A lot of algebra prelims

D. Zack Garza

Tuesday 12$^{\text{th}}$ May, 2020

Contents

1 2018

Show that no finite group is the union of conjugates of a proper subgroup.

Classify all groups of order 18 up to isomorphism.

Let α, β denote the unique positive real 5^{th} root of 7 and 4^{th} root of 5, respectively. Determine the degree of $\mathbb{Q}(\alpha, \beta)$ over $\mathbb{Q}$.

Show that the field extension $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ is Galois and determine its Galois group.

Let M be a square matrix over a field K. Use a suitable canonical form to show that M is similar to its transpose M^T.

Let G be a finite group and π, π' be two irreducible representations of G. Prove or disprove the following assertion: π and π' are equivalent if and only if $\det \pi(g) = \det \pi'(g)$ for all $g \in G$.

2 2017

Let R be a Noetherian ring. Prove that $R[x]$ and $R[[x]]$ are both Noetherian. (The first part of the question is asking you to prove the Hilbert Basis Theorem, not to use it!)

Classify (with proof) all fields with finitely many elements.

Suppose A is a commutative ring and M is a finitely presented module. Given any surjection $\phi : A^n \to M$ from a finite free A-module, show that $\ker \phi$ is finitely generated.

Classify all groups of order 57.

Show that a finite simple group cannot have a 2-dimensional irreducible representation over $\mathbb{C}$. (Hint: the determinant might prove useful.)

3 2016

Let G be a finite simple group. Assume that every proper subgroup of G is abelian. Prove that then G is cyclic of prime order.

Let $a \in \mathbb{N}$, $a > 0$. Compute the Galois group of the splitting field of the polynomial $x^5 - 5a^4x + a$ over $\mathbb{Q}$.

Recall that an inner automorphism of a group is an automorphism given by conjugation by an element of the group. An outer automorphism is an automorphism that is not inner.

(a) Prove that S_5 has a subgroup of order 20.

(b) Use the subgroup from (a) to construct a degree 6 permutation representation of S_5 (i.e., an embedding $S_5 \hookrightarrow S_6$ as a transitive permutation group on 6 letters).

(c) Conclude that S_6 has an outer automorphism.

Let A be a commutative ring and M a finitely generated A-module. Define

$$\mathrm{Ann}(M) = \{a \in A : am = 0 \text{ for all } m \in M\}.$$

Show that for a prime ideal $\mathfrak{p} \subset A$, the following are equivalent:

(a) $\mathrm{Ann}(M) \not\subset \mathfrak{p}$

(b) The localization of M at the prime ideal $\mathfrak{p}$ is 0.

(c) $M \otimes_A k(\mathfrak{p}) = 0$, where $k(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ is the residue field of A at $\mathfrak{p}$.

Let $A = \mathbb{C}[x, y]/(y^2 - (x-1)^3 - (x-1)^2)$.

(a) Show that A is an integral domain and sketch the $\mathbb{R}$-points of Spec$A$.

(b) Find the integral closure of A. Recall that for an integral domain A with fraction field K, the integral closure of A in K is the set of all elements of K integral over A.

Let $R = k[x, y]$ where k is a field, and let $I = (x, y)R$.

1. Show that

   $$2 \longrightarrow R \xrightarrow{\phi} R \oplus R \xrightarrow{\psi} R \longrightarrow k \longrightarrow 0$$

   where $\phi(a) = (-ya, xa)$, $\psi((a, b)) = xa + yb$ for $a, b \in R$, is a projective resolution of the R-module $k \simeq R/I$.

2. Show that I is not a flat R-module by computing $\underset{i}{\overset{R}{\mathrm{Tor}}}(I, k)$

4 2015

(a) Find an irreducible polynomial of degree 5 over the field $\mathbb{Z}/2$ of two elements and use it to construct a field of order 32 as a quotient of the polynomial ring $\mathbb{Z}/2[x]$.

(b) Using the polynomial found in part (a), find a 5×5 matrix M over $\mathbb{Z}/2$ of order 31, so that $M^{31} = I$ but $M \neq I$.

Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. Justify your answer.

(a) Let R be a commutative ring with no nonzero nilpotent elements. Show that the only units in the polynomial ring $R[x]$ are the units of R, regarded as constant polynomials.

(b) Find all units in the polynomial ring $\mathbb{Z}_4[x]$.

Let p, q be two distinct primes. Prove that there is at most one non-abelian group of order pq and describe the pairs (p, q) such that there is no non-abelian group of order pq.

(a) Let L be a Galois extension of a field K of degree 4. What is the minimum number of subfields there could be strictly between K and L? What is the maximum number of such subfields? Give examples where these bounds are attained.

(b) How do these numbers change if we assume only that L is separable (but not necessarily Galois) over K?

Let R be a commutative algebra over $\mathbb{C}$. A derivation of R is a $\mathbb{C}$-linear map $D : R \to R$ such that (i) $D(1) = 0$ and (ii) $D(ab) = D(a)b + aD(b)$ for all $a, b \in R$.

(a) Describe all derivations of the polynomial ring $\mathbb{C}[x]$.

(b) Let A be the subring (or $\mathbb{C}$-subalgebra) of $\underset{\mathbb{C}}{\mathrm{End}}(\mathbb{C}[x])$ generated by all derivations of $\mathbb{C}[x]$ and the left multiplications by x. Prove that $\mathbb{C}[x]$ is a simple left A-module. Note that the inclusion $A \to \underset{\mathbb{C}}{\mathrm{End}}(\mathbb{C}[x])$ defines a natural left A-module structure on $\mathbb{C}[x]$.

Let G be a non-abelian group of order p^3 with p a prime.

(a) Determine the order of the center Z of G.

(b) Determine the number of inequivalent complex 1-dimensional representations of G.

(c) Compute the dimensions of all the inequivalent irreducible representations of G and verify that the number of such representations equals the number of conjugacy classes of G.

5 2014

(a) Let G be a group (not necessarily finite) that contains a subgroup of index n. Show that G contains a *normal* subgroup N such that $n \leq [G : N] \leq n!$

(b) Use part (a) to show that there is no simple group of order 36.

Let p be a prime, let $\mathbb{F}_p$ be the p-element field, and let $K = \mathbb{F}_p(t)$ be the field of rational functions in t with coefficients in $\mathbb{F}_p$. Consider the polynomial $f(x) = x^p - t \in K[x]$.

(a) Show that f does not have a root in K.

(b) Let E be the splitting field of f over K. Find the factorization of f over E.

(c) Conclude that f is irreducible over K.

Recall that a ring A is called *graded* if it admits a direct sum decomposition $A = \oplus_{n=0}^{\infty} A_n$ as abelian groups, with the property that $A_i A_j \subseteq A_{i+j}$ for all $i, j \geq 0$. Prove that a graded commutative ring $A = \oplus_{n=0}^{\infty} A_n$ is Noetherian if and only if A_0 is Noetherian and A is finitely generated as an algebra over A_0.

Let R be a ring with the property that $a^2 = a$ for all $a \in R$.

(a) Compute the Jacobson radical of R.

(b) What is the characteristic of R?

(c) Prove that R is commutative.

(d) Prove that if R is finite, then R is isomorphic (as a ring) to $(\mathbb{Z}/2\mathbb{Z})^d$ for some d.

Let $\overline{\mathbb{F}_p}$ denote the algebraic closure of $\mathbb{F}_p$. Show that the Galois group $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ has no non-trivial finite subgroups.

Let C_p denote the cyclic group of order p.

(a) Show that C_p has two irreducible representations over $\mathbb{Q}$ (up to isomorphism), one of dimension 1 and one of dimension $p - 1$.

(b) Let G be a finite group, and let $\rho : G \to \underset{n}{\mathrm{GL}}(\mathbb{Q})$ be a representation of G over $\mathbb{Q}$. Let $\rho_{\mathbb{C}} : G \to \underset{n}{\mathrm{GL}}(\mathbb{C})$ denote ρ followed by the inclusion $\underset{n}{\mathrm{GL}}(\mathbb{Q}) \to \underset{n}{\mathrm{GL}}(\mathbb{C})$. Thus $\rho_{\mathbb{C}}$ is a representation of G over $\mathbb{C}$, called the *complexification* of ρ. We say that an irreducible representation ρ of G is *absolutely irreducible* if its complexification remains irreducible over $\mathbb{C}$.
Now suppose G is abelian and that every representation of G over $\mathbb{Q}$ is absolutely irreducible. Show that $G \cong (C_2)^k$ for some k (i.e., is a product of cyclic groups of order 2).

Let G be a finite group and $\mathbb{Z}[G]$ the internal group algebra. Let $\mathcal{Z}$ be the center of $\mathbb{Z}[G]$. For each conjugacy class $C \subseteq G$, let $P_C = \sum_{g \in C} g$.

(a) Show that the elements P_C form a $\mathbb{Z}$-basis for $\mathcal{Z}$. Hence $\mathcal{Z} \cong \mathbb{Z}^d$ as an abelian group, where d is the number of conjugacy classes in G.

(b) Show that if a ring R is isomorphic to $\mathbb{Z}^d$ as an abelian group, then every element in R satisfies a monic integral polynomial. (**Hint:** Let $\{v_1, \ldots, v_d\}$ be a basis of R and for a fixed non-zero $r \in R$, write $rv_i = \sum_j a_{ij} v_j$. Use the Hamilton-Cayley theorem.)

(c) Let $\pi : G \to \mathrm{GL}(V)$ be an irreducible representation of G (over $\mathbb{C}$). Show that $\pi(P_C)$ acts on V as multiplication by the scalar

$$\frac{|C|\chi_\pi(C)}{\dim V},$$

where $\chi_\pi(C)$ is the value of the character χ_π on any element of C.

(d) Conclude that $|C|\chi_\pi(C)/\dim V$ is an algebraic integer.

6 2013

(a) Suppose that G is a finitely generated group. Let n be a positive integer. Prove that G has only finitely many subgroups of index n

(b) Let p be a prime number. If G is any finitely-generated abelian group, let $t_p(G)$ denote the number of subgroups of G of index p. Determine the possible values of $t_p(G)$ as G varies over all finitely-generated abelian groups.

Suppose that G is a finite group of order 2013. Prove that G has a normal subgroup N of index 3 and that N is a cyclic group. Furthermore, prove that the center of G has order divisible by 11. (You will need the factorization $2013 = 3 \cdot 11 \cdot 61$.)

This question concerns an extension K of $\mathbb{Q}$ such that $[K : \mathbb{Q}] = 8$. Assume that $K/\mathbb{Q}$ is Galois and let $G = \mathrm{Gal}(K/\mathbb{Q})$. Furthermore, assume that G is non-abelian.

(a) Prove that K has a unique subfield F such that $F/\mathbb{Q}$ is Galois and $[F : \mathbb{Q}] = 4$.

(b) Prove that F has the form $F = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ where d_1, d_2 are non-zero integers.

(c) Suppose that G is the quaternionic group. Prove that d_1 and d_2 are positive integers.

This question concerns the polynomial ring $R = \mathbb{Z}[x, y]$ and the ideal $I = (5, x^2 + 2)$ in R.

(a) Prove that I is a prime ideal of R and that R/I is a PID.

(b) Give an explicit example of a maximal ideal of R which contains I. (Give a set of generators for such an ideal.)

(c) Show that there are infinitely many distinct maximal ideals in R which contain I.

7 2012

Classify all groups of order 2012 up to isomorphism. (Hint: 503 is prime).

For any positive integer n, let G_n be the group generated by a and b subject to the following three relations:

$$a^2 = 1, \quad b^2 = 1, \quad \text{and} \quad (ab)^n = 1.$$

(a) Find the order of the group G_n

(We don't know how to do the rest of the problem)

Determine the Galois groups of the following polynomials over $\mathbb{Q}$.

(a) $f(x) = x^4 + 4x^2 + 1$

(b) $f(x) = x^4 + 4x^2 - 5$.

Let R be a (commutative) principal ideal domain, let M and N be finitely generated free R-modules, and let $\varphi : M \to N$ be an R-module homomorphism.

(a) Let K be the kernel of φ. Prove that K is a direct summand of M.

(b) Let C be the image of φ. Show by example (specifying R, M, N, and φ) that C need not be a direct summand of N.

8 2011

In this problem, as you apply Sylow's Theorem, state precisely which portions you are using.

(a) Prove that there is no simple group of order 30.

(b) Suppose that G is a simple group of order 60. Determine the number of p-Sylow subgroups of G for each prime p dividing 60, then prove that G is isomorphic to the alternating group A_5.

Note: in the second part, you needn't show that A_5 is simple. You need only show that if there is a simple group of order 60, then it must be isomorphic to A_5.

Describe the Galois group and the intermediate fields of the cyclotomic extension $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$.

Let

$$R = \mathbb{Z}[x]/(x^2 + x + 1).$$

(a) Answer the following questions with suitable justification.

(i) Is R a Noetherian ring?

(ii) Is R an Artinian ring?

(b) Prove that R is an integrally closed domain.

Let R be a commutative ring. Recall that an element r of R is *nilpotent* if $r^n = 0$ for some positive integer n and that the *nilradical* of R is the set $N(R)$ of nilpotent elements.

(a) Prove that

$$N(R) = \cap_{P \text{ prime}} P.$$

(Hint: given a non-nilpotent element r of R, you may wish to construct a prime ideal that does not contain r or its powers.)

(b) Given a positive integer m, determine the nilradical of $\mathbb{Z}/(m)$.

(c) Determine the nilradical of $\mathbb{C}[x,y]/(y^2-x^3)$.

(d) Let $p(x,y)$ be a polynomial in $\mathbb{C}[x,y]$ such that for any complex number a, $p(a,a^{3/2})=0$. Prove that $p(x,y)$ is divisible by y^2-x^3.

Given a finite group G, recall that its *regular representation* is the representation on the complex group algebra $\mathbb{C}[G]$ induced by left multiplication of G on itself and its *adjoint representation* is the representation on the complex group algebra $\mathbb{C}[G]$ induced by conjugation of G on itself.

(a) Let $G=\mathrm{GL}_2(\mathbb{F}_2)$. Describe the number and dimensions of the irreducible representations of G. Then describe the decomposition of its regular representation as a direct sum of irreducible representations.

(b) Let G be a group of order 12. Show that its adjoint representation is reducible; that is, there is an H-invariant subspace of $\mathbb{C}[H]$ besides 0 and $\mathbb{C}[H]$.

Let R be a commutative integral domain. Show that the following are equivalent:

(a) R is a field;

(b) R is a semi-simple ring;

(c) Any R-module is projective.

9 2010

Let p be a positive prime number, $\mathbb{F}_p$ the field with p elements, and let $G=\mathrm{GL}_2(\mathbb{F}_p)$.

(a) Compute the order of G, $|G|$.

(b) Write down an explicit isomorphism from $\mathbb{Z}/p\mathbb{Z}$ to

$$U=\left\{\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\middle| a\in\mathbb{F}_p\right\}.$$

(c) How many subgroups of order p does G have? Hint: compute gug^{-1} for $g\in G$ and $u\in U$; use this to find the size of the normalizer of U in G.

(a) Give definitions of the following terms: (i) a finite length (left) module, (ii) a composition series for a module, and (iii) the length of a module,

(b) Let $l(M)$ denote the length of a module M. Prove that if

$$0\to M_1\to M_2\to\cdots\to M_n\to 0$$

is an exact sequence of modules of finite length, then

$$\sum_{i=1}^{n}(-1)^k l(M_i)=0.$$

Let $\mathbb{F}$ be a field of characteristic p, and G a group of order p^n. Let $R=\mathbb{F}[G]$ be the group ring (group algebra) of G over $\mathbb{F}$, and let $u:=\sum_{x\in G}x$ (so u is an element of R).

(a) Prove that u lies in the center of R.

(b) Verify that Ru is a 2-sided ideal of R.

(c) Show there exists a positive integer k such that $u^k = 0$. Conclude that for such a k, $(Ru)^k = 0$.

(d) Show that R is **not** a semi-simple ring. (**Warning:** Please use the definition of a semi-simple ring: do **not** use the result that a finite length ring fails to be semisimple if and only if it has a non-zero nilpotent ideal.)

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ (where $a_n \neq 0$) and let $R = \mathbb{Z}[x]/(f)$. Prove that R is a finitely generated module over $\mathbb{Z}$ if and only if $a_n = \pm 1$.

Consider the ring

$$S = C[0,1] = \{f : [0,1] \to \mathbb{R} : f \text{ is continuous}\}$$

with the usual operations of addition and multiplication of functions.

(a) What are the invertible elements of S?

(b) For $a \in [0,1]$, define $I_a = \{f \in S : f(a) = 0\}$. Show that I_a is a maximal ideal of S.

(c) Show that the elements of any proper ideal of S have a common zero, i.e., if I is a proper ideal of S, then there exists $a \in [0,1]$ such that $f(a) = 0$ for all $f \in I$. Conclude that every maximal ideal of S is of the form I_a for some $a \in [0,1]$. **Hint:** as $[0,1]$ is compact, every open cover of $[0,1]$ contains a finite subcover.

Let F be a field of characteristic zero, and let K be an *algebraic* extension of F that possesses the following property: every polynomial $f \in F[x]$ has a root in K. Show that K is algebraically closed. **Hint:** if $K(\theta)/K$ is algebraic, consider $F(\theta)/F$ and its normal closure; primitive elements might be of help.

Let G be the unique non-abelian group of order 21.

(a) Describe all 1-dimensional complex representations of G.

(b) How many (non-isomorphic) irreducible complex representations does G have and what are their dimensions?

(c) Determine the character table of G.

10 2009

(a) Classify all groups of order $2009 = 7^2 \times 41$.

(b) Suppose that G is a group of order 2009. How many intermediate groups are there—that is, how many groups H are there with $1 \subsetneq H \subsetneq G$, where both inclusions are proper? (There may be several cases to consider.)

Let K be a field. A discrete valuation on K is a function $\nu : K \setminus \{0\} \to \mathbb{Z}$ such that

(i) $\nu(ab) = \nu(a) + \nu(b)$

(ii) ν is surjective

(iii) $\nu(a+b) \geq \min\{(\nu(a), \nu(b)\}$ for $a, b \in K \setminus \{0\}$ with $a+b \neq 0$.

Let $R := \{x \in K \setminus \{0\} : \nu(x) \geq 0\} \cup \{0\}$. Then R is called the valuation ring of ν. Prove the following:

(a) R is a subring of K containing the 1 in K.

(b) for all $x \in K \setminus \{0\}$, either x or x^{-1} is in R.

(c) x is a unit of R if and only if $\nu(x) = 0$.

(d) Let p be a prime number, $K = \mathbb{Q}$, and $\nu_p : \mathbb{Q} \setminus \{0\} \to \mathbb{Z}$ be the function defined by $\nu_p(\frac{a}{b}) = n$ where $\frac{a}{b} = p^n \frac{c}{d}$ and p does not divide c and d. Prove that the corresponding valuation ring R is the ring of all rational numbers whose denominators are relatively prime to p.

Let F be a field of characteristic not equal to 2.

(a) Prove that any extension K of F of degree 2 is of the form $F(\sqrt{D})$ where $D \in F$ is not a square in F and, conversely, that each such extension has degree 2 over F.

(b) Let $D_1, D_2 \in F$ neither of which is a square in F. Prove that $[F(\sqrt{D_1}, \sqrt{D_2}) : F] = 4$ if $D_1 D_2$ is not a square in F and is of degree 2 otherwise.

Let F be a field and $p(x) \in F[x]$ an irreducible polynomial.

(a) Prove that there exists a field extension K of F in which $p(x)$ has a root.

(b) Determine the dimension of K as a vector space over F and exhibit a vector space basis for K.

(c) If $\theta \in K$ denotes a root of $p(x)$, express θ^{-1} in terms of the basis found in part (b).

(d) Suppose $p(x) = x^3 + 9x + 6$. Show $p(x)$ is irreducible over $\mathbb{Q}$. If θ is a root of $p(x)$, compute the inverse of $(1+\theta)$ in $\mathbb{Q}(\theta)$.

Fix a ring R, an R-module M, and an R-module homomorphism $f : M \to M$.

(a) If M satisfies the descending chain condition on submodules, show that if f is injective, then f is surjective. (Hint: note that if f is injective, so are $f \circ f$, $f \circ f \circ f$, etc.)

(b) Give an example of a ring R, an R-module M, and an injective R-module homomorphism $f : M \to M$ which is not surjective.

(c) If M satisfies the ascending chain condition on submodules, show that if f is surjective, then f is injective.

(d) Give an exampe of a ring R, and R-module M, and a surjective R-module homomorphism $f : M \to M$ which is not injective.

Let G be a finite group, k an algebraically closed field, and V an irreducible k-linear representation of G.

(a) Show that $\underset{kG}{\mathrm{Hom}}(V, V)$ is a division algebra with k in its center.

(b) Show that V is finite-dimensional over k, and conclude that $\underset{kG}{\mathrm{Hom}}(V, V)$ is also finite dimensional.

(c) Show the inclusion $k \hookrightarrow \underset{kG}{\mathrm{Hom}}(V,V)$ found in (a) is an isomorphism. (For $f \in \underset{kG}{\mathrm{Hom}}(V,V)$, view f as a linear transformation and consider $f - \alpha I$, where α is an eigenvalue of f).

11 2008

Let $f(x)$ be an irreducible polynomial of degree 5 over the field $\mathbb{Q}$ of rational numbers with exactly 3 real roots.

(a) Show that $f(x)$ is not solvable by radicals.

(b) Let E be the splitting field of f over $\mathbb{Q}$. Construct a Galois extension K of degree 2 over $\mathbb{Q}$ lying in E such that *no* field F strictly between K and E is Galois over $\mathbb{Q}$.

Let F be a finite field. Show for any positive integer n that there are irreducible polynomials of degree n in $F[x]$.

Show that the order of the group $\mathrm{GL}_n(\mathbb{F}_q)$ of invertible $n \times n$ matrices over the field $\mathbb{F}_q$ of q elements is given by $(q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$.

(a) Let R be a commutative principal ideal domain. Show that any R-module M generated by two elements takes the form $R/(a) \oplus R/(b)$ for some $a, b \in R$. What more can you say about a and b?

(b) Give a necessary and sufficient condition for two direct sums as in part (a) to be isomorphic as R-modules.

Let G be the subgroup of $\mathrm{GL}_3(\mathbb{C})$ generated by the three matrices

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} i & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where $i^2 = -1$. Here $\mathbb{C}$ denotes the complex field.

(a) Compute the order of G.

(b) Find a matrix in G of largest possible order (as an element of G) and compute this order.

(c) Compute the number of elements in G with this largest order.

(a) Let G be a group of (finite) order n. Show that any irreducible left module over the group algebra $\mathbb{C}G$ has complex dimension at least $\sqrt{n}$.

(b) Give an example of a group G of order $n \geq 5$ and an irreducible left module over $\mathbb{C}G$ of complex dimension $\lfloor \sqrt{n} \rfloor$, the greatest integer to $\sqrt{n}$.

Use the rational canonical form to show that any square matrix M over a field k is similar to its transpose M^t, recalling that $p(M) = 0$ for some $p \in k[t]$ if and only if $p(M^t) = 0$.

12 2007

Let K be a field of characteristic zero and L a Galois extension of K. Let f be an irreducible polynomial in $K[x]$ of degree 7 and suppose f has no zeroes in L. Show that f is irreducible in $L[x]$.

Let K be a field of characteristic zero and $f \in K[x]$ an irreducible polynomial of degree n. Let L be a splitting field for f. Let G be the group of automorphisms of L which act trivially on K.

(a) Show that G embeds in the symmetric group S_n.

(b) For each n, give an example of a field K and polynomial f such that $G = S_n$.

(c) What are the possible groups G when $n = 3$. Justify your answer.

Show there are exactly two groups of order 21 up to isomorphism.

13 2006

Let K be the field $\mathbb{Q}(z)$ of rational functions in a variable z with coeffiecients in the rational field $\mathbb{Q}$. Let n be a positive integer. Consider the polynomial $x^n - z \in K[x]$.

(a) Show that the polynomial $x^n - z$ is irreducible over K.

(b) Describe the splitting field of $x^n - z$ over K.

(c) Determine the Galois group of the splitting field of $x^5 - z$ over the field K.

(a) Let $p < q < r$ be prime integers. Show that a group of order pqr cannot be simple.

(b) Consider groups of orders $2^2 \cdot 3 \cdot p$ where p has the values 5, 7, and 11. For each of those values of p, either display a simple group of order $2^2 \cdot 3 \cdot p$, or show that there cannot be a simple group of that order.

Let K/F be a finite Galois extension and let $n = [K : F]$. There is a theorem (often referred to as the "normal basis theorem") which states that there exists an irreducible polynomial $f(x) \in F[x]$ whose roots form a basis for K as a vector space over F. You may assume that theorem in this problem.

(a) Let $G = \mathrm{Gal}(K/F)$. The action of G on K makes K into a finite-dimensional representation space for G over F. Prove that K is isomorphic to the regular representation for G over F. (The regular representation is defined by letting G act on the group algebra $F[G]$ by multiplication on the left.)

(b) Suppose that the Galois group G is cyclic and that F contains a primitive n^{th} root of unity. Show that there exists an injective homomorphism $\chi : G \to F^\times$.

(c) Show that K contains a non-zero element a with the following property:

$$g(a) = \chi(g) \cdot a$$

for all $g \in G$.

(d) If a has the property stated in (c), show that $K = F(a)$ and that $a^n \in F^\times$.

Let G be the group of matrices of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

with entries in the finite field $\mathbb{F}_p$ of p element, where p is a prime.

(a) Prove that G is non-abelian.

(b) Suppose p is odd. Prove that $g^p = I_3$ for all $g \in G$.

(c) Suppose that $p = 2$. It is known that there are exactly two non-abelian groups of order 8, up to isomorphism: the dihedral group D_8 and the quaternionic group. Assuming this fact without proof, determine which of these groups G is isomorphic to.

There are five nonisomorphic groups of order 8. For each of those groups G, find the smallest positive integer n such that there is an injective homomorphism $\varphi : G \to S_n$.

14 2005

For any group G we define $\Omega(G)$ to be the image of the group homomorphism $\rho : G \to \mathrm{Aut}(G)$ where ρ maps $g \in G$ to the conjugation automorphism $x \mapsto gxg^{-1}$. Starting with a group G_0, we define $G_1 = \Omega(G_0)$ and $G_{i+1} = \Omega(G_i)$ for all $i \geq 0$. If G_0 is of order p^e for a prime p and integer $e \geq 2$, prove that G_{e-1} is the trivial group.

Let $\mathbb{F}_2$ be the field with two elements.

(a) What is the order of $\mathrm{GL}_3(\mathbb{F}_2)$?

(b) Use the fact that $\mathrm{GL}_3(\mathbb{F}_2)$ is a simple group (which you should not prove) to find the number of elements of order 7 in $\mathrm{GL}_3(\mathbb{F}_2)$.

Let G be a finite abelian group. Let $f : \mathbb{Z}^m \to G$ be a surjection of abelian groups. We may think of f as a homomorphism of $\mathbb{Z}$-modules. Let K be the kernel of f.

(a) Prove that K is isomorphic to $\mathbb{Z}^m$.

(b) We can therefore write the inclusion map $K \to \mathbb{Z}^m$ as $\mathbb{Z}^m \to \mathbb{Z}^m$ and represent it by an $m \times m$ integer matrix A. Prove that $|\det A| = |G|$.

Let $R = C([0,1])$ be the ring of all continuous real-valued functions on the closed interval $[0,1]$, and for each $c \in [0,1]$, denote by M_c the set of all functions $f \in R$ such that $f(c) = 0$.

(a) Prove that $g \in R$ is a unit if and only if $g(c) \neq 0$ for all $c \in [0,1]$.

(b) Prove that for each $c \in [0,1]$, M_c is a maximal ideal of R.

(c) Prove that if M is a maximal ideal of T, then $M = M_c$ for some $c \in [0,1]$. (Hint: compactness of $[0,1]$ may be relevant.)

Let R and S be commutative rings, and $f : R \to S$ a ring homomorphism.

(a) Show that if I is a prime ideal of S, then

$$f^{-1}(I) = \{r \in R : f(r) \in I\}$$

is a prime ideal of R.

(b) Let N be the set of nilpotent elements of R:

$$N = \{r \in R : r^m = 0 \text{ for some } m \geq 1\}.$$

N is called the *nilradical* of R. Prove that it is an ideal which is contained in every prime ideal.

(c) Part (a) lets us define a function

$$f^* : \{\text{prime ideals of } S\} \to \{\text{prime ideals of } R\}.$$

$$I \mapsto f^{-1}(I).$$

Let N be the nilradical of R. Show that if $S = R/N$ and $f : R \to R/N$ is the quotient map, then f^* is a bijection

Consider the polynomial $f(x) = x^{10} + x^5 + 1 \in \mathbb{Q}[x]$ with splitting field K over $\mathbb{Q}$.

(a) Determine whether $f(x)$ is irreducible over $\mathbb{Q}$ and find $[K : \mathbb{Q}]$.

(b) Determine the structure of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

For each prime number p and each positive integer n, how many elements α are there in $\mathbb{F}_{p^n}$ such that $F_p(\alpha) = F_{p^6}$?