$. So the subfields are those with $2^1$, $2^2$, $2^3$, $2^4$, $2^6$, and $2^{12}$ elements.

Problem 5. Let $R$ be a commutative ring. For each of the following statements, either explain briefly why it is true, or give a counterexample together with an explanation of why it is a counterexample.

(a) If $R$ is a unique factorization domain, then $R$ is a principal ideal domain.
(b) If $R$ is a principal ideal domain, then $R$ is a unique factorization domain.
(c) If $R$ is a Euclidean domain, then $R$ is a unique factorization domain.

Solution. (a) $R = \mathbb{Z}[x]$ is a counterexample: it has unique factorization by Gauss’s lemma (since $\mathbb{Q}[x]$ is Euclidean and hence has unique factorization), but the ideal $(2, x)$ is not principal.

(b) True: for any infinite sequence $a_1, a_2, \ldots$ such that $a_{i+1} | a_i$, the union of the ideals $(a_1) \subset (a_2) \subset \ldots$ is an ideal, and hence a principal ideal $(a)$, but then $a \in (a_n)$ for some $n$, so $a_n | a_k$ for $k > n$. Thus each nonzero $a_1 \in R$ has a factorization, since if $a_1$ is neither irreducible nor a unit then $a_1 = a_2b_2$ where neither $a_2$ nor $b_2$ is a unit, and the above argument shows that after repeating this process finitely many times we will obtain a factorization of $a_1$. Now suppose $a_1$ has two factorizations $p_1 \ldots p_r = q_1 \ldots q_s$, where each $p_i$ and $q_j$ is irreducible. Note that $(p_i)$ is maximal, and hence prime, because if $(p_i) \subset (a)$ then $a \mid p_i$ so $a$ is either a unit or an associate of $p_i$. Since $(p_i)$ contains $q_1 \ldots q_s$, it follows that $p_i \mid q_j$ for some $j$, whence $p_i$ and $q_j$ are associates. Repeating this process shows that the two factorizations of $a_1$ are the same up to unit multiples.

(c) True: Euclideanity implies that any ideal is generated by any of its nonzero elements of minimal norm, so $R$ is a principal ideal domain, and hence a unique factorization domain by (b).
Problem 1. Suppose a finite group $G$ of order $n$ acts on a finite set $X$ of cardinality $m$, Assume that $m$ cannot be written as a sum of divisors of $n$ which are greater than 1. Show that there must be an $x$ in $X$ which is fixed by every $g$ in $G$.

Solution. The set is the disjoint union of the orbits of the action, and the cardinality of the orbit of $x$ is $[G : G_x]$ where $G_x$ is the stabilizer of $x$ in $G$. Since these numbers cannot all be greater than 1, some $x$ in $X$ must satisfy $G_x = G$.

Problem 2. Let $M_n(K)$ be the $K$-algebra of $n$ by $n$ matrices over the field $K$. Construct an isomorphism of $K$-algebras

$$M_m(K) \otimes_K M_n(K) \cong M_{mn}(K).$$

Solution. For any vector spaces $V$ and $W$ over $K$, one has a canonical homomorphism of $K$-algebras

$$\text{End}(V) \otimes_K \text{End}(W) \to \text{End}(V \otimes_K W),$$

taking $L \otimes M$ to the endomorphism that sends $v \otimes w$ to $L(v) \otimes M(w)$, for $v \in V$ and $w \in W$. Identify $M_m(K)$ with $\text{End}(K^m)$ and $M_n(K)$ with $\text{End}(K^n)$. Since $K^m \otimes K K^n$ is isomorphic to $K^{mn}$, we can identify $M_{mn}(K)$ with $\text{End}(K^m \otimes_K K^n)$, which gives the required homomorphism. Using standard bases, one checks that this homomorphism is one-to-one, and therefore an isomorphism, since the two spaces have the same dimension.

Problem 3. Suppose that $K/\mathbb{Q}$ is a (finite) Galois field extension. Prove that for any subfield $L$ of $K$ there exist subfields $L_1, L_2, \ldots, L_r$ of $K$ such that $L = L_1 \cap L_2 \cap \cdots \cap L_r$ and the degree $[K : L_i]$ is a prime power for every $i$.

Solution. Let $H$ be the subgroup of $\text{Gal}(K/\mathbb{Q})$ consisting of elements fixing each element of $L$, so $K/L$ is Galois with group $H$. Let $P_1, \ldots, P_r$ be the Sylow subgroups of $H$, and let $L_i$ be the subfield of $K$ fixed by $P_i$. Then $[K : L_i]$ is a prime power for each $i$, and the intersection $L_1 \cap \cdots \cap L_r$ is the subfield of $K$ fixed by the group $\langle P_1, \ldots, P_r \rangle$ generated by the various $P_i$. This subgroup of $H$ has order of divisible by every prime power divisor of $\#H$, so the subgroup equals $H$ and thus $L_1 \cap \cdots \cap L_r = K^H = L$.

Problem 4. Describe, using Jordan canonical forms, the $4 \times 4$ matrices $M$ over the complex numbers such that $M^4 = M^2$. (Note: you may express your answer in terms of similarity/conjugacy.)

Solution. Any complex matrix $M$ is similar to its Jordan canonical form, and the property $M^4 = M^2$ is preserved under similarity. So suppose $M$ is in Jordan canonical form. Consider a Jordan block of $M$ with diagonal entry $\alpha$. Equating diagonal entries of $M^4$ and $M^2$ shows that $\alpha^4 = \alpha^2$, so $\alpha \in \{0, 1, -1\}$. If the size of the block is at least 2, then equating superdiagonal entries of $M^4$ and $M^2$ shows that $4\alpha^3 = 2\alpha$, so $\alpha = 0$. If the size of the block is at least 3, then equating supersuperdiagonal entries of $M^4$ and $M^2$ shows that $0 = 1$, contradiction. Hence $M$ is similar to a matrix in Jordan canonical form, in which
each Jordan block has diagonal entry 0, 1, or $-1$, and has size at most 2, with size 2 only occurring for diagonal entry 0. These conditions are necessary and sufficient.

**Problem 5.** Let $T : V \to V$ be a linear transformation of a finite-dimensional vector space over a field $K$. Prove that there is a $v$ in $V$ with the property that, for any polynomial $P(X)$ in $K[X]$, $P(T) = 0$ in the endomorphism ring of $V$ if and only if $P(T)(v) = 0$ in $V$.

**Solution.** By the correspondence between endomorphisms of vector spaces and $K[X]$-modules, and the structure theorem for modules over a principal ideal domain, one can write $V$ as a direct sum of $K[X]/(P_1) \oplus \cdots \oplus K[X]/(P_r)$, where each $P_i$ is a monic polynomial, each dividing the next. The image of $X$ in the last factor gives the desired element $v$, since for any $P$, $P(T) = 0$ exactly when it is divisible by $P_r$, which is the condition for $P(T)(v)$ to vanish.