2002-I-3 Let $K = \mathbb{Q}(\cos(2\pi/11)$. Find the degree of $K/\mathbb{Q}$ and $\mathrm{Gal}(K/\mathbb{Q})$. Is it a Galois extension?

2002-II-3 Let $A$ denote a finite abelian group of order $3^{20}$. For each integer $k = 1, 2, 3, \ldots$, let $A(k)$ denote the set of all $x \in A$ such that order$(x)$ is a divisor of $3^k$.

(a) Show that each $A(k)$ is a subgroup of $A$ and that $A(k-1)$ is contained in $A(k)$ for all $k$.

(b) Why is each quotient group $A(k)/A(k-1)$ a vector space over the field with 3 elements in $\mathbb{Z}_3$?

(c) Suppose that $\dim A(5)/A(4) = 0$, $\dim(A(4)/A(3)) = \dim(A(3)/A(2)) = 2$, and $\dim(A(2)/A(1)) = 7$. (here dimension means as a vector space over the field with 3 elements $\mathbb{Z}_3$. Express $A$ as a direct sum of cyclic groups; write down generators for the summands in terms of bases for the various quotients $A(k)/A(k-1)$.

2003-I-5 Let $f(x) = x^5 - 2$. Find generators and relations for the Galois group $G := \mathrm{Gal}(F/\mathbb{Q})$ of the splitting field $F$ of $f(x)$ over the rational numbers $\mathbb{Q}$.

2003-I-6 (a) Prove that a group of order $p^2$, $p$ a prime number, is abelian.

(b) Classify groups of order $p^2$ up to isomorphism.

2003-II-4 Let $A$ be an $n$-dimensional commutative, associative algebra with unit over the field of complex numbers $\mathbb{C}$. let $\dim_{\mathbb{C}} A \geq 2$. Prove that $A$ has zero-divisors.

2004-I-4 Determine up to isomorphism all finite groups which have a unique maximal proper subgroup.

2004-II-2 Let $F$ be a field of characteristic 3, and consider the field of rational functions $F(x)$. Set

$$E = \{f \in F(x) \mid f(x) = f(2x+1)\}.$$

Show that $F(x)$ is a Galois extension of $E$, and determine its Galois group.

2004-II-5 Let $A$ denote an integral domain and let $A[x]$ denote the polynomial ring over $A$. Show that the group of $A$-algebra automorphisms of $A[x]$ is isomorphic to the subgroup of $GL(2, A)$ consisting of all $2 \times 2$ matrices over $A$ of the form

$$a, 0$$

$$b, 1$$

where $a$ is an invertible element of $A$ and $b$ is an arbitrary element of $A$.

2005-I-3 Let $R = \mathbb{C}[x, y]/(x^2 - y^3)$.

(a) Describe the field of fractions $F$ of $R$.

(b) An element $\alpha \in F$ is called *integer* over $R$ if $\alpha$ is a root of polynomial

$$\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0, \qquad a_i \in R.$$

Show that the set of all integers in $F$ coincides with $\mathbb{C}[x/y]$.

2005-I-4 Find the Galois group of the polynomial $p(x) = x^3 - 3x + 1$ over $\mathbb{Q}$.

2005-II-3 (a) Show that the alternating group $A_n$ is generated by all cycles of length 3, where we assume that $n \geq 3$

(b) Show that the alernating group is actually generated by the cycles

$$(1, 2, 3)(1, 2, 4), \ldots, (1, 2, n).$$

(c) What is the highest order of a permutation in $A_8$? How many conjugacy classes are there consisting of permutations of this order, and how many elements are there in each conjugacy class?

2006-I-1 Find (up to an isomorphism) all finite groups which have precisely three conjugacy classes.

2006-II-3 Let $K$ be a field of characteristic $p$, and $f(x) = x^p - x - a$, where $a \in K$.

(a) Show that if $f$ has a root in $K$, then it decomposes into the product of linear factors in $K$.

(b) Show that $f$ is either irreducible in $K$, or it decomposes into the product of linear factors in $K$.

2007-I-1 Consider the set $\mathbb{Q}$ of rational numbers as a group with respect to addition. Prove that there is no proper subgroup $G \subset \mathbb{Q}$ of finite index.

2007-II-4 Let $G$ be a finite group and let $H$ be a subgroup of index $n > 1$. Use the multiplicative action of $G$ on $G/H$ to show that $G$ has a normal subgroup $N \subset H$ whose index $[G : N]$ divides $n!$. If the order of $G$ does not divide $n!$, conclude that $G$ is not a simple group.

2008-II-2 Let $\mathbb{F}$ denote the splitting field over the rational numbers $\mathbb{Q}$ for the polynomial $p(x) = x^4 + 2x^3 + 2x + 1$. Show that $4 \leq [\mathbb{F} : \mathbb{Q}] \leq 8$. (**Hint:** Note that if $p(\alpha) = 0$ for $\alpha \in \mathbb{F}$ then $p(\alpha^{-1}) = 0$ also.)

2008-II-6 Let $F$ denote a field; $F[x]$ denotes the ring of polynomials over $F$ in one variable $x$; $R$ denotes the ring of rational functions $\{\frac{f}{g} \mid f, g \in F[x], g \neq 0\}$ over $F$. For $a \in K$ an element in the algebraic closure $K$ for $F$, set $R_a = \{\frac{f}{g} \in \mathbb{R} \mid g(a) \neq 0\}$.

Show that $R_a$ is a principal ideal domain and describe all the ideals of $R_a$.

2009-I-5 Let $G$ be a group of order 63. Prove that $G$ is not simple (i.e., that $G$ contains a non-trivial normal subgroup).

2009-I-6 Let $\mathbb{C}$ be the complex numbers, let $\mathbb{C}[x, y]$ be the ring of polynomials in 2 variables with coefficients in $\mathbb{C}$, let $I$ be the ideal generated by $y^2 - x^3$ and let $R$ be the quotient ring $R = \mathbb{C}[x, y]/I$.

(a) Prove the $R$ is an integral domain.

(b) Prove that $R$ is not a unique factorization domain.
(Hint: recall the proof by contradiction that $\sqrt{2}$ is irrational.

2009-II-5 Let $R$ be a ring and let $A$ be an $R$-module. A free resolution of $A$ over $R$ is an infinite exact sequence of $R$-modules

$$\cdots \xrightarrow{d_3} F_3 \xrightarrow{d_2} F_2 \xrightarrow{d_1} F_1 \xrightarrow{d_0} A \to 0$$

where each $F_i$ is a free $R$-module. (Exact means that the image of each map is the kernel of the next map).

Prove that any $R$-module $A$ has a free resolution.