Problem 1. For each positive integer $n$, show that the map $x \mapsto x^4 + x$ is an endomorphism of the additive group of the finite field $\mathbb{F}_{2^n}$, and determine the size of the kernel and image of this endomorphism.

Solution. Since both $x \mapsto x^4$ and $x \mapsto x$ are automorphisms of the field $\mathbb{F}_{2^n}$, indeed $\phi: x \mapsto x^4 + x$ is an endomorphism of the additive group of $\mathbb{F}_{2^n}$. The nonzero elements of the kernel of $\phi$ are the cube roots of unity in $\mathbb{F}_{2^n}$; since the multiplicative group of $\mathbb{F}_{2^n}$ is cyclic of order $2^n - 1$, it contains precisely $\gcd(3, 2^n - 1)$ cube roots of unity. Thus the kernel of $\phi$ has size $\kappa := 1 + \gcd(3, 2^n - 1)$, and the image of $\phi$ has size $2^n/\kappa$. More explicitly, the kernel has size $2$ (resp., $4$) and the image has size $2^{n-1}$ (resp., $2^{n-2}$) if $n$ is odd (resp., $n$ is even).

Problem 2. Let $\phi: \mathbb{Z}^4 \to \mathbb{Z}^4$ be the homomorphism given by the matrix

$$
\begin{pmatrix}
3 & -3 & 9 & 3 \\
3 & 3 & 15 & -3 \\
-6 & 0 & 12 & 0 \\
-3 & 3 & 3 & -3
\end{pmatrix}.
$$

Determine the group structure of the kernel of $\phi$ and the cokernel of $\phi$.

Solution. By elementary row and column operations, the matrix can be brought to the form

$$
\begin{pmatrix}
3 & 0 & 0 & 0 \\
0 & 6 & 0 & 0 \\
0 & 0 & 12 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}.
$$

So the kernel is $\mathbb{Z}$, and the cokernel is $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}$.

Problem 3. If $p$ is a prime number, show that every subgroup of $\text{GL}_2(\mathbb{F}_p)$ of order a power of $p$ is abelian. (Hint: consider the group of upper-triangular matrices with 1’s on the diagonal.)

Solution. Writing $q = p^k$, the order of $G := \text{GL}_2(q)$ is the number of invertible 2-by-2 matrices over $\mathbb{F}_q$, or equivalently the number of 2-by-2 matrices whose rows are linearly independent. The first row can be any of the $q^2 - 1$ nonzero vectors of length 2 over $\mathbb{F}_q$, and the second row can be any of the $q^2 - q$ vectors outside the span of the first row. Thus the order of $G$ is $(q^2 - 1)(q^2 - q)$, so a Sylow $p$-subgroup of $G$ has order $q$. The group $U$ of upper-triangular matrices with 1’s on the diagonal has this order, and is thus a Sylow $p$-subgroup of $G$. Since $U$ is abelian, and every $p$-subgroup of $G$ is conjugate to a subgroup of the Sylow subgroup $U$, it follows that every $p$-subgroup is abelian.

Problem 4. If $A$ is an invertible $n$-by-$n$ matrix over a field $K$, must there be a polynomial $P$ in $K[x]$ such that $P(A) = A^{-1}$?
Solution. Yes. By the Cayley-Hamilton theorem, the characteristic polynomial $Q(x) := \det(xI - A)$ satisfies $Q(A) = 0$. Write $Q(x) = xR(x) + Q(0)$ with $R \in K[x]$. Since $Q(0) = \det(-A) = (-1)^n \det(A)$ is nonzero, it follows that $-AR(A)/Q(0) = I$, so $P(x) := -R(x)/Q(0)$ has the required property.

Problem 5. (a) Describe all maximal ideals in the polynomial ring $\mathbb{Z}[x]$.

(b) Is every nonzero prime ideal maximal?

(c) Is $(3, x^2 + x + 1)$ prime?

Solution. The residue field of any maximal ideal $M$ of $\mathbb{Z}[x]$ is generated by $\mathbb{Z}$ and the image of $x$, and thus cannot contain $\mathbb{Q}$. Hence the residue field is finite, say of characteristic $p$, so $M$ has the form $(p, f)$, where $f$ is monic in $\mathbb{Z}[x]$ and maps to an irreducible polynomial in $\mathbb{F}_p[x]$. Neither ideal $(p)$ nor $(f)$ is maximal, although they are prime. The ideal in (c) is not prime, since $(x - 1)^2$ is in the ideal, but $x - 1$ is not.
Problem 1. Let $L/K$ be a Galois extension with Galois group $S_5$. For how many fields $N$ with $K \subseteq N \subseteq L$ is the extension $L/N$ Galois with cyclic Galois group?

Solution. By the Galois correspondence, the number of such fields $N$ equals the number of cyclic subgroups of $S_5$. The number of $k$-cycles in $S_5$ is 24 if $k = 5$; 30 if $k = 4$; 20 if $k = 3$; and 10 if $k = 2$. Thus the number of groups having a $k$-cycle generator is 6 if $k = 5$; 15 if $k = 4$; 10 if $k = 3$; and 10 if $k = 2$. Finally, any other nontrivial cyclic subgroup of $S_5$ must be generated by either the product of two disjoint 2-cycles or the product of a 2-cycle and a disjoint 3-cycle; there are 15 subgroups of the first form and 10 subgroups of the second form. Hence the number of cyclic subgroups of $S_5$ is $6 + 15 + 10 + 10 + 1 + 15 + 10 = 67$.

Problem 2. Let $V$ be a vector space.

(a) Show that there is a unique linear transformation $T : V \otimes V \otimes V \to V \otimes V \otimes V$ such that $T(u \otimes v \otimes w) = w \otimes u \otimes v$ for all $u, v, w \in V$.

(b) If $V$ has finite dimension $n$, find the minimal and characteristic polynomials of $T$.

Solution. The map $V \times V \times V \to V \otimes V \otimes V$ sending $u \times v \times w$ to $w \otimes u \otimes v$ is multilinear, so determines the required unique mapping. Let $\{e_i : 1 \leq i \leq n\}$ be a basis of $V$. The vector space $W := V \otimes V \otimes V$ has a basis consisting of the elements $f_{ijk} := e_i \otimes e_j \otimes e_k$, where $1 \leq i, j, k \leq n$. Let $W_{ijk}$ be the vector subspace of $W$ spanned by $f_{ijk}$, $f_{kij}$, and $f_{jki}$. Then $W_{ijk}$ has dimension 1 for each of the triples with $i = j = k$, and has dimension 3 for each of the other triples. Thus $W$ is the direct sum of the various $W_{ijk}$ (ignoring repetitions), which consist of $n$ subspaces of dimension 1 and $(n^3 - n)/3$ subspaces of dimension 3. Since each $W_{ijk}$ is invariant under $T$, we have written $W$ as the direct sum of $T$-invariant subspaces, so the characteristic polynomial of $T$ is the product of the characteristic polynomials of the restrictions of $T$ to these subspaces. If $i = j = k$ then $T$ is the identity on $W_{ijk}$, so the characteristic polynomial of $T |_{W_{ijk}}$ is $x - 1$. If at least two of $i, j, k$ are distinct then the matrix for $T |_{W_{ijk}}$ is the permutation matrix of a 3-cycle, so the characteristic polynomial of $T |_{W_{ijk}}$ is $x^3 - 1$. This is also the minimal polynomial of $T |_{W_{ijk}}$: if the characteristic of the ground field is not 3 then this follows from the facts that the minimal polynomial divides the characteristic polynomial, that the two polynomials have the same roots, and that $x^3 - 1$ has distinct roots in the algebraic closure. If the characteristic is 3 then $x^3 - 1 = (x - 1)^3$, so it is enough to note that $(T - 1)^2(f_{ijk}) = f_{jki} - 2f_{kij} + f_{ijk} \neq 0$.

We have shown that the characteristic polynomial of $T$ is $(x - 1)^n(x^3 - 1)^{(n^3 - n)/3}$. Since $T^3 = 1$, we have also shown that the minimal polynomial of $T$ is $x^3 - 1$.

Problem 3. (a) Is the complex number $\frac{2+i}{\sqrt{3}}$ an algebraic number?

(b) Is it integral over $\mathbb{Z}$, in the sense that it satisfies an equation $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$ in which each $a_i$ is in $\mathbb{Z}$? (Hint: you may use the fact that every monic irreducible polynomial in $\mathbb{Z}[x]$ remains irreducible in $\mathbb{Q}[x]$.)

(c) Is it an $n$th root of unity for some $n$?

Solution. We compute $\alpha^2 = \frac{3 + 4i}{5}$ and $(5\alpha^2 - 3)^2 = -16$, so $\alpha$ is a root of $f(x) := x^4 - \frac{6}{5} \alpha^2 + 1$, and hence is algebraic. Since $\alpha$ lies in the field $\mathbb{Q}(i, \sqrt{5})$, but is not rational, its minimal
polynomial over $\mathbb{Q}$ has degree 2 or 4. Since $\alpha^2 = \frac{3+4i}{5}$ is not a $\mathbb{Q}$-linear combination of 1 and $\alpha$, we must have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, so that $f(x)$ is the minimal polynomial of $\alpha$ over $\mathbb{Q}$. If $\alpha$ is a root of a monic polynomial $g(x)$ in $\mathbb{Z}[x]$, then $g(x)$ has a monic irreducible factor $h(x)$ in $\mathbb{Z}[x]$ such that $h(\alpha) = 0$; the hint implies that $h(x)$ is irreducible in $\mathbb{Q}[x]$, so $h(x) = f(x)$ which visibly is not in $\mathbb{Z}[x]$, contradiction. Hence $\alpha$ is not integral, and therefore is not a root of unity.

**Problem 4.** Compute the number of $k$-dimensional subspaces of an $n$-dimensional vector space $V$ over $\mathbb{F}_q$. (Hint: count bases.)

*Solution.* A sequence $v_1, \ldots, v_k$ of vectors in $V$ is linearly independent if and only if no $v_i$ is in the span of $v_1, \ldots, v_{i-1}$; assuming linear independence of $v_1, \ldots, v_{i-1}$, this says there are $q^n - q^{i-1}$ choices for $v_i$. Thus the number of sequences of $k$ linearly independent vectors in $V$ is $A := \prod_{i=1}^{k}(q^n - q^{i-1})$. Any such sequence spans a $k$-dimensional subspace of $V$, and the number of bases of any such subspace is $B := \prod_{i=1}^{k}(q^k - q^{i-1})$. Hence the number in question is $A/B = \prod_{i=0}^{k-1}(q^{n-i} - 1)/(q^{k-i} - 1)$.

**Problem 5.** Find the least positive integer $n$ such that: for every pair of groups $H \subset G$ which satisfy $[G : H] = 7$, there is a normal subgroup $N$ of $G$ such that $N \subseteq H$ and $[H : N] \leq n$.

*Solution.* The group $G$ acts by left multiplication on the set $S$ of left cosets of $H$ in $G$. Thus the kernel $N$ of this action is a normal subgroup of $G$ such that $N \subseteq H$. Since $\#S \leq 7$, we have $[G : N] \leq 7!$ so $[H : N] \leq 6! = 720$. To see that 720 is the least $n$ with the required property, consider the subgroup $H = S_6$ of the group $G = S_7$, and note that $N$ must be the trivial group since neither of the other normal subgroups of $S_7$ (namely, $S_7$ and $A_7$) is contained in $H$. 