Generators for abelian groups, and free abelian groups

0) Read pages 6-16 of my web notes 845 part1. [and the reference given there to the splitting criterion, in 844 part 2?]

1) prove: if A-->B--->C--->0 is an exact sequence of abelian groups, and if A and C are finitely generated, then so is B. [hint: use the images of some generators of A, and some choice of preimages of some generators of C.]

2) prove if 0--->A--->B--->Z^t--->0 is an exact sequence, then B is isomorphic to Ax(Z^t). [hint: if b1,...,bt are preimages of the standard generators of Z^t, then the map A x (Z^t) --->B induced by the given map A--->B, and by sending the generators of Z^t to the elements bi, should be an isomorphism. i.e. this "splits" the sequence above.

Give an example of an exact sequence 0--->Z^s--->Z^t----->C--->0 that does not split, and where Z^t is not isomorphic [by any map], to Z^s x C.

3) prove if 0--->Z^s--->K----->Z--->0 is an exact sequence, then there is a linearly indepedent generating set consisting of s+1 elements for K, and hence K is isomorphic to Z^(s+1).

4) Prove that Hom(Z^s, Q) is isomorphic as a Q - vector space to Q^s, by sending the map f:Z^S--->Q to the vector $(f(e_1),....,f(e_S))$. (and where we multiply maps by rational numbers by multiplying their values, to make Hom(Z^s,Q) into a Q vector space.) [hint: one proof would be to find a Q - basis for Hom(Z^s, Q), consisting of exactly s elements.]

5) Assuming the dimension of a Q vector space is well defined, use the result of 4, to deduce that Z^s cannot be isomorphic to Z^t unless s = t.

6) Prove that (Q,+) is not a free abelian group, i.e. is not isomorpic to a coproduct of either a finite or an infinite number of copies of Z. [hint: show that Hom(Q,Z) = {0}, but that Hom(G,Z) is not zero, if G is free abelian.]

This shows that (Q,+), the additive abelian group of all rationals, is quite diferent from (Q+, .), the multiplicative group of positive rationals. This may be one reason that statements like the famous Goldbach conjecture that every even number is the sum of at most 2 primes, i.e. statements which mix the two structures, are so difficult to prove.

Euclidean domains, Unique Factorization, Fin. gen. modules

Definition: A ring R is a "domain" if the only zero divisor is 0, we will also say R has "no" zero divisors.

Definition: A domain R is called "Euclidean" if there is a notion of "size", i.e. a function | |:R - {0}--->Z, whose values are bounded below, say by 0, such that after division, the remainder has smaller size. I.e. given a,b, in R with b not zero, there exist q,r, in R such that a = bq + r, and either r=0, or |r| < |b|.

Definition: A map of R modules f:M--->N is a homomorphism, or simply R mopdule map, iff it is a group map and preserves multiplication by scalars, i.e. f(ax) = af(x) for all a in R all x in M.

Assume R is a Euclidean domain.

Problem 1: Prove every ideal I in R is principal, i.e. is a cyclic module. (hint: If I contains non zero elements, choose one x of smallest size, and prove x divides all the other elements of I.) conclude that either I = {0}, or I is isomorphic to R.

problem 2: Prove every submodule of R^m is finitely generated, and in fact isomorphic to R^n where n is at most equal to m. hint: read the proof for Z.

problem 3: If M is any R module, and $x_1,...,x_m$ are any elements of M, prove there is a unique R module map f:R^m--->M taking ei to xi , where $e_1 = (1,0,...,0)$, $e_2 = (0,1,0,...,)$, etc.... Show moreover f is surjective if and only if the $\{x_i\}$ generate M and injective iff the $\{x_i\}$ are linearly independent over R.

problem 4. If M is a finitely generated R module, say with m generators, prove M is isomorphic to the cokernel of an R module map f:R^n--->R^m, where f can be given by an m by n matrix of elements of R.

problem 5. Prove every m by n matrix over R can be diagonalized by invertible row and column operations. hint: use induction on the "size" of the upper left entry of the matrix instead of on the number of prime factors.

problem 6: prove if f:M--->N is any R module map, and g:M--->M and h:N--->N are isomorphisms, then hfg:M--->N has kernel and cokernel isomorphic to those of f.

problem 7: Prove R^m/($Ra_1e_1x...xRa_me_m$) is isomorphic to (R/Ra_1) x...x (R/Ra_m).

problem 8: Conclude that if M is a finitely generated R module, with minimal set of generators $x_1,...,x_m$, then M is isomorphic to some product of form (R/Ra_1) x...x (R/Ra_m), where some a_i may be zero, but not units.

Clarification: In problem 7, the a_i are elements of R.
In problem 8, you may wish to prove first that if M is finitely generated by $x_1,...,x_m$, then M is isomorphic to some product of some cyclic modules R/Ra_i, and then afterwards prove that if m is the minimum cardinality of a set of generators, then none of the a_i is a unit.

Call a domain "strongly euclidean" if it is a euclidean domain with a size function | | satisfying the extra property that |ab| = |a| if b is a unit, and that |a| < |ab| and |b| > 0, if b is not a unit.

problem 9. prove that if a is a non zero, non unit, element, then a can be factored into at most |a| irreducible elements.

As remarked above, the proof of existence of factorization is harder for a p.i.d. than for a strongly euclidean domain. Thus if you are asked to prove that a general euclidean domain is a ufd, you have to work harder, but if your euclidean domain happens to be strongly euclidean, as many favorites examples are (rational integers, polynomials over a field, gaussian integers), it is easier.

Finitely generated abelian grps and k[X] modules

#1)a) Write down one abelian group of order n = (2^3)(3^4), in each isomorphism class. How many are there?

b) Write down one k[t] module V, in each k[t] isomorphism class, of k - dimension 7, and such that the subspace V(2) = {x in V: for some r, (t-2)^r .v = 0} has k dimension 3, and the subspace V(3) = {x in V: for some r, (t-3)^r .v = 0 } has k dimension 4. How many are there?

c) Write down one jordan matrix (over Q) in each "conjugacy" class, with char. polynomial (t-2)^3 (t-3)^4. how many are there?

#2) a) Write down all abelian groups of order 648 annihilated by 6 (always up to isomorphism).
b) Write down all k[t] modules of k dim'n 7, annihilated by (t-2)(t-3).
c) Write down all 7by 7 jordan matrices with min'l poly. (t-2)(t-3).

3) a) Find all abelian groups of order 2^3.3^4 with ker(2) ≈ Z/2 x Z/2, and ker(2^2) ≈ Z/2 x Z/2^2, i.e. ker (2) has dim 2 over Z/2, and ker(2^2)/ker(2) has dim 1 over Z/2, and ker(3) ≈ Z/3 x Z/3, and ker(3^2) ≈ Z/3^2 x Z/3^2, i.e. ker(3) has dim 2 over Z/3, and ker(3^2)/ker(3) has dim 2 over Z/3.

b) find all jordan matrices A with characteristic poly = (t-2)^3 .(t-3)^4, and ker(A-2) of dim 2, ker(A-2)^2 of dim 3, ker(A-3) of dim 2, and ker(A-3)^2 of dim 4. I.e. dim(ker(A-2)^2/ker(A-2)) = 1, dim(A-3) = 2, dim(ker(A-3)^2/ker(A-3)) = 2.

Find all abelian groups of order 648 = 2^3. 3^4, with annihilator 648.

Find all 7 by 7 jordan matrices over Q, with minimal polynomial

(t-2)^3.(t-3)^4.

#4) If k = Z/2Z, find all k[X] module structures on k^3 up to isomorphism (which extend the natural k module structure).

Jordan forms

Exercise 1) (i) Find all 5x5 Jordan matrices with $m(t) = (X-5)^{\wedge 2}$.
(ii) Find all 5x5 Jordan matrices with m(t) = (X-1)(X-3)(X+6).
(iii) Find all 6x6 Jordan matrices with $m(t) = (X-1)^{\wedge 2}(X-2)^2$.
(iv) Find the Jordan form of T, if the k[X] module (M,T) has invariant factors (X-1)(X-2), $(X-1)^{\wedge 3}(X-2)$, $(X-1)^{\wedge 3}(X-2)^{\wedge 2}(X-5)^{\wedge 3}$.

Exercise 2) (i) If A is a 3x3 matrix with $ch(t) = (X-4)^{\wedge 3}$, find all Jordan forms for A, each with its minimal polynomial.
(ii) If $ch(t) = \prod(X-t)^{m_t}$ is the characteristic polynomial of f:M-->M, prove every root of ch(t) is also a root of the minimal polynomial m(t), and if $M_t = \{v \text{ in } M: \text{ for some } r > 0, (T-t)^{\wedge r}(v) = 0\}$ is the primary subspace of M corresponding to the root t, prove that $\dim(M_t) = m_t$.
(iii) Use determinants to compute ch(t) for these matrices:

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \quad B = \begin{bmatrix} 3 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix}. \quad C = \begin{bmatrix} 1 & -1 & 4 \\ 3 & 2 & -1 \\ 2 & 1 & -1 \end{bmatrix}. \quad D = \begin{bmatrix} 1 & -2 & -1 & 0 \\ 1 & 0 & -3 & 0 \\ -1 & -2 & 1 & 0 \\ 1 & 2 & 1 & 2 \end{bmatrix}.$$

Exercise 3) Find the Jordan forms of these matrices:

$$\text{(i) } A = \begin{bmatrix} 0 & -1 & 2 \\ 3 & -4 & 6 \\ 2 & -2 & 3 \end{bmatrix}. \quad \text{(ii) } B = \begin{bmatrix} 2 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & -1 \\ 1 & 1 & 1 & 2 \end{bmatrix}. \quad \text{(iii) } C = \begin{bmatrix} 1 & 0 & -1 & 1 & 0 \\ -4 & 1 & -3 & 2 & 1 \\ -2 & -1 & 0 & 1 & 1 \\ -3 & -1 & -3 & 4 & 1 \\ -8 & -2 & -7 & 5 & 4 \end{bmatrix}.$$

Exercise 4): Find matrices Q which put each of the following matrices in upper (or lower) Jordan form over C:

$$\textbf{(i)} \quad A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \quad \textbf{(ii)} \quad B = \begin{bmatrix} 3 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix}. \quad \textbf{(iii)} \quad C = \begin{bmatrix} 1 & -1 & 4 \\ 3 & 2 & -1 \\ 2 & 1 & -1 \end{bmatrix}.$$

(ii) $D = \begin{bmatrix} 1 & -2 & -1 & 0 \\ 1 & 0 & -3 & 0 \\ -1 & -2 & 1 & 0 \\ 1 & 2 & 1 & 2 \end{bmatrix}$. **(ii)** $E = \begin{bmatrix} 5 & -1 & -3 & 2 & -5 \\ 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & -2 \\ 0 & -1 & 0 & 3 & 1 \\ 1 & -1 & -1 & 1 & 1 \end{bmatrix}$.

Noetherian rings, max'l ideals, rank of free f.g. modules

1. If R is a noetherian ring, prove every ideal I of R is contained in a maximal ideal without using Zorn's lemma.

2. If R is a noetherian ring and I any ideal, then R/I is noetherian too.

3. If R is a ring, 0--->A--->B--->C--->0 an exact sequence of R modules, prove B is noetherian if and only if both A and C are. [If A,C are fin. gen. prove C is too.] If N is a submodule of M, then N and M/N are both noetherian modules, if and only if M is.

4. If R is a noetherian ring, prove any fin gen R module M is noetherian.

5. If R is any ring, and I an ideal, R/I is a domain if and only if I is prime, and R/I is a field if and only if I is maximal.

6. If { Ij } is any linearly ordered indexed set of proper ideals in a ring R, i.e. if for any two ideals I_j and I_k, one is contained in the other, then their union is a proper ideal.

7. Using Zorn's lemma, prove in any ring R, that every ideal I of R is contained in a maximal ideal .

8. If f:R--->S is a ring map, I an ideal of S, then $f^{-1}(I)$ is an ideal of R, the induced map $R/f^{-1}(I)$--->S/I is injective, and $f^{-1}(I)$ is prime if I is.

9. If f:R--->S is a ring map, I an ideal of R, f(I) may not be an ideal of S. If f is surjective, f(I) is an ideal of S, and sending I to f(I) gives a 1-1 correspondence between ideals I of R containing kerf, and all ideals of S.

10. For an R module M, and ideal I, let IM be the submodule generated by all products rx, with r in I, x in M. Prove $R^{\wedge n}/IR^{\wedge n}$ is isomorphic to $(R/I)^{\wedge n}$ as R modules, and as R/I modules. If $R^{\wedge n} \approx R^{\wedge m}$, deduce n = m, assuming it holds when R is a field.

"Normality" (integral closure) of rings

Assume R is a noetherian domain if helpful.
Definition: A polynomial is monic if it has leading coefficient 1.
An element of the fraction field K of a domain R is integral over R if it is the root of a monic polynomial in R[X].
A domain R is normal, or integrally closed, if the only elements of K that are integral over R are elements of R.

Further properties of ufd's.
Exercise1: Any ufd is normal. [hint: look at the proof of the "rational root" theorem from precalculus.]

Exercise2: In a ufd R, prove all "minimal" prime ideals are principal. I.e. if the only prime ideal contained in P is {0}, then P is principal.

Exercise3,4,5: If R is a ufd in which all non zero prime ideals are minimal, prove R is a pid. (see DF, problem 6, parts a,b,c, page 283.)

Definition: If R is a domain, the fraction field K, of R, is defined as the set of all formal quotients {x/y: x,y are in R, and $y \neq 0$}, subject to the equivalence relation, x/y = a/b iff xb=ay. This is a field containing an isomorphic copy {x/1: x is in R} of R.

Localization of rings
Definition: If R is a domain and P a prime ideal, the "partial" fraction ring R_P, called "the localization of R at P", is the following subring of K.
R_P = {x/y in K such that y is not in P}. Since P is prime, the product of two such fractions is another such fraction.

Fact: If R is a normal noetherian domain, then for all minimal primes P of R, the localization R_P is a pid, in particular PR_P is principal in R_P. This is weaker than the analogous property for a ufd, but both allow us to define the order of the zero or pole of a rational function along a subvariety of codimension one.

Exercise6: Prove that the ideal PR_P generated by P in R_P is maximal, and that all elements of R_P not in this ideal are units. Conclude that there is only this one maximal ideal in R_P. [R_P is called a "local ring".]

Example: If k is a field, and R = k[X,Y] is the ring of polynomial functions on the affine plane k^2, then (X,Y) = P is a maximal, hence prime, ideal consisting of polynomial functions vanishing at the point (0,0). Then R_P is the ring of those rational functions which are defined at (0,0), i.e. whose denominators do not vanish at (0,0).

Exercise7: If R is normal, P prime, prove R_P also normal.

Exercise 8: If R is ufd, P prime, prove R_P also ufd.

Sylow subgroups

1. Imitate the proof we gave today for the number of sylow subgroups to prove that if #G = m(p^r) where p does not divide m, and if Q is any subgroup of G of order p^s where s < r, then Q is contained in some sylow subgroup of order p^r. [We proved the case where s= r in class. The point is to let Q act on the set of sylow subgroups by conjugation, prove there is a fixed point, and Q is contained in the fixed sylow group.]

2. Prove every group G of order 45 is abelian. [Prove both sylow subgroups H,K of G are normal. Then prove that G is a direct product HxK. Deduce that every group of order 45 is abelian, and write down all of them, up to isomorphism.]

3. Prove no group of order 182 is simple.

4. If the "normalizer" N(H) of a subgroup H of G, equals N(H) = {those g in G such that gHg^(-1) = H, and if P is a sylow subgroup of G, prove N(N(P)) = N(P).

Def: A group G is called "solvable" if there exists a sequence of subgroups
G = H1, ...,Hn = {e}, such that

a) each H(i+1) is a normal subgroup of Hi, and
b) each quotient Hi/H(i+1) is abelian.

A sequence with a) is called a subnormal tower, or just a normal tower, and one with a), b) is called an abelian subnormal tower. So a solvable group is one with an abelian subnormal tower. [These groups are called solvable because the Galois group of a polynomial which is solvable by radicals, has this property, as we will see later.]

5. If p,q are distinct primes prove
i) every group of order pq is solvable.
ii) every group of order (p^2)q is solvable.

6. Prove S(n) is not solvable if n > 4, assuming S(5) ≈ Icos.

7. i) Prove the number of fixed points for the action of a p - group on a finite set is congruent mod p, to the cardinality of the set.
ii) if P, P' are any two sylow subgroups of a group G, using only part i), and nothing else, except that P, and P' exist, prove P is conjugate to P' by looking at an action of P' on the set G/P of cosets of P in G.

8. i) If P is a sylow subgroup of S(2p), prove P is abelian.
ii) Prove it for p > 3, and P a sylow p-subgroup of S(3p).
iii) Prove it for p > n, P a sylow p-subgroup of S(np).

9. Determine how many sylow subgroups exist for each prime, in the group GL3(Z/2) of

invertible 3 x 3 matrices over Z/2.
In fact, learn everything you can about this group: the order of the group, the number of elements of each order, the number of sylow subgroups of each order. find all possible characteristic polynomials for elements of this group, and for each characteristic polynomial, find all rational forms having this polynomial, and jordan forms if they exist.

Actually find elements of each order, and find elements in each conjugacy class. Note whether any elements of the same order fail to be conjugate. Note that there is exactly one (invertible) rational form for each conjugacy class of elements in the group, i.e. two matrices have the same rational form if and only if they are conjugate.

You may use all three tools we have to study this group, jordan forms, rational forms, and the fact that it acts linearly on the vector space (Z/2)^3, hence on the 7 point projective plane, carrying lines to lines.

Try to prove this group is simple, along the lines of the proof we gave for Icos, i.e. use conjugacy classes, [but they are harder to compute].

10. Prove that if G is a finite group such that p^s divides #G, then G has a subgroup, of order p^s.
hint: use induction, and the center of a group of order p^r is non trivial.

Cycles in S(n), and commutators

A k- cycle represents the action of a permutation on an orbit with k elements. Within a cycle, action is from left to right, i.e. (123) takes 1 to 2, and 2 to 3, and 3 to 1, (cyclically, 1 is to the right of 3). For consistency with DF, we compose cycles like functions, i.e. (123)(345) means first (345), then (123). so the composition is (123)(345) = (12345), while (345)(123) = (12453).

1. Prove if s is any permutation in S(n), and $(a_1a_2...a_k)$ is the cycle taking a_1 to a_2, etc,..., then $s(a_1a_2...a_k)s^{-1} = (s(a_1)s(a_2)....s(a_k))$.

2. Prove disjoint cycles commute, i.e. if no a_i equals any b_j, then $(a_1a_2...a_r)(b_1b_2...b_s) = (b_1b_2...b_s)(a_1a_2...a_r)$.

3. Prove S(n) is generated by 2 - cycles: **Hint**: $(a_1a_k)(a_1a_2...a_{k-1}) = (a_1a_2...a_k)$.

4. Prove S(n) is generated by these 2 - cycles (12), (13), (14),....,(1n).
Hint: (1i)(1j)(1i) = (ij).

5. Let $f(X) = \prod_{i<j} (X_i-X_j)$, and let S(n) act on $Z[X_1,...,X_n]$ by permuting the indices of the variables. E.g. if n = 3, (12) sends $f(X) = (X_1-X_2)(X_1-X3)(X_2-X3)$ to $(X_2-X_1)(X_2-X3)(X_1-X3) = -f(X)$. **Deduce** that every permutation m takes f to either f or -f, and that setting sgn(m) = c, where m(f) = c.f, defines a surjective homomorphism S(n)-->{±1}, whose kernel is those

permutations which can be written as a product of an even number of 2 - cycles. Call that subgroup A(n).

6. Prove A(n) is generated by 3 - cycles. **Hint**: If a,b,c, d are all different, (ac)(ab) = (abc), (cd)(ab) = (abc)(bcd).

7. Prove, for a subgroup H of S(n), that setting j ≈ k if and only if the 2 - cycle (jk) belongs to H, defines an equivalence relation on {1,2,...,n}.

8. Prove if H is a transitive subgroup of S(n), any two of the equivalence classes defined in #6 have the same number of elements. Hence a transitive subgroup of S(p) where p is prime, either contains no 2 - cycles, or all 2 - cycles. Thus a transitive subgroup of S(p) containing one 2 cycle, e.g. a subgroup containing a 2-cycle and a p-cycle, is all of S(p). **Hint:** use problems 6,7.

Define the commutator of x,y to be the element $xyx^{-1}y^{-1}$, and note x and y commute iff their commutator is 1. The commutator subgroup G' of G is the subgroup generated by all commutators. The commutator of the commutator is denoted $G^{(2)}$, and so on,...,$G^{(k)}$.

Defn a subgroup H of G is a characteristic subgroup iff f(H) = H for all automorphisms f of G. In particular H characetristic implies H normal.

9. Prove the commutator subgroup G' of G is a characteristic subgroup, hence normal, that G/G' is abelian, and if a homomorphism f:G-->K exists where K is abelian then ker(f) contains G'.

10. Prove G is solvable iff some repeated commutator $G^{(n)} = \{e\}$.

Galois groups

Work these prelim problems
1) #1 sep 1997,
2) #7 march 1998,
3) #4 fall 1998,
4) #8 presumably spring 1999 (just before fall 1999), typeset by ams tex;
5) #8 spring 2000
6) #5 jan 2001,
7) #8 jan 2004,
8) #5 august 2004,
9) #4 jan 2006,
10) #6 jan 2006.

1. i. Prove the polynomial f(X) = X^2 + X + 1 is irreducible over k = Z/2 and hence the quotient k[X]/(f) defines a field of 4 elements.

ii. Prove the splitting field of X^2+X+1 over Z/2 has dimension 2, hence the galois group is Z/2, a solvable group, but prove the polynomial is not "solvable by radicals", i.e. the root field is not a radical extension.

2. Find an irreducible cubic polynomial mod 5, and hence construct a field with 125 elements.

3. Find 2 different irreducible cubic polynomials mod 5, hence 2 different realizations of the unique field with 125 elements. can you find an isomorphism between them?

4, 5, 6, 7, 8: Work problems 14, 15, 16, 17, page 557 of DF, and then deduce cor 28, p. 600, that every finite abelian group occurs as the galois group over Q of some subextension of a cyclotomic extension.

FACT: If f is an monic polynomial of degree n over Z, and which is separable mod p, with irreducible factors mod p of degrees a,b,....,c, then the galois group of f over Q, as a subgroup of S(n), contains a cycle with decomposition of type a,b,....,c.

E.g. If f is a monic quintic and factors mod p into an irreducible quadratic times an irreducible cubic, then G(f), as a permutation of the 5 distinct roots of f over Q, contains a cycle like (12)(345).

9. Show X^5 - X - 1 is irreducible and separable mod 3.

10. Show X^5 - X - 1 factors mod 2 into an irreducible quadratic and an irreducible cubic. Show there is also a transposition, and deduce that the galois group over Q is S(5).

8000 Fall 2006 Midterm, Do as many problems as you can.

1a) State Zorn's lemma.
b) Prove that in a commutative ring R with identity 1, that if x is any non unit, there exists a proper maximal ideal of R containing x.

2a) Prove every principal ideal domain R has "unique factorization".
b) Give an example of a ring with unique factorization that is not a principal ideal domain. (You do not have to prove it.)

3a) State the classification theorem for finitely generated modules over a Euclidean domain, and give a brief sketch of the main steps of the existence proof.
b) Give an explicit example of one abelian group in each isomorphism class of abelian groups of order 360.

4a) If f:M--->M is a surjective endomorphism of an R module, that is not injective, prove that {ker(f^n)}, n = 1,2,3,.... is a strictly increasing sequence of submodules.
b) What can you conclude about a surjective endomorphism of a noetherian module?

5) State and prove the Cayley - Hamilton theorem.

6) a) Compute both the characteristic and the minimal polynomials, and also the Jordan form J of this matrix:

$$A = \begin{bmatrix} -1 & 1 & 0 & 0 & 0 \\ -4 & 3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix}$$

You do not need to find a matrix Q such that $Q^{-1}AQ = J$.

b) Write the matrix J as the sum of a diagonal matrix, plus a nilpotent matrix.

Math 8000 Fall 2006, Final exam.

DEFINITIONS

A. Define what is meant by:
i) a normal subgroup of a group G.
ii) a Sylow subgroup of G.
iii) a simple group.
iv) a left action of a group G on a set S.
v) the semi direct product group defined by a homomorphism
c:H-->Aut(K).

B. Assume k is a subfield of a field E, and c an element of E.
Define what is meant by:
i) c is algebraic over k.
ii) the minimal polynomial of (an algebraic element) c over k.
iii) E is separable (algebraic) over k (give 2 characterizations).
iv) E is normal (algebraic) over k (give 2 characterizations).
v) E is an algebraic closure of k.
vi) the galois group $Gal_k(E)$, (i.e. $Aut_k(E)$).

STATEMENTS

C. i) State all 3 parts of Sylow's theorem.

and, ii) State the Jordan Holder theorem.
(and prove one of them.)

PROOFS

D. Prove One:
Either i) There are no non abelian groups of order 9, and only one non abelian group of order 10.
OR ii) Icos (or A(5)) is a simple group.

E. Prove One:
Either i) If k is a field and E a finite dimensional extension field (as k vector space), then E is algebraic over k.
OR ii) If k is a field and f a polynomial of degree ≥ 1 in k[X], there is a field E containing k in which f has at least one root.

F. Prove One:
Either i) Every field k has an algebraic closure.
OR ii) If E is an algebraic field extension of k (not necessarily finite), and F is an algebraically closed field containing k, there is a field homomorphism E-->F which is the identity on k.

G. Prove One:
Either i) If E is a finite Galois extension of k, the map from subgroups of $Gal_k(E)$ to fields intermediate between k and E, taking a subgroup to its fixed field, is surjective.
OR ii) If $c_1,...,c_r$ are the primitive nth roots of 1 contained in the complex field, then the "cyclotomic" polynomial $f_n = \prod(X-c_i)$, i =1,..,r, lies in Z[X] and is irreducible over Q.

H. Prove One:
Either i) Every real symmetric matrix is orthogonally diagonalizable,
OR ii) The Cayley Hamilton theorem. Say what your hypotheses are.

PROBLEMS
I. Do all parts: For each of the following polynomials over Q:
a) Prove the polynomial is irreducible over Q.

b) Say as much as you can about the splitting field E, i.e. the degree over Q, whether or not it is a solvable extension, whether it is contained in R, and compute the Galois group as well as you can.

c) Say whatever you can about those intermediate fields between E and Q which are normal over Q.

i) $X^3 - 3X + 1$,
ii) $X^5 - 20X + 4$,
iii) $X^7 - 2$.