Algebra Prelim
Autumn 2001

Instructions: There are eight problems altogether. Do as many problems as you can; complete solutions are preferable to partial results. You should write enough so that there is no doubt that you know what is going on, but you needn't write a lot when a few lines suffice. You should not reprove major theorems, but if you use a major result, you should clearly state what you are doing.

1. Up to isomorphism, how many groups are there of order 2001? Prove your answer. (Note: $2001 = 3 \cdot 23 \cdot 29$.)

2. Write $\mathbb{Z}^3 / \langle (1,2,3), (4,5,6), (7,8,9) \rangle$ as a product of cyclic groups. (Here, "$\langle \cdots \rangle$" denotes the subgroup generated by those elements.)

3. Suppose K is a field of characteristic $p > 0$, and let A denote the K-algebra $K[x]/(1-x^p)$.

   (a) Define a map $\varphi : K[y] \to A$ by $\varphi(f(y)) = f(1-x)$ for any $f(y) \in K[y]$. Show that φ is a surjective ring homomorphism, identify the kernel, and use this to get an alternate description of A.

   (b) Use part (a) to classify the finitely generated A-modules.

4. (a) Suppose R is a commutative noetherian ring. Prove that any nonzero ideal in R contains a finite product of nonzero prime ideals.

   (b) Let $R = \mathbb{C}[x, y]$. Find a nonzero ideal in R which does not contain a finite product of maximal ideals.

5. Suppose K is a field, and $f(x)$ and $g(x)$ are irreducible polynomials in $K[x]$. Let α be a root of $f(x)$ and β a root of $g(x)$.

   (a) Prove that $f(x)$ remains irreducible in $K(\beta)[x]$ if and only if $g(x)$ remains irreducible in $K(\alpha)[x]$.

   (b) Give an example where both remain irreducible.

   (c) Give an example (with $f(x)$ not proportional to $g(x)$) where neither remains irreducible.

- over -

6. Let $\zeta \in \mathbb{C}$ be a primitive 5th root of unity. Consider the polynomial $f(x) = x^5 - 3$ over the fields

   (a) $\mathbb{Q}(\zeta)$,

   (b) $\mathbb{R}$,

   (c) $\mathbb{C}$.

   For each of the cases (a)–(c), find the splitting field and the Galois group of $f(x)$. What is the order of the Galois group of $f(x)$ over the field $\mathbb{Q}$?

7. Suppose K is a field of characteristic 0, and $f(x) \in K[x]$ is an irreducible polynomial of degree 11.

   (a) Explain (with proof) why the splitting field of $f(x)$ cannot have degree 33.

   (b) Why does your proof for part (a) fail for degree 55?

8. Prove: any invertible real matrix A can be written as a product of a real symmetric positive definite matrix and an orthogonal matrix. [Hint: find a real symmetric positive definite matrix S so that $S^2 = AA^t$.]

Algebra Prelim
Autumn 2000

Instructions: Do as many problems as you can, but you needn't try to say something about every problem, especially if you don't have something to say about every problem. Complete solutions are preferable to partial results. Indeed, four complete, correct solutions constitute a passing performance. You should write enough so that there is no doubt that you know what is going on, but you needn't write a lot when a few lines suffice. You should not reprove major theorems, but if you use a major result, you should clearly state what you are using.

1. Show that every group of order 616 is solvable.

2. Let F be a field of characteristic 0 and let $f(x)$ be an irreducible polynomial of degree 4 in $F[x]$. Suppose that L is a splitting field of $f(x)$ over F.

   (a) Show that the degree $[L : F]$ is divisible by 4 and divides 24. You may quote basic facts about degrees of field extensions in towers.

   (b) Suppose α is a root of $f(x)$ in L and let $K = F[\alpha]$. Describe three qualitatively different ways that $f(x)$ might factor in $K[x]$ as a product of irreducible polynomials. For each one, describe the possible values $[L : F]$ can assume.

   (c) Give an explicit example of F, of $f(x)$, and of L for which $[L : F] = 4$. Be sure to demonstrate the irreducibility of your chosen $f(x)$ in $F[x]$.

3. Let p be a prime number and let G be a group of order $p^r m$, with r a positive integer and $(p, m) = 1$. The regular action of G on itself by left multiplication induces an action of G on the collection $\mathcal{X}$ of subsets of G of cardinality p^r. Let X be an element of $\mathcal{X}$ and let G_X be the stabilizer subgroup of X. Show that the order of G_X divides p^r.

4. Let R be a commutative ring. Recall that an element t of R is *nilpotent* if $t^n = 0$ for some positive integer n.

   (a) Suppose t is not nilpotent. Let T be the set $\{t^n : n \geq 0\}$ and let $\mathcal{I}$ be the set of ideals of R disjoint from T. Prove that $\mathcal{I}$ contains an element that is maximal with respect to inclusion; that is, show that there is an ideal M of R disjoint from T such that any ideal of R properly containing M contains an element of T.

   (b) Prove that the ideal M whose existence you have demonstrated in the first part is a prime ideal. (Hint: Suppose r and s are elements of R for which $rs \in M$. Consider the ideals $(r) + M$ and $(s) + M$.)

   (c) Let $N(R)$ be the intersection of the prime ideals of R. Prove that every element of $N(R)$ is nilpotent.

5. Let I_n denote the identity map on $\mathbb{R}^n$ and suppose that $T : \mathbb{R}^n \to \mathbb{R}^n$ is a linear map.

   (a) Suppose $n = 2$ and $T^2 = -I_2$. Prove that there are no T-eigenvectors in $\mathbb{R}^2$.

   (b) Suppose $n = 2$ and $T^2 = I_2$. Prove that $\mathbb{R}^2$ has a basis consisting of T-eigenvectors.

   (c) Suppose $n = 3$. Prove that $\mathbb{R}^3$ contains a T-eigenvector. Give an example of an operator T such that $\mathbb{R}^3$ contains a T-eigenvector, but $\mathbb{R}^3$ does not have a basis consisting of T-eigenvectors.

6. Let K be a field, let n be an integer greater than 1, and let $T : K^n \to K^n$ be a linear map. Suppose that $T^n = 0$ but $T^{n-1} \neq 0$. Prove that there is no linear map $S : K^n \to K^n$ satisfying $S^2 = T$.

7. A module M over a commutative ring R is *Artinian* if it satisfies the descending chain condition on submodules; that is, given any sequence of submodules

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots$$

   of M, there is a positive integer r such that $M_r = M_{r+t}$ for any positive integer t.

   (a) Suppose K is a submodule of M such that K and M/K are Artinian. Prove that M is Artinian.

   (b) Give an example of a principal ideal domain R and an R-module M such that M is finitely generated but not Artinian.

   (c) Give an example of a principal ideal domain R and an R-module M such that M is torsion but not Artinian.

   (d) Suppose that R is a principal ideal domain and M is a finitely-generated torsion R-module. Prove that M is Artinian.

8. The four parts of this problem are independent of each other. What ties them together is that they are all "quickies"; each can be done briefly and with relative ease once you see the right path.

   (a) Let R be a commutative integral domain. Show that R can't have exactly 20 elements.

   (b) Recall that an *algebraic number* is a complex number that is algebraic over $\mathbb{Q}$. Suppose that a and $b^2 + a$ are algebraic numbers. Prove that b is an algebraic number.

   (c) Find a unique factorization domain D and two elements u and v of D such that no greatest common divisor of u and v is of the form $au + bv$ for any elements a and b of D.

   (d) Describe the prime ideals of the ring $\mathbb{Z}[x]/(x^{30}, 30)$.

Algebra Prelim
Autumn 1999

Instructions: Do as many problems as you can. Complete solutions are preferable to partial results. You should not reprove major theorems, but if you use a major theorem, you should state what you are using clearly.

1. Suppose that R is a principal ideal domain. Let M and N be finitely generated free R-modules and let $\phi : M \longrightarrow N$ be an R-module homomorphism.

   (a) Let A be the kernel of ϕ, which is an R-submodule of M. Prove that A is a direct summand of M (i.e., that M contains an R-submodule B such that $M = A + B$ and $A \cap B = \{0\}$.)

   (b) Let C be the image of ϕ, which is an R-submodule of N. Show by example that C is not necessarily a direct summand of N. (Give explicit choices for R, M, N, and ϕ.)

2. Let R be a ring.

   (a) Suppose that M is a left R-module that satisfies the descending chain condition on submodules. Show that if $f : M \longrightarrow M$ is an injective R-module mapping, then f is surjective. (Note that if f is injective, so is each composite $f \circ \cdots \circ f$ of f with itself n-times.)

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

   (c) Suppose that M is a left R-module that satisfies the ascending chain condition on submodules. Show that if $f : M \longrightarrow M$ is an surjective R-module mapping, then f is injective. (Note that if f is surjective, so is each composite $f \circ \cdots \circ f$ of f with itself n-times.)

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

3. Let $R = \mathbb{Z}[X]$, the polynomial ring in one variable X with integral coefficients.

   (a) Prove that if k is any finite field, then there is at least one maximal ideal M of R such that R/M is isomorphic to k.

   (b) Suppose that $k = \mathbb{F}_{81}$, the field with 81 elements. Prove that R has exactly eighteen maximal ideals M such that R/M is isomorphic to k.

4. Let $R = Mat_{2\times 2}(\mathbb{C})$ be the ring of 2×2-matrices with entries in the field $\mathbb{C}$ of complex numbers, and let T be the subring of upper triangular matrices in R.

   (a) Show that the elements of a set of commuting matrices in R have an eigenvector in common.

   (b) Suppose that S is a subset of R consisting of mutually commuting matrices. Prove that there is an invertible matrix A in R such that $S \subset ATA^{-1}$.

   (c) Prove that there cannot be three commuting linearly independent matrices in R.

5. Let G be a finite group.

   (a) Show that a group of order 15 is abelian.

   (b) Show that a group of order 30 has a subgroup of order 15.

   (c) Describe all groups of order 30.

6. Suppose that G is a group. Denote the number of elements in G by $|G|$. Let $< x >$ be the cyclic subgroup of G generated by an element x. Consider the following property that a group might or might not have: If x and y are elements of G such that $< x >=< y >$, then x and y are conjugate elements of G.

   (a) Describe all abelian groups with that property.

   (b) Show that for any integer $n \geq 3$, the symmetric group S_n has that property.

   (c) Show that the alternating groups A_3 and A_4 do not have that property.

   (d) Suppose that G is a finite group with that property. Prove that if p is a prime divisor of $|G|$, then $p-1$ divides $|G|$ too.

7. Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of prime degree $p \geq 3$ over the field $\mathbb{Q}$ of rational numbers. Suppose that $f(X)$ has exactly two nonreal roots. Let K be the splitting field of $f(X)$ over $\mathbb{Q}$, and let G be the Galois group of $K/\mathbb{Q}$. G can be identified with a subgroup of the symmetric group S_p, the permutation group of the roots of $f(X)$.

   (a) Show that G, as a subgroup of the symmetric group S_p, contains a transposition and a p-cycle.

   (b) Show that $G = S_p$.

8. Consider the field $F = \mathbb{Q}(t)$ of rational functions in a variable t with coefficients in the field $\mathbb{Q}$ of rational numbers. Consider the polynomial $f(X) = X^n - t \in F[X]$. Let K be the splitting field of $f(X)$ over F. Let G be the Galois group of K over F. Describe G as an abstract group for each value of $n > 1$. (Your description should be precise enough to determine G up to isomorphism as an abstract group.)

ALGEBRA PRELIM
FALL 1998

1. Let E be the splitting field over $\mathbb{Q}$ of $x^5 - 2$. Let G denote the Galois group of E over $\mathbb{Q}$.

(a) Show that $[E : \mathbb{Q}] = 20$.
(b) Show that the Sylow 5-subgroup of G is normal.
(c) Show that the Sylow 2-subgroups are not normal.
(d) What is the Galois correspondence for the Sylow 2-subgroups?

2. Let p be a prime number. Let G be the group of 3×3 upper triangular matrices over $\mathbb{Z}_p$ with 1's on the diagonal. That is,

$$G = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}.$$

(a) Show that G is a non-abelian group of order p^3.
(b) Show that if $p \neq 2$, then $x^p = 1$ for all $x \in G$.
(c) If $p = 2$ which of the non-abelian groups of order 8 is G? The dihedral or quaternion group? Explain your answer.

3.

(a) What is the automorphism group of the group of order 7?
(b) Let G be a group of order 385. Show that either G is cyclic or that its center has order 7.

4. Let D be an integer that is not a perfect square. Let $p \in \mathbb{Z}$ be a prime. Show that p is a prime in $\mathbb{Z}[\sqrt{D}]$ if and only if $x^2 - D$ is irreducible in $\mathbb{Z}_p[x]$. (Hint: consider the ideal $(p, x^2 - D)$ in $\mathbb{Z}[x]$.)

5. Let $p \in \mathbb{Z}$ be prime. Let A be the $p \times p$ matrix all of whose entries are 1. Find the Jordan normal form of A over $\mathbb{Z}_p$.

6.

(a) State the structure theorem for finitely generated modules over a P.I.D.

(b) Apply this theorem to describe the structure of the $\mathbb{Z}$-module $\mathbb{Z}^3/M$, where M is the submodule generated by $(2,-1,1)$ and $(1,1,5)$.

7. Let $i = \sqrt{-1}$. Give examples of two cyclic $\mathbb{Z}[i]$-modules, one semisimple, say M, and one not, say N. (Justify your answer.) Let I and J denote their respective annihilators. (The annihilator of a module consists of the elements x in the ring such that $xm = 0$ for every element m in the module. It is a two-sided ideal.) Determine I and J, and if possible express $\mathbb{Z}[i]/I$ and $\mathbb{Z}[i]/J$ as a direct sum of two smaller rings.

8. Let F be an infinite field. Suppose that E is a Galois extension of F with Galois group G.

(a) Show that for $a \in E$, $F(a) = E$ if and only if $\sigma(a) \neq a$ for all non-identity elements $\sigma \in G$.

(b) Show that if E is viewed as affine n-space over F, then

$$\{a \in E \mid F(a) = E\}$$

is a Zariski-open dense subset of E. (You may use the fact that the intersection of two dense open subsets of a space is dense.)

Algebra Prelim
Autumn 1997

Instructions: Do as many problems as you can, neatly. Complete solutions are much preferable to partial results. You should write enough so that there is no doubt that you know what is going on, but do not write a book when a few lines suffice. You should not reprove major theorems (unless asked to do so), but if you use a major result, you should clearly state what you are using.

1. a. Prove that the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a Galois extension over $\mathbb{Q}$.
   b. Find the Galois group of $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.
   c. Describe all fields F with $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

2. a. State Sylow's theorems.
   b. Up to isomorphism, how many groups of order 20 are there? Describe them.

3. Let G be a free abelian group of rank $n \geq 1$, and let G' be a subgroup of the same rank. Let $v_1, \ldots, v_n$ be a basis of G, and let $w_1, \ldots, w_n$ be a basis of G' (as $\mathbb{Z}$-modules). Write
$$w_i = \sum_{j=1}^{n} a_{ij} v_j.$$
Prove that the index $[G : G']$ is $|\det A|$, where A is the $n \times n$ matrix (a_{ij}).

4. Let $T : V \to V$ be a linear transformation, where V is an n-dimensional vector space over the field F. Say that $z \in V$ is a *cyclic vector* for T if $\{z, Tz, \ldots, T^{n-1}z\}$ is a basis for V. Prove that T has a cyclic vector if and only if the only linear transformations commuting with T are polynomials in T.

5. Let E be an extension field of $\mathbb{C}$ such that $E = \mathbb{C}(t, u)$, where t is transcendental over $\mathbb{C}$ and u satisfies $u^2 + t^2 = 1$ over $\mathbb{C}(t)$. Determine the Galois group of $\mathbb{C}(t, u)$ over $\mathbb{C}(t^n, u^n)$ for any $n \in \mathbb{N}$.

6. Recall that a commutative ring A is said to be Noetherian if it satisfies the ascending chain condition; that is, there does not exist a sequence of ideals such that
$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_j \subsetneq \cdots.$$
   a. Prove that A is Noetherian if and only if each of its ideals is finitely generated.

b. Prove that if A is Noetherian, then any A-submodule of $\underbrace{A \oplus \cdots \oplus A}_{n}$ is finitely generated, $n \in \mathbb{N}$. (Use induction on n.)

c. Again assume that A is Noetherian. Prove that any submodule of a finitely generated A-module M is finitely generated.

7. Let $A = \mathbb{R}[x, y]$. Determine all of the maximal ideals of A. For each maximal ideal $\mathfrak{m}$, find elements f and g in A such that $\mathfrak{m} = (f, g)$. (Hint: You may assume the following fact. If E is a field extension of F which is finitely generated as an F-algebra, then it is finitely generated as an F-vector space.)

8. Let $GL_n(\mathbb{C})$ denote the group of invertible $n \times n$ matrices over $\mathbb{C}$, and let

$$f : GL_n(\mathbb{C}) \to \mathbb{C}^\times$$

be a group homomorphism, where $\mathbb{C}^\times$ denotes the multiplicative group of nonzero complex numbers. Let $SL_n(\mathbb{C})$ be the subgroup of $GL_n(\mathbb{C})$ consisting of those matrices with determinant 1.

a. Prove that there exists a homomorphism $g_f : \mathbb{C}^\times \to \mathbb{C}^\times$ such that, if A is any diagonal matrix with diagonal entries $c_1, \ldots, c_n$, then

$$f(A) = g_f(c_1 c_2 \ldots c_n).$$

b. Prove that $SL_n(\mathbb{C}) \subseteq \ker f$. (Hint: Use the fact that any invertible matrix is a product of elementary matrices.)

Algebra Prelim
Autumn 1996

Instructions: Do as many problems as you can. Complete solutions are much preferable to partial results. You should write enough so that there is no doubt that you know what is going on, but do not write a book when a few lines suffice. Be neat. You should not reprove major theorems, but if you use a major result, you should state what you are using clearly.

1. Let L be a finite Galois field extension of F with Galois group G. A field K is called an intermediate field if $F \subseteq K \subseteq L$.
   (a) Describe the one-to-one correspondence between intermediate fields K and subgroups H of G.
   (b) Suppose H_1 and H_2 are two conjugate subgroups of G. What is the relation between the corresponding intermediate fields K_1 and K_2?
   (c) Let K be an intermediate field. If K/F is a Galois extension, describe the Galois group of K/F in terms of G.
   (d) Give an example of three fields $F \subseteq K \subseteq L$ such that L is a Galois extension of F but K is not a Galois extension of F. Justify your answer.

2. Let F be the field of rational functions $\mathbb{C}(z)$ over $\mathbb{C}$ in an indeterminate z and let $f(X)$ in $F[X]$ be the polynomial $X^4 - z$.
   (a) Prove that $f(X)$ is irreducible in $F[X]$.
   (b) Describe a splitting field L for $f(X)$ over F.
   (c) Describe the Galois group of L/F.

3. In this problem, you can use the first part to answer the second and third parts.
   (a) State the classification theorem for finite abelian groups.
   (b) Suppose G is an abelian group of order 81 with a subgroup N that is cyclic of order 9 such that the quotient group G/N is also cyclic of order 9. List the possibilities for G up to isomorphism, specifying for each such G an appropriate choice of subgroup N.
   (c) Let A, B, and C be finite abelian groups such that $A \times B \cong A \times C$. Prove that $B \cong C$.

4. Let G be a finite group and let p be a prime number. Recall that if G has order $p^a t$ with t relatively prime to p, then a p-Sylow subgroup of G is a subgroup of order p^a.
   (a) Suppose G is an arbitrary group of order 60. Prove that G has exactly one or six 5-Sylow subgroups. List three possibilities for the number of 3-Sylow subgroups.
   (b) Let G be the dihedral group of order 60. Show that G has exactly one 3-Sylow subgroup and exactly one 5-Sylow subgroup. Describe a 2-Sylow subgroup of G and then state how many 2-Sylow subgroups there are.
   (c) Let G be the alternating group A_5. How many 3-Sylow subgroups does G have? How many 5-Sylow subgroups? Describe one 2-Sylow subgroup of G as an explicit set of permutations. How many 2-Sylow subgroups does G have?

5. In this problem, all rings will be assumed to be commutative with identity. Under this assumption, a ring is defined to be noetherian if it satisfies the ascending chain condition on ideals and Artinian if it satisfies the descending chain condition on ideals.

   (a) Give an example of a ring that isn't noetherian.

   (b) Must a principal ideal domain be noetherian? Prove or give a counter-example.

   (c) Give an example of a noetherian ring that isn't Artinian.

   (d) Give an example of a noetherian ring, other than a field, that is Artinian.

   (Note: One can prove in contrast that any Artinian ring is automatically noetherian.)

6. Let F be any field and let V be a finite-dimensional vector space over F. Let A and B be two linear transformations from V to itself such that $A^2 = B^2 = I_V$, where I_V denotes the identity map of V to itself. Show that if rank $(A - I_V) =$ rank $(B - I_V)$, then A and B are similar. (Hint: Consider separately the cases in which F has characteristic distinct from 2 and F has characteristic 2.)

7. Let A be an orthogonal $n \times n$ matrix; that is, A has real entries and $AA^T = I_n$.

   (a) Prove that $\det(I_n - A) \geq 0$.

   (b) Prove that $Tr(I_n - A) \geq 0$ and that equality holds if and only if $A = I_n$.

8. Recall that a group G is said to act linearly on a vector space V if there is a group action of G on V such that the action of each element of G on V is linear. A subspace W of V is called invariant with respect to the given action if $g \cdot w \in W$ for every $w \in W$ and every $g \in G$. If the only invariant subspaces of G with respect to the action are (0) and V, then the action is called irreducible.

   (a) For any prime number p, construct a finite p-group G and a linear action of G on a real vector space V of dimension greater than 1 such that the action is irreducible.

   (b) In contrast, for any prime number p, let G be a finite p-group that acts linearly on a vector space V of dimension greater than 1 over the finite field $\mathbb{F}_p$. Prove that the action isn't irreducible. (Hint: Show that in fact V contains a one-dimensional invariant subspace.)

Algebra Prelim Fall 1995

Instructions: Try to do at least five problems. In general, four *complete* solutions will constitute a pass. One complete solution will count more that two partial solutions.

1. Let F be a field and let $F^\times$ denote the group of nonzero elements of F. Show that every finite subgroup of $F^\times$ is cyclic.

2. a) State the three Sylow theorems. b) Classify up to isomorphism all groups of order 12.

3. Let S_n denote the symmetric group on n elements. Let G be a finite group.

a) Show that there is a bijective correspondence between (i) the set of conjugacy classes of homomorphisms $G \to S_n$ and (ii) the set of isomorphism classes of finite left G-sets of cardinality n. (Two group homomorphisms $f, g : H \to K$ are *conjugate* if there is an element $\sigma \in K$ such $\sigma f(x)\sigma^{-1} = g(x)$ for all $x \in H$).

b) Take $G = S_3$. Using part (a), find a "formula" for the number of conjugacy classes of homomorphisms $G \to S_n$. Your formula should express this number in terms of certain partitions of n.

4. Let L be a Galois extension of a field F, with Galois group G. Let K be an intermediate field - that is, a subfield of L containing F. Let H denote the Galois group of L over K. Show that $N_G H = H$ if and only if $Aut_F K$ is the trivial group. ($N_G H$ denotes the normalizer of H in G.)

5. a) Prove that every non-unit in a commutative Noetherian integral domain is a product of irreducible elements.

b) Let A be a Noetherian unique factorization domain, $x \in A$ a nonzero element. Show that the subring $A[x^{-1}]$ of the fraction field of A is also a Noetherian unique factorization domain.

6. Let A be a commutative algebra over $\mathbb{C}$, of dimension $n < \infty$.

a) Show that $N = \{x \in A : x^n = 0\}$ is an ideal in A (note this is the same n)

b) Show that A/N is isomorphic as an algebra to a product of d copies of $\mathbb{C}$, where d is the dimension of A/N.

7. Let V be a finite-dimensional vector space over the field $\mathbb{R}$ of real numbers, and let $T : V \to V$ be an $\mathbb{R}$-linear map. Show that T has an invariant subspace (that is, a subspace $W \subset V$ such that $TW \subset W$) of dimension one or two.

8. Let $f(x)$ be an irreducible polynomial of degree 5 over $\mathbb{Q}$ that has exactly three real roots. Show that the Galois group of the splitting field of f over $\mathbb{Q}$ is the symmetric group S_5.

Fall 1994

Algebra Prelim

1. Let G be a group.

   (a) Define the notion of a (left) group action on a set.

   (b) Write down the class equation for a group action on a finite set.

   (c) Let $Z(G)$ be the center of G. Use the class equation to prove: if G is a finite p-group, and $N \neq \{1\}$ is a normal subgroup of G, then $N \cap Z(G) \neq \{1\}$.

2. Let K be a field of characteristic 0 which contains the nth roots of 1. Let F be an extension field of K and let $a \in K$. Show that if $a^n \in K$, then $[K(a):K]$ divides n. Give a counterexample when K does not contain the nth roots of 1.

3. Let R_o be a subring of R, both unique factorization domains. Suppose that they have the same group of units. Let a, b be nonzero elements of R_o. Let d_o (resp. d) denote their g.c.d. in R_o (resp. R).

   (a) Show that $d_o | d$ in R.

   (b) Show that d_o and d are associates in R if R_o is a PID.

   (c) Give an example where d_o and d are not associates.

4. A complex matrix A is unitary if $A\bar{A}^T = I$, i.e., if the inverse of A is its conjugate transpose. A real matrix C is orthogonal if $CC^T = I$, i.e., if it is real unitary. Show that each unitary matrix is diagonalizable by a unitary matrix. What will keep a real orthogonal matrix from being diagonalizable by a real orthogonal matrix?

5. Let G be a finite group with Sylow p-subgroups P and P' and with Sylow q-subgroups Q and Q'. Suppose that P normalizes Q and P' normalizes Q'. Show that there is an element g in G such that $gPg^{-1} = P'$ and $gQg^{-1} = Q'$.

6. Let $a_1, \ldots, a_n$ be elements of a principal ideal domain R. Show that there is an invertible $n \times n$ matrix with entries in R and with first row $(a_1, \ldots, a_n)$ if and only if $a_1, \ldots, a_n$ are relatively prime.

Hints: Recall that a free module is projective. For one direction, consider the R-module $R^n / R \cdot (a_1, \ldots, a_n)$ and use the structure theorem for PID's.

7. Let $I = (a)$ be a principal ideal in a commutative ring R with 1. Let P be a prime ideal contained in, but not equal, to I.

(a) Prove that P is contained in $\bigcap_{n \geq 1} I^n$.

(b) Give an example for $R = Z \oplus Z_2$ of such a $P \neq 0$ and $I \neq R$. (Z=ring of integers, Z_2 =ring of integers modulo 2.)

8. Let K be a field of characteristic other than 2 and let $K(x)$ be the field of rational functions in a variable x. Let G be the group of automorphisms of $K(x)$ generated by the automorphism determined by $x \mapsto -x$ and the automorphism determined by $x \mapsto \frac{1}{x}$. Find, as explicitly as you can, the fixed field of G.

ALGEBRA PRELIM
FALL 1993

1.

(a) State the Main Theorem of Galois Theory.

(b) Fix a prime p, let F be a subfield of C containing $\zeta = e^{2\pi i/p}$, and let $a \in F$ which is not a p^{th} power in F. Show that the splitting field of $f(x) = x^p - a$ has degree p over F, and its Galois group is cyclic of order p.

2.

(a) State Sylow's Theorems.

(b) Prove there is no simple group of order 148.

(c) Prove there is no simple group of order 56.

3. Let G be a group of order 400 with a normal subgroup H of order 100. What is the maximum number of subgroups that G could have containing H? What is the minimum possible number of such subgroups? Prove your answer in both cases and give examples to show these bounds are attained.

4.

(a) Let F_q be the finite field of order q, and $GL_n(F_q)$ the group of $n \times n$ invertible matrices over F_q. Show that $GL_n(F_q)$ acts transitively on the d-dimensional subspaces of F_q^n if $d \leq n$; that is, if S and T are two such subspaces then there is $g \in GL_n(F_q)$ with $g \cdot S = T$.

(b) Use the result of (a) and the formula

$$|GL_n(F_q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$$

to derive a formula for the number of d-dimensional subspaces of F_q^n in terms of d and n. You will also need the formula for the number of elements in an orbit in terms of the order of the stabilizer of any element of it.

5. As in problem No.4 let F_q be the finite field of *odd* order q. If q is prime, then it is well known that F_q has a square root of -1 if and only if q is congruent to $1 (\text{mod} 4)$. Using this fact, derive a general necessary and sufficient condition on q for F_q to have a square root of -1.

6. Give an example of a Galois extension K of Q, the field of rational numbers, with non-abelian Galois group. How many intermediate fields are there between Q and K?

7. Let R be a commutative Artinian ring. Show that every prime ideal of R is maximal.

8. Let R be a commutative ring with 1. Let

$$N = \{x \in R \mid x^n = 0 \text{ for some } n\}.$$

(a) Show that N is an ideal of R contained in every prime ideal.

(b) Using Zorn's Lemma, show that N is exactly the intersection of the prime ideals of R. (Hint: suppose the result is false, and x is a non-nilpotent element contained in every prime ideal, and consider the set $S = \{1, x, x^2, \ldots\}$.)

(c) If R is noetherian, show that N is nilpotent; i.e., that $N^m = 0$ for some m.

Algebra **Fall 1992**

Preliminary Examination

There are eight problems below. Attempt as many as you can, but keep in mind that complete solutions are considerably better than partial solutions.

1. Let H be a normal subgroup of a finite group G. Fix a prime number p and let P_0 be a p-Sylow subgroup of G/H.

a.) Prove there exists a p-Sylow subgroup P of G whose image in G/H is P_0.

b.) Prove that P is unique if H is in the center of G.

2. Fix a prime number p. Let G be an abelian group, and let

$$G^* = Hom(G, \mathbb{Q}/\mathbb{Z}_{(p)}).$$

Here Hom denotes the group homomorphisms and $\mathbb{Z}_{(p)}$ is the integers localized at p under addition; that is, $\mathbb{Z}_{(p)}$ is the set of fractions a/b where p doesn't divide b. Note that G^* is an abelian group under addition of functions. Define

$$\tau : G \longrightarrow G^{**}$$

by the formula

$$(\tau(g))(f) = f(g)$$

where $f \in G^*$.

a.) Prove that τ is an isomorphism of abelian groups if G is a finite abelian p-group.

b.) Is τ an isomorphism when $G = \mathbb{Z}_{(p)}$? Justify your answer.

3. This problem asks you to recover some of the theory of finite fields. Fix a prime number p and let $\mathbb{F}_p$ be the field with p elements. Then let $\mathbb{F}_{p^n}$ be a splitting field for

$$x^{p^n} - x \in \mathbb{F}_p[x].$$

a.) Prove that $\mathbb{F}_{p^n}$ has p^n elements; in fact, prove that $\mathbb{F}_{p^n}$ consists of exactly the roots of $x^{p^n} - x$.

b.) Prove that any field with p^n elements is a splitting field for $x^{p^n} - x$ and that a finite field is uniquely determined up to isomorphism by the number of its elements.

c.) Prove that the Galois group of the extension $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ is isomorphic to $\mathbb{Z}/n$, generated by the Frobenius $\phi(a) = a^p$.

d.) Prove that $\mathbb{F}_{p^n}$ is isomorphic to a sub-field of $\mathbb{F}_{p^k}$ if and only if n divides k.

4. Let E be a finite separable extension of a field F with $[E : F] = n$. Prove that there are at most 2^n fields K with

$$F \subseteq K \subseteq E.$$

5. Recall that two $n \times n$ matrices A and B over a field are similar if there is an invertible $n \times n$ matrix Q so that

$$A = QBQ^{-1}.$$

A partition of a positive integer n is a sequence of positive integers $n_1 \geq n_2 \geq \ldots \geq n_k$ so that

$$n_1 + \cdots + n_k = n.$$

Let $P(n)$ be the number of distinct partitions of n. For example, $P(4) = 5$.
Prove that up to similarity of matrices, there are exactly $P(n)$ $n \times n$ matrices A so that $A^n = 0$ (same n).

6. Let R be a subring of a commutative ring S. Recall that an element of S is integral over R if it is a root of a polynomial with coefficients in R that has leading coefficient 1. Then S is integral over R if every element of S is integral over R.

a.) Let S be a (commutative) integral domain and $R \subseteq S$ a subring so that S is integral over R. Prove R is a field if and only if S is a field.

b.) Let $R \subseteq S$ be an inclusion of commutative rings, with S integral over R. Then prove that a prime ideal $m \subset S$ is maximal if and only if $m \cap R \subset R$ is maximal.

7. This problem asks you to recover some of the theory of semi-simple rings.

a.) Let R be a ring, not necessarily commutative. A left ideal $L \subset R$ is simple if it has no non-trivial sub-left ideals. If L_1 and L_2 are two simple left ideals, prove that either $L_1 L_2 = 0$ or there is an R-module isomorphism $L_1 \cong L_2$.

b.) Let R be a semi-simple ring; that is, $\sum L = R$ where the sum is over all simple left ideals. If $L \subseteq R$ is a simple left ideal let

$$R(L) = \sum L'$$

where this sum is over all simple left ideals L' isomorphic to L as R-modules. Prove there is a *direct* sum decomposition of left R-modules

$$\oplus R(L) = R$$

where the direct sum is over the isomorphism classes of simple left ideals.

c.) Prove that if R is semi-simple there are elements $e_1, \ldots, e_n$, each e_i in some $R(L)$, so that

$$1 = e_1 + \cdots + e_n$$

and

$$e_i^2 = e_i \qquad \text{and} \qquad e_i e_j = 0 \quad \text{if} \quad i \neq j.$$

d.) Prove that the direct sum in b.) is finite; that is, that there are only finitely many isomorphism classes of simple left ideals.

8.a.) Let A be a commutative Noetherian ring. Suppose that for every non-unit $x \in A$ there is a positive integer n so that $x^n = 0$. Prove that if $I \subset A$ is an ideal and $I \neq A$, then there is a positive integer k so that $I^k = 0$.

b.) Does this conclusion hold if A is not Noetherian? Provide a proof or a counterexample.

Directions: Do as many problems as you can. Try for complete solutions.

Notation: $Z(G)$ = center of G. $N_G(A)$ = normalizer of A in G.

F_q = finite field of order q. $G(L/K)$ = Galois group of L over K.

$\mathrm{Tr}(T)$ = trace of T. $GL_n(K)$ = the group of $n \times n$ invertible matrices with entries in K.

1. How many conjugacy classes are there in a nonabelian group of order p^3, where p is a prime? Prove your answer. (It is a polynomial in p.)

2. Suppose G is a finite group, and suppose P is a p-Sylow subgroup of G. Suppose $x, y \in Z(P)$, and suppose x and y are conjugate in G. Show that x and y are conjugate in $N_G(P)$.

3. a) Show that $GL_n(F_q)$ has order $(q^n-1)(q^n-q)\ldots(q^n-q^{n-1})$. (HINT: How many possibilities are there for the first column of $A \in GL_n(F_q)$?)

   b) Determine the total number of 3×3 matrices over F_2 (not necessarily invertible) which are diagonalizable over F_2.

4. Suppose M is a finitely generated module over a principal ideal domain R, and suppose that for all $x \in M$, $\mathrm{ann}(x) = \{r \in R: rx = 0\} \neq \{0\}$. Suppose that $\phi: M \to M$ is an R-module endomorphism such that for all nonzero prime ideals P of R, the natural homomorphism $\overline{\phi}: M/PM \to M/PM$ is zero. Show that ϕ is nilpotent.

5. Suppose R is a commutative Noetherian ring with unit, and suppose that I is an ideal in R, with $I \neq R$. Show that there exists an $x \in R$ such that
$$P = \{r \in R : rx \in I\}$$
is a proper prime ideal in R.

6. Suppose V is a finite dimensional vector space over a field K, and suppose $T \in \mathrm{Hom}_K(V,V)$ and $f(x) \in K[x]$. Show that Λ is an eigenvalue of $f(T)$ if and only if $\Lambda = f(\lambda)$ for some eigenvalue λ of T. (Λ and λ may lie in extension fields of K.)

CONTINUED OVER →

7. Let K be a field of characteristic zero. Fix an integer $n \geq 2$ and assume

(*) K contains a primitive n^{th} root of unity.

a) Let L be an extension field of K obtained by adjoining an n^{th} root of some $a \in K$. Show that L is a Galois extension of K, with $G(L/K)$ cyclic of order dividing n.

b) Give an example showing that (a) is false without assumption (*).

8. Suppose K is a field of characteristic 0, and suppose that L is a finite Galois extension of K. If $a \in L$, denote by T_a the operation of multiplication by a (i.e. $T_a(b) = ab$), considered as a linear transformation from L, a vector space over K, to itself. That is, T_a is viewed in $\mathrm{Hom}_K(L,L)$.

a) Show that $\mathrm{Tr}(T_a) = \sum_{\sigma \in G(L/K)} \sigma(a)$.

b) Show that $\mathrm{Det}(T_a) = \prod_{\sigma \in G(L/K)} \sigma(a)$.

<u>Note</u>: The characteristic polynomial of T_a is $\prod_{\sigma \in G(L/K)} (x - \sigma(a))$.

If you use this result you must provide a proof. This may or may not be a good way to do the problem, depending on your approach. (There are several.)

Spring 1991

ALGEBRA PRELIM

Directions: Do as many problems as you can. Try for complete solutions.

1. Let $f(X) = c_nX^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$ be a polynomial with coefficients in a field. Let $A = (a_{ij})_{1\le i,j\le n}$ be the $n \times n$-matrix whose entry a_{ij} is the coefficient of X^{2i-j} in $f(x)$. Prove that A is nilpotent if and only if $f(X)$ is a constant.

2. Find an example of a degree 12 galois field extension of $\mathbf{Q}$ which is (a) cyclic, (b) non-cyclic but abelian, (c) non-abelian. In each case give your answer in the form $\mathbf{Q}(\alpha)$ or $\mathbf{Q}(\alpha, \beta)$ for some concrete α, β. No proofs are required in this problem.

3. Let G be a finite group and H a subgroup. Recall the definitions:

$$N(H) = \{g \in G \mid gHg^{-1} = H\}; \qquad C(H) = \{g \in G \mid hg = gh \text{ for all } h \in H\}.$$

Prove that if G is a finite simple nonabelian group of even order, then either
(i) 8 divides $|G|$, or
(ii) $N(P) = C(P)$ for every 2-Sylow subgroup, or
(iii) 12 divides $|G|$.

4. This problem concerns S_n, the symmetric group on n objects.
(a) Let G be a finite cyclic p-group (p a prime), and define $K = \min\{n \mid G \hookrightarrow S_n\}$. Prove that $K = |G|$.
(b) Let G be a finite cyclic group which is **not** a p-group. Show by an example that one can have $K < |G|$.
(c) Describe the conjugacy classes in S_4.

5. Let K be a field of characteristic not 2, and let G be the group of all 2×2-matrices with entries in K and determinant 1. Let $H_1 \subset G$ be the subgroup consisting of elements of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $a, b \in K$, and let $H_2 \subset G$ be the subgroup consisting of elements of the form $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$, $\alpha, \beta \in K$. Find a condition on K which is necessary and sufficient for H_1 to be isomorphic to H_2. In the case when this condition is fulfilled, construct an isomorphism between H_1 and H_2.

(CONTINUED ON NEXT PAGE)

6. Let R be a commutative ring with 1, $1 \neq 0$. Prove that there exists a polynomial $f(X) \in R[X]$ such that

$$f(r) = \begin{cases} 0, & \text{if } r = 0; \\ 1, & \text{if } r \in R \text{ is nonzero} \end{cases}$$

if and only if R is a finite field.

7. Let $\mathcal{P}(n) = \{\text{one-dimensional linear subspaces of } \mathbf{R}^n\}$, and let $SO(k) = \{k \times k \text{ real matrices } A \mid \|Ax\| = \|x\| \text{ for all } x \in \mathbf{R}^k, \text{ and } \det A = 1\}$, $k \in \mathbf{N}^+$. Define an action of $SO(n)$ on $\mathcal{P}(n)$, prove that the action is transitive, and show that it leads to the identification: $\mathcal{P}(n) = SO(n)/SO(n-1)$ as left $SO(n)$-sets.

8. (a) Let R be a commutative ring with identity which is Noetherian. Let M be a finitely generated R-module, and let $f : M \longrightarrow M$ be an onto R-homomorphism. Prove that f is an isomorphism.

(b) Give an example showing that without the assumption that M is finitely generated, an onto R-homomorphism $f : M \longrightarrow M$ is **not** necessarily an isomorphism.

Algebra Prelim **Fall 1990**

Directions: Do as many problems as you can. One complete solution is better than two partial solutions.

1. A commutative ring R has the descending chain condition if every decreasing chain of ideals $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$ has finite length.

   (a) Show that a commutative ring with the descending chain condition has only finitely many minimal prime ideals. (Actually, all its prime ideals are minimal prime ideals.)

   (b) Let $k[x]$ be the polynomial ring in one variable over a field k and let n be a positive integer. Does the ring $k[x]/(x^n)$ have the descending chain condition? Explain your answer.

   (c) What are the prime ideals of $k[x]/(x^n)$?

2. (a) Find a Galois extension field F of the rational field $\mathbb{Q}$ of degree 18.

   (b) For your extension F of $\mathbb{Q}$ in (a), what are all the intermediate fields? Which are Galois extensions of $\mathbb{Q}$?

3. (a) Find four non-isomorphic groups of order 66.

   (b) Show that the four groups in (a) are the only groups of order 66, up to isomorphism.

4. Let $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ be the space of real linear transformations from $\mathbb{R}^n$ to $\mathbb{R}$. Let $f_1, \ldots, f_m$ be elements of $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$. Define a symmetric bilinear form on $\mathbb{R}^n$ by $\langle X, Y\rangle = \sum_{i=1}^{m} f_i(X) f_i(Y)$, for $X, Y \in \mathbb{R}^n$.

   f_i

   Show that the form $\langle\ ,\ \rangle$ is non-degenerate if and only if $\{f_i\}_{i=1}^{m}$ spans $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$.

   (A symmetric bilinear form $\langle\ ,\ \rangle$ is non-degenerate if each non-zero vector X in $\mathbb{R}^n$ may be paired with a vector Y in $\mathbb{R}^n$ so that $\langle X, Y\rangle \neq 0$.)

TURN OVER →

5. Let G be a finite group of invertible linear transformations of $\mathbb{Q}^n$. Let $\{u_1, \ldots, u_m\}$ be a set of vectors in $\mathbb{Q}^n$ which G transforms transitively. Show that $\sum_{g \in G} g \cdot u_1$ is an integer multiple of $u_1 + \cdots + u_m$.

   (G transforms $\{u_1, \ldots, u_m\}$ <u>transitively</u> if $G \cdot u_1 = \{g \cdot u_1 | g \in G\}$ equals $\{u_1, \ldots, u_m\}$.)

6. Let $k[X, Y]$ be the polynomial ring in two variables X, Y over a field k. Let $R = k[X, XY, XY^2, \ldots]$ be the subring of $k[X, Y]$ that is generated by $\{XY^j\}_{j=0}^{\infty}$. Is R a Noetherian ring or not? Give a reason for your answer.

7. Let $n \geq 2$ be an integer. Let $\{e_1, \ldots, e_n\}$ be the standard basis for $\mathbb{R}^n$. The symmetry group G of the n-dimensional cube in $\mathbb{R}^n$ equals $S_n K = \{\sigma\tau | \sigma \in S_n, \tau \in K\}$ where S_n is the group of permutations of $\{e_1, \ldots, e_n\}$ and K is the group of sign changes of $\{e_1, \ldots, e_n\}$, i.e., $\sigma \in S_n$ transforms e_i to $e_{\sigma(i)}$ and $\tau \in K$ transforms each e_i to either e_i or $-e_i$.

   (a) Show which of the subgroups S_n, K is normal in G and which is not normal in G.

   (b) What is the order of K? What is the order of G? What is the structure of K? Explain your answers.

8. Let A and B be real $n \times n$ matrices.

   (a) Show that if A and B are skew-symmetric, then the commutator $[A, B] = AB - BA$ is also skew-symmetric.

   (b) Show that if A and B are symmetric, then the combination $(A, B) = AB + BA$ is also symmetric.

   (c) If A and B are symmetric, when is the commutator $[A, B] = AB - BA$ also symmetric?

ALGEBRA PRELIM SPRING 1990

Directions: Do as many problems as you can.
One complete solution is better than two partial solutions.

1. Let V be an n-dimensional vector space over a field of characteristic zero. Let $T : V \to V$ be a linear transformation. Suppose that T is idempotent (that is, $T^2 = T$).

   (a) Let $1 - T : V \to V$ be given by $(1 - T)\, x = x - Tx$ for $x \in V$. Prove that $1 - T$ is also idempotent.

   (b) Let W_1 = Image of T and W_2 = Image of $1 - T$. Prove that V is the direct sum of W_1 and W_2.

   (c) What are the possibilities for the minimal polynomial and the Jordan form of T?

2. Let G be a finite abelian group. For every $n \geq 1$, let $f_G(n)$ = the number of elements of G of order n. Prove that the function f_G determines G up to isomorphism.

3. (a) Let G be a finite p-group, where p is a prime. Let $\rho : G \to \mathrm{Aut}\,(V)$ be a homomorphism. (Here V is a finite dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$ with dimension ≥ 1. $\mathrm{Aut}\,(V)$ is the group of invertible linear transformations of V.) Prove that V contains a vector $v \neq 0$ such that $\rho(g)\, v = v$ for all $g \in G$.

   (b) Let G be a finite p-group. Let $n \geq 1$. Assume $G \subseteq GL_n(\mathbb{Z}/p\mathbb{Z})$. Let U = the group of triangular matrices with 1's on the main diagonal. Prove that $SGS^{-1} \subseteq U$ for some matrix $S \in GL_n(\mathbb{Z}/p\mathbb{Z})$.

4. Let R be a commutative ring with identity. Let I_1, I_2 be two ideals of R which are relatively prime in the sense that $I_1 + I_2 = R$. Let $I = I_1 \cap I_2$. Prove that there is a ring isomorphism $R/_I \cong (R/_{I_1}) \oplus (R/_{I_2})$

5. (a) Give an example of a field extension in characteristic zero, $F \subsetneq K$, such that $F \neq K$ but nevertheless the group of field automorphisms of K over F is trivial.

   (b) Suppose that $p(x) \in F[x]$ is an irreducible polynomial of degree > 1 and that K is the splitting field of $p(x)$ over F. Is the conclusion in (a) still possible? Prove your assertion.

   (c) Is the conclusion in (b) still true if $\operatorname{char}(F) \neq 0$? Give a proof or a counterexample.

6. Let R be a commutative ring with identity. Assume that R is noetherian.

   (a) Prove that every non zero ideal of R contains a finite product of non zero prime ideals of R.

   (b) Is the above statement true if the word prime is replaced by maximal? Give a proof or a counterexample.

7. Let K be the splitting field over $\mathbb{Q}$ for the polynomial $p(x) = x^5 - 3$.

   (a) Determine $[K:\mathbb{Q}]$.

   (b) Show that $\operatorname{Gal}(K/\mathbb{Q})$ is solvable by giving explicitly a sequence of subfields

$$F_0 = \mathbb{Q} \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_n = K$$

   so that $\operatorname{Gal}(F_{i+1}/F_i)$ is cyclic of prime order. ("Explicit" <u>means</u> give generators over $\mathbb{Q}$.)

8. There are five groups (up to isomorphism) of order 8 - three abelian groups, the dihedral group and the quaternionic group. For each group of order 8 find the smallest n so that there is an injective homomorphism $g : G \to S_n$.