Handout # 1 July 12,2000

GENERAL REMARKS ON GENERAL EXAMS

1) **You do not need to answer all questions** on the general exam; passing grades vary from exam to exam, but anyone getting 66% of the questions right is almost sure to pass.

2) **You do not need to answer the questions completely** – partial credit is given. However, it will have serious repercussions on your grade if you don't do a single problem correctly all the way through.

3) **Write what you know**: relevant definitions, theorems. This is a good way to start attacking a problem, and will show you know the basic material even if you don't discover the tricks needed to get the answer.

4) **Write the truth, the whole truth, but nothing but the truth** – it is a much more serious sin to state something that is false than not to state anything at all.

5) **Write clearly** – the proctor will gladly give you extra time to rewrite your answers (it makes grading infinitely easier).

SYLOW QUESTIONS

Know the 3 parts to the Sylow Theorem: if $|G| = p^e m$ for $(p, m) = 1$ a *p-Sylow subgroup* is any subgroup P with $|P| = p^e$.

(I) p-Sylow subgroups exist

(II) any two are conjugate

(III) the number n_p of them is congruent to 1 mod p, and divides m.

(The number is exactly the *index of the normalizer* of any particular P, $n_p = [G : N_G(P)]$).

Know the 3 principal methods of proving a group is NOT SIMPLE:
(1) **Simple Sylow Count**: use (III) to show the number of p-Sylows is 1. **Basic fact**: any conjugate of a Sylow subgroup is Sylow, so *if for some p there is only one p-Sylow subgroup, it must be a* **proper** *normal subgroup* [recall that $|G| = p^e$ implies G is nilpotent, hence solvable, hence not simple (even if $|G| = p$, by convention)]. Examples: $|G| = 1776$ [Sep 83 # 1], 1989 [Jan 89 # 1], 1995 [Jan 95 # 1; show G solvable], 1001 [Aug 95 # 2; show G abelian, cyclic], 200 [Aug 88 #4 ;1985 #1a]; $n = 20, 28, 44, 52; n = p^e m$ for $p > m$. What can you say about simple groups of order $n = 2^m + 1$? $n = 2.3.5$? $n = 2^2.3.5$? [Jan 98 # 1b].

(2) **Small Index**: show $|G|$ does not divide $n_p!$ for some prime p, eg p^e doesn't divide $(m - 1)!$ [Reason: G acts transitively on set $\mathcal{P}$ of p-Sylow subgroups by conjugation, so by simplicity either G imbeds (i) faithfully in $Symm(\mathcal{P})$ of size $n_p!$, so $|G| \mid n_p! \, |m!$, or G imbeds (ii) trivially, in which case by transitivity there would be only one P, contrary to the Basic Fact]. Examples: $|G| = 24, 36, 48; 72$ [Jan 87 #1, Sep 84 #1] .

(3) **Element Count**: Use (III) to get estimates on $n_p > 1$ for the relevant p's, and count how many elements there are of order p^k for the various k and p [crucial: two subgroups of prime order p can overlap only in one element; the answer

is not so simple for Sylow subgroups of higher order p^k], and show the number of elements would be $> |G|$. Examples: $|G| = 30, 56$.

RELATED PROBLEMS

(1) A group of order p^k is nilpotent.

(2) [May 90 #2] A group of order 441 is solvable.

(3) [Sep 86 #2] Find ALL groups of order 99.

(4) [Nov 77 #7] Must a group of order 70 be abelian? Solvable? Can you say anything about its normal subgroups?

(5) [Jan 98 # 1a] What can you say about groups of the following orders n? (Give reasons, making free use of any theorems you know.) (a) $n = 2^4 + 1$. (b) $n = 2^3 + 1$.

(6) [Sep 82 #6] If G is nonabelian of order 21, show it is generated by elements s, t with $s^7 = t^3 = 1, t^{-1}st = s^2$.

(7) [Aug 98 #1ab] Let G be a finite group of order $3 \cdot 5 \cdot 17$. Show that the Sylow 17-subgroup is normal. *If there exists an element of order* 15 *in* G, show that the Sylow 3- and 5-subgroups are also normal. [Hint: show they are properly contained in their normalizers.]

(8) If G and its normal subgroup N have the same power of p, then all p-Sylow subgroups of G live in N; if one is normal in N, then it is the unique p-Sylow subgroup of G.

(9) [January 82 # VIIa, May 89 #8, Sep 93 # 3] If a normal subgroup N of G contains a Sylow subgroup P of G, then $G = N.N_G(P)$.

(10) [Fall 87 #1] If G of order 160 has two distinct subgroups of order 80, then G has a normal subgroup of order 5.

(11) [August 98 #1c] If all Sylow subgroups of a finite group G are normal and abelian, show that G itself is abelian.

(12) [January 81 #5, Sep 78 #3] If G of order 60 has exactly 4 elements of order 5, there is a proper normal subgroup.

(13) [May 92 # 3] Prove $V = \{1, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of the symmetric group S_4 on 4 symbols, and that $S_4/V \cong S_3$.

(14) [Jan 92 # 4] If a finite group G has a normal p-Sylow subgroup P, then $\phi(P) \subseteq P$ for every endomorphism ϕ of G.

(15) [Jan 94 # 4] Let $f : G \longrightarrow H$ be a surjective homomorphism of finite groups, and let p be a prime. (a) Prove that if P is a p-Sylow subgroup of G, then $f(P)$ is a p-Sylow subgroup of H. (b) Prove that every p-Sylow subgroup of H has the form $f(P)$ for some p-Sylow subgroup P of G.

(16) [Aug 94 # 1] Let P be a p-Sylow subgroup of a finite group G, p a prime dividing the order of G. (a) Prove that P consists of all the p-torsion elements of the normalizer $N_G(P)$, that is, all elements of $N_G(P)$ whose order is a power of p. [Hint: apply Sylow to $N_G(P)$.] (b) Prove that P is a characteristic subgroup of $N_G(P)$, that is, is invariant under all automorphisms of $N_G(P)$. (c) Prove that $N_G\big(N_G(P)\big) = N_G(P)$.

(17) [Aug 96 # 8] Give an example of two finite groups whose Sylow subgroups are isomorphic for each prime, but which are not themselves isomorphic.

(18) [Jan 97 # 6] Let P be a p-Sylow subgroup of a finite group G. Prove that if H is a subgroup of G, then for some $g \in G$, $H \cap gPg^{-1}$ is a p-Sylow subgroup of H.

(19) [May 91 # 4b] If G is a group of order 231, show the 11-Sylow subgroup H of G is normal in G and lies in the center of G. (Hint: Let G act on H by conjugation.)

Handout #2 July 15, 2000

2. GENERAL GROUP QUESTIONS

GENERAL GROUP KNOWLEDGE

1) **Know basic definitions**: groups (sub-, normal, quotient or factor, simple, abelian, solvable, nilpotent, commutator); morphisms (homo, iso, mono, epi, auto, inner); order, index, center; group action, transitive, orbit, fixed point.

2) **Know the 3 parts of the Fundamental Theorem of Homomorphisms**:

(I) If $f : G \longrightarrow G'$ is a group homomorphism then $G/Ker(f) \cong Im(f)$ via the mapping $\bar{f}(\bar{x}) = f(x)$ ($\bar{x} = \pi(x) =$ the coset of x)

(II) The subgroups of $\bar{G} = G/N$ are in 1-1 correspondence with the subgroups of G containing N under $H \to \pi(H)$, $\bar{H} \to \pi^{-1}(\bar{H})$; normals correspond to normals, and $\bar{G}/\bar{H} \cong G/H$.

(III) If $H < G$, $K \lhd G$ then $H/H \cap K \cong HK/K$.

3) **Know Lagrange's Theorem**: $|G| = [G : H]|H|$, so $|H|, order(x) \mid |G|$.

4) Know all subgroups of $\mathcal{Z}$ ($m\mathcal{Z}$ for $m \geq 0$), of $\mathcal{Z}_n$ ($m\mathcal{Z}_n \cong \mathcal{Z}_{n/m}$ for $m \geq 1, m|n$); **know all automorphisms** $Aut(\mathcal{Z}) = \{\pm 1\}$, $Aut(\mathcal{Z}_n) = \mathcal{Z}_n^* = \{f_k : x \longrightarrow x^k \text{ for } (k,n) = 1\ \}$.

5) **Know** S_n : order $n!$, cycle decomposition of permutations, conjugation.

6) **Know Group Actions**: If G acts on S then (I) S is disjoint union of orbits, (II) $|orbit(s)| = [G : Fix(s)]$; (III) class equation; (IV) $|conjugacy - class(x)| = [G : C(x)]$; (V) if G is p-group, $|fixed - points| \equiv |S| \bmod p$.

NOTES ON SEMI-DIRECT PRODUCTS

Given groups G, N with an action of G on N by automorphisms (a homomorphism $G \xrightarrow{\sigma} Aut(N)$), we form the group $G \overset{\sigma}{\rtimes} N$ (the triangle indicates N will be a normal subgroup) which is just $G \times N$ as a set, but with product twisted via σ (in comparison to the direct product, where the product is merely componentwise)

$$(g_1, n_1) \odot (g_2, n_2) = (g_1 g_2, \sigma(g_2^{-1})(n_1) n_2).$$

Properties: (1) the subgroup $G \times 1 \cong G$ is naturally isomorphic to G; (2) the subgroup $1 \times N$ is normal, and the automophisms $\sigma(g)$ become inner, $\sigma(g)(n) = g \odot n \odot g^{-1}$; (3) G and N generate $G \overset{\sigma}{\rtimes} N$.

Characterization: a given group $\tilde{G}$ is isomorphic to $G \overset{\sigma}{\rtimes} N$ for *some* σ iff (1) G is a subgroup $G < \tilde{G}$, (2) N is a normal subgroup $N \lhd \tilde{G}$, (3) G, N disjointly generate $\tilde{G}$: $GN = \tilde{G}, G \cap N = 1$. In this case $\sigma(g) = \hat{g}|_N$ is is restriction to N of conjugation by g. This insures that semidirect products appear frequently.

Example: $G \times N = G \overset{\sigma}{\rtimes} N$ for trivial $\sigma = 1$.

Example: the affine maps of calculus form a semidirect product $(\mathcal{R}^*, \cdot) \overset{\sigma}{\ltimes} (\mathcal{R}, +)$ under $\sigma(a)(x) = a \cdot x$: the map $(a, b) \longrightarrow \alpha_{a,b} = \delta_a \tau_b : x \longrightarrow a \cdot (x + b)$ is an isomorphism, since $\alpha_{a_1,b_1} \circ \alpha_{a_2,b_2} = [a_1 a_2](x + [a_2^{-1} b_1 + b_2])$.

Affine Realization of the Semidirect Product

You can think of $G \overset{\sigma}{\ltimes} N$ as "affine maps" of some big group $\tilde{G}$ containing G, N on which G conjugates via σ on N but "non-centrally" on $\tilde{G}$ $(\hat{g}(n) = \sigma(g)(n),\ \hat{g} = 1$ on $\tilde{G}$ implies $g = 1$ in $G)$ since then $(g, n) \longrightarrow \hat{g} \circ L_n$ is a bijection $G \overset{\sigma}{\ltimes} N \longrightarrow \hat{G} \circ L_N$, and it is a homomorphism from the relations $\hat{x}\hat{y} = \widehat{xy},\ L_x L_y = L_{xy},\ \phi L_x \phi^{-1} = L_{\phi(x)}$ for any elements x, y and any automorphism ϕ of any group. We can write this *additively* : $G \overset{\sigma}{\ltimes} N$ is isomorphic to the affine transformations $\alpha_{g,n} = \delta_g \tau_n$ for $\delta_g(x) = \hat{g}(x) = gxg^{-1},\ \tau_n(x) = n + x$.

PROBLEMS

(1) [May 78 #1] Name a nonabelian simple group.

(2) [Jan 79 #8] Do the elements of finite order in a group always form a subgroup?

(3) [May 89 #5] If H, K are subgroups of G show G is a disjoint union of double cosets HgK.

(4) [Feb 84 #7] If H, K are subgroups of G with $Ha = Kb$ for some a, b in G, prove $H = K$. What can you say if $aH = Kb$?

(5) [Jan 89 #2] (a) If G has a normal subgroup N with $G/N = \mathcal{Z}$, show for all $n \neq 0$ there is a normal subgroup N_n with $G/N_n = \mathcal{Z}_n$. (b) If all proper factor groups G/N of G are finite, must G be finite?

(6) [Aug 89 # 1] State the class equation for a finite group, and use it to show $C(G) > 1$ for a nontrivial p-group G, then prove G is nilpotent.

(7) [May 78 # 2] If a finite p-group G acts linearly on a finite-dimensional vector space over $\mathcal{Z}_p$, show G has a nonzero fixed point.

(8) [Aug 95 # 1] Let G be a finite group of permutations of a finite set X. For $x \in X$ let $G_x = Stab(x) = \{g \in G \mid gx = x\}$. If $|X| = [G : G_x]$ for some $x \in X$, show the same holds for *all* $x \in X$.

(9) [Jan 82 #VIIb,c] The *Frattini subgroup* F of G is defined to be the intersection of all maximal subgroups of G. Show (a) F is normal in G, (b) if G is finitely generated then F is inessential $(G = FH \Longrightarrow G = H)$, (c) if F contains a p-Sylow subgroup of G then that subgroup is normal.

(10) A member g of a group G is called a *nongenerator* of G is whenever G is generated by a subset containing g, it is also generated by the subset with g removed. It is a fact that the set of all nongenerators of G forms a subgroup, the *Frattini subgroup* of G. If F is the Frattini subgroup of a finite p-group G (p a prime), show that $g \in F$ iff g is in every subgroup of index p of G. (You may use the fact that if H is a proper subgroup of G, then H is a proper subgroup of its normalizer $N_G(H)$). Conclude that G/F is an abelian group of exponent p.

(11) [Sep 86 # 6] For what n is $S_n \longrightarrow Aut(S_n)$ (via $g \longrightarrow \hat{g}$ conjugation by g) a monomorphism?

(12) [March 83 # 3] Show that S_8 contains a subgroup H of order 15, but S_n for $n < 8$ doesn't.

(13) [April 77 # 5] (a) Show the alternating group A_n is normal in S_n. (b) Show A_n is generated by all 3-cycles $(12k)$ for $k = 3, 4, \ldots, n$. (c) Show any normal subgroup of A_n which contains a 3-cycle must be all of A_n.

(14) [Jan 94 # 6] (a) Explain why the inner automorphism group of the alternating group A_n is isomorphic to A_n for $n \geq 4$. (b) Prove that for $n \geq 3$, A_n has outer automorphisms.

(15) [May 90 # 1] If G has no nontrivial automorphisms, prove it has order 1 or 2.

(16) [Jan 87 # 2] If G is infinite but some nontrivial element $x \neq 1$ has only a finite number of conjugates, show G is not simple.

(17) [Jan 92 # 7, Jan 95 # 2] Apply the Jordan-Hölder-Schreier Theorem on composition series to a finite cyclic group of order n to prove that n has a unique factorization as a product of primes.

(18) [May 92 # 5] Use the subgroup structure of the cyclic group of order $n \geq 1$ to show that $n = \sum_{d|n} \phi(d)$, where the Euler ϕ-function $\phi(n)$ is the number of integers $1 \leq k \leq n$ which are relatively prime to n.

(19) [Jan 95 # 5] Give definitions of the terms "maximal subgroup" and "minimal subgroup" ; it is not assumed that you have seen these terms previously. Then from your definitions, prove the following facts: (a) A minimal subgroup must be cyclic of prime order. (b) If a subgroup has prime index, it is a maximal subgroup. (c) If a subgroup is both maximal and normal, it has prime index. (d) A subgroup of an abelian group is maximal if and only if it has prime index. (e) Find all maximal and minimal subgroups of $\mathcal{Z}$.

(20) [Aug 95 Comprehensive # 7] Find the order of the group $GL(n, \mathcal{Z}_p)$ and describe one of its p-Sylow subgroups.

(21) [Aug 98 #2] Let $GL_2(p)$ for a prime p denote the group of invertible 2×2 matrices over the finite field F_p of p elements. (a) Find the order n of the group $GL_2(p)$. (b) For λ in F_p, and $B := \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$, find the order m of the subgroup

$$G_\lambda := \{A \in GL_2(p) \mid ABA^{-1} = B\}.$$

(c) Find how many 2×2 matrices over F_p are similar to the matrix B. [Hint: express it in terms of m and n.]

(22) [Aug 96 # 1] A *Hall subgroup* H of a finite group G is a subgroup whose order and index are relatively prime. Use isomorphism theorems to prove that if N is a normal subgroup of G and H is a Hall subgroup of G, then HN/N is a Hall subgroup of G/N, and $H \cap N$ is a Hall subgroup of N.

(23) [Aug 97 # 2] (a) Prove that if G is a finite group with exactly two conjugacy classes of elements, then $|G| = 2$. (b) If G has exactly three conjugacy

classes of elements, show that $|G|$ involves at most two primes. (c) There are, in fact, only two finite groups with exactly three conjugacy classes of elements. Can you guess which ones they are?

(24) [Sep 93 # 7] A well-known puzzle has tiles numbered 1 to 15 in 4 rows of 4 each, with the (4,4) square empty. An allowable move consists of sliding a tile adjacent to the empty square horizontally or vertically into the empty square. If a sequence of moves ends up with the empty square back at (4,4), prove the resulting permutation π of the numbers 1 to 15 belongs to A_{15}.

Handout #3 July 18, 2000

3. ABELIAN GROUP QUESTIONS

ABELIAN GROUP KNOWLEDGE

1) **Know basic definitions**: Free abelian, rank, torsion, direct sum, elementary divisor, invariant factor; composition series, composition factors. Jordan-Holder Theorem.

2) **Know the Fundamental Theorem of Finitely Generated Abelian Groups**: [*Elementary Divisor Form* (longest decomposition into cyclics)] $A = \mathcal{Z}_{p_1^{e_1}} \oplus \ldots \oplus \mathcal{Z}_{p_r^{e_r}} \oplus \mathcal{Z}^n$ where the rank n and the number of summands of type $\mathcal{Z}_{p^e}$ (the elementary divisors) are invariants [A is cyclic iff $n = 1$, no elementary divisors or $n = 0$, elementary divisors have distinct primes]. [*Invariant Factor Form* (shortest decomposition into cyclics)] $A = \mathcal{Z}_{d_1} \oplus \ldots \oplus \mathcal{Z}_{d_s}$ for $d_1 \mid d_2 \mid \ldots \mid d_s$ where the invariant factors $d_i \geq 0$ are invariants [$d = 0$ is allowed (free summands) but not $d = 1$; A is cyclic iff $s = 1$].

3) **Know How to Count**: the number of non-isomorphic finite abelian groups of order $n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ is $\mathcal{P}(e_1)\mathcal{P}(e_2)\ldots\mathcal{P}(e_r)$ for $\mathcal{P}(e)$ = number of partitions of the exponent e (the number of ways of writing $e = f_1 + \ldots + f_s$ for $1 \leq f_1 \leq \ldots \leq f_s$).

4) **Know How to Decompose**: (I) Write $A = F/K$ for F free on N generators $\{x_1, \ldots, x_N\}$ with M relations $B\vec{x} = \vec{0}$ (ie. $b_{i1}x_1 + \ldots + b_{iN}x_N = 0$ for $i = 1, 2, \ldots, M$). (II) Rewrite equations $B \longrightarrow UB$ for elementary U (elementary row operations), change basis of free module F by $B \longrightarrow BV$ for elementary V (elementary column operations), until reach diagonal form $Diag d_1, \ldots, d_N$ with $d_1 \mid d_2 \mid \ldots \mid d_N$. (III) Then $F = \bigoplus \mathcal{Z}_{y_i}$, $K = \bigoplus \mathcal{Z}_{d_i y_i}$, $A = F/K = \bigoplus \mathcal{Z}/\mathcal{Z}_{d_i} = \bigoplus_{d_i \neq 1} \mathcal{Z}_{d_i}$.

5) **Know how to go back and forth between Invariant Factors and Elementary Divisors**: $InvFac \longrightarrow ElDiv$ by factoring each $d_i = \prod p_{ij}^{e_{ij}}$, $ElDiv \longrightarrow InvFac$ by $d_N = \prod p_i^{\text{highest } e_i}$, $d_{N-1} = \prod p_i^{\text{next highest } e_i}$, etc.

COUNTING PROBLEMS

Describe (up to isomorphism) all abelian groups of order: [May 91 # 4a] 4851; [85 #1c] 2334; [Aug 88 #4] 200; [Jan 87 #1] 72; [Feb 84 #1] 1984; [Sep 80 #1] 80; [May 80 #1] 375.

How many non-isomorphic abelian groups are there of order: [Sep 83 #1] 1776, [Jan 98 # 2a] 360.

RELATED PROBLEMS

(1) [Mar 83 #6] Show a finite abelian group is cyclic iff it has no subgroup isomorphic to $B \oplus B$ for $B \neq 0$.

(2) [Aug 98 #1d] If G is a finite abelian group of order $p \cdot q \cdot r$ for distinct primes p, q, r, show that G is cyclic.

(3) [May 78 #6] Give an example of a torsion-free group which is not free. Can you give an example which is finitely generated?

(4) [April 77 #3] Use the Fundamental Theorem of Finite Abelian Groups to show the multiplicative group of the ring $\mathcal{Z}_{p^n}$ for prime $p,\ n > 1$ has a subgroup of order p.

(5) [Aug 89 #6] Find the structure of all abelian groups generated by 3 elements a, b, c satisfying relations $-4a + 2b + 6c = 0,\ -6a + 2b + 6c = 0,\ 7a + 4b + 15c = 0$.

(6) [Jan 98 # 2] Take the free abelian group on three generators x, y, z, and divide by the relations $2x + 4y + 5z = 0,\ 6x + 8y + 10z = 0,\ 8x + 12y + 20z = 0$. Write the resulting group as a direct sum of cyclic groups.

(7) [Aug 95 # 3] Find the order of the abelian group generated by x, y, z subject to the relations $4x - 2y + 4z = 0,\ 7x - 8y + z = 0,\ 8x + y + 13z = 0$.

(8) [Jan 97 # 2] Let G be a finite abelian group of order k. Use the fact that the map $g \longrightarrow g^n$ (n an integer) is a homomorphism, to show that if K_n is the number of solutions of $g^n = 1$ in G, and $k^{(n)}$ is the number of n-th powers in G, then $k = k_n\, k^{(n)}$.

(9) [Aug 96 # 2] Determine all pairs of positive integers a, b with $a \leq b$ such that $\mathcal{Z}_a \times \mathcal{Z}_b$ is isomorphic to $\mathcal{Z}_{15} \times \mathcal{Z}_{18} \times \mathcal{Z}_{20}$.

(10) [Aug 94 # 2] If G is a finite abelian group of order n, show that G has a subgroup of order d for each divisor d of n. Show that this need not be true if G is not abelian.

(11) [Jan 92 # 1] Show that an infinite abelian group is cyclic iff every nonzero subgroup has finite index.

(12) [May 92 # 1] Show that an abelian group has a composition series iff it is finite.

(13) [Sep 82 #3] Describe all finite abelian groups having EXACTLY 3 composition series.

(14) [Sep 79 #4] Find all composition factors for $\mathcal{Z}_4 \times \mathcal{Z}_5$, and exhibit composition series for them.

(15) [Aug 98 #3] For an abelian group A, the *dual group* A^* is defined to be $Hom(A, U)$ where the *circle group* U is the multiplicative group of complex numbers of modulus 1 (the unit circle in the complex plane). Here $Hom(A, B)$ denotes the abelian group of homomorphisms of A into B (under $(f + g)(a) = f(a) + g(a)$); you may use the additivity property $Hom(A_1 \oplus A_2, B) \cong Hom(A_1, B) \oplus Hom(A_2, B)$ and the isomorphism property that if $A \cong A', B \cong B'$ then $Hom(A, B) \cong Hom(A', B')$. (a) Prove that Z_n^* is cyclic of order n. (b) Prove that A^* is isomorphic to A for *any* finite abelian group A.

Handout #4 July 21, 1999

4. RING QUESTIONS

GENERAL RING KNOWLEDGE

1) **Know basic ring definitions**: Ring (sub-, quotient or factor, artinian, noetherian, division, polynomial $R[X]$, power series $R[[x]]$, matrix $M_n(R)$); ideal (maximal); field; invertible element, multiplicative group (group of units).

2) **Know: Fundamental Theorem of Homomorphisms for Rings.**

3) **Know**: finite domain is a division ring; quaternions as example of a division algebra which is not a field.

4) **Know**: Universal property of polynomial ring $R[X]$ (any homomorphism $f : R \longrightarrow S$ and "evaluation map" $g : X \longrightarrow S$ extend uniquely to homomorphism $R[X] \longrightarrow S$.

5) **Know**: Zorn's Lemma (Given a subset S of R not containing 0, there exists an ideal or one-sided ideal M maximal with respect to $S \cap M = \emptyset$; if S is finite there exists M maximal with respect to $S \not\subseteq M$).

COMMUTATIVE RING KNOWLEDGE

1) **Know basic commutative ring definitions**: Principal or prime ideal; domain (integral, Euclidean, PID, UFD); element (unit = invertible, irreducible, prime, integral over a subring); two elements (divides, associates, gcd, lcm).

2) **Know 3 basic examples of PIDs**: $\mathcal{Z}$, fields F, polynomials $F[x]$.

3) **Know the basic relations between Euclidean, Principal, and Unique Factorization Domains**: Euclidean $\Longrightarrow$ PID $\Longrightarrow$ UFD, R UFD $\Longrightarrow R[x]$ UFD, but R PID $\not\Longrightarrow R[x]$ PID by the 2 basic non-PIDs $\mathcal{Z}[x], F[x,y]$.

4) **Know Hilbert's Basis Theorem**: R noetherian $\Longrightarrow R[x]$ noetherian.

5) **Know**: I maximal $\Longleftrightarrow R/I$ field, I prime $\Longleftrightarrow R/I$ domain.

6) **Know**: All ideals, images of $\mathcal{Z}_n$; $\mathcal{Z}_p$ is a field with $a^p = a$ and $a^{p-1} = 1$ $(a \neq 0)$.

7) **Know Eisenstein's Criterion** for irreducible polynomials in $\mathcal{Z}[x]$.

8) **Know Gauss' Lemma**: if R is UFD with quotient field F, then nonconstant irreducible f in $R[x]$ remains irreducible in $F[x]$; equivalently the content satisfies $c(fg) = c(f)c(g)$.

9) **Know Euclidean algorithm** for finding gcd of two elements in a Euclidean ring.

COMMUTATIVE RING PROBLEMS

(Unless otherwise stated, all rings R are commutative with unit 1; F denotes a field.)

(1) [1985 #3c] If a, b are relatively prime integers, show the ring $\mathcal{Z}_{ab}$ is isomorphic to the direct sum $\mathcal{Z}_a \oplus \mathcal{Z}_b$ of rings. Show (in ≤ 1 word) why this implies if $m = p_1^{e_1} \dots p_t^{e_t}$ that $\mathcal{Z}_m$ is isomorphic to $\mathcal{Z}_{p_1^{e_1}} \dots \mathcal{Z}_{p_t^{e_t}}$.

(2) [May 92 # 2] If a, b in an integral domain R satisfy $a^n = b^n,\ a^m = b^m$ for m and n relatively prime, show $a = b$.

(3) [Feb 84 #3] If R is finite, show every prime ideal is maximal.

(4) [Sept 93 # 2] If P is a prime ideal which is *not* maximal, show P has infinitely many cosets in R.

(5) [May 1990 #5] If R is an integral domain with only finite number n of ideals, show R is a field, and give an upper bound for n.

(6) [Jan 92 # 6] Prove that an integral domain has the descending chain condition on ideals iff it is a field.

(7) [Jan 94 # 8] Let ZD denote the set of zero divisors of R (including 0). Let $\mathcal{I}$ be the set of ideals of R which are contained in ZD. (a) Show that if M is a maximal member of $\mathcal{I}$, then M is a prime ideal. (b) Use Zorn's Lemma to show that each member of ZD is contained in a maximal member of $\mathcal{I}$. (c) Conclude that the set ZD is a union of prime ideals.

(8) [Jan 82 #6] If I is an ideal of R with $I \cap S = \emptyset$ for some multiplicatively closed subset S of R containing 1, show there exists an ideal M of R containing I and maximal with respect to $M \cap S = \emptyset$. Find an M if $R = \mathcal{Z},\ S = \{3^n \mid n \neq 0\},\ I = 2\mathcal{Z}$.

(9) [Sep 78 # 6] R is called a *local ring* if it has a unique maximal ideal; a domain is called a *valuation domain* if for every two elements a, b either a divides b or b divides a. (a) Show R is local iff the non-units form an ideal M. (b) Show every valuation domain is local. (c) Show a local ring has no idempotents ($e^2 = e$) other than 1,0.

(10) [Aug 97 # 8] (a) Show that the set N of all nilpotent elements z ($z^n = 0$ for some n) of R forms an ideal (called the *nil radical* of R). (b) The intersection J of all maximal ideals of R is called the *Jacobson radical* of R; show that $N \subseteq J$. (d) Give an example where N and J are different.

(11†) [May 89 # 7; Aug 97 # 8c] Show an element $a \in R$ belongs to $J = \bigcap\{\text{maximal ideals of } R\} \iff 1 + ra$ is a unit for all $r \in R$.

(12) [May 78 # 5] Is the ring $C[0, 1]$ of continuous real-valued functions on the closed interval [0,1] noetherian?

(13) [Sep 79 # 7a; Nov 77 # 5] Give two examples of non-noetherian rings.

(14) [May 80 # 2] Hilbert's Theorem says that $F[x_1, \dots, x_n]$ is noetherian. Show that ANY finitely generated commutative F-algebra A is noetherian.

(15) [Aug 88 # 7] Prove that every rational number which is integral over the integers $\mathcal{Z}$ is already in $\mathcal{Z}$.

(16†) [Fall 87 # 3] Show that a complex number a is an algebraic integer iff $\mathcal{Z}[a]$ is a finitely generated $\mathcal{Z}$-module.

UFD PROBLEMS

(1) [Sep 80 #2] (a) Give 3 examples of PIDs. (b) Show that the homomorphic image of a PIR (Principal Ideal Ring: all ideals are principal, but perhaps not a domain) is again a PIR. (c) Give an example of a PID with a homomorphic image which is not a PID.

(2) [Aug 88 #1] If F is a field, PROVE $F[x]$ is a PID.

(3) [Jan 81 #4] (a) SHOW $F[x]$ is a Euclidean domain, but $F[x, y]$ is *not.*

(4) [Jan 79 #2; May 91 # 2a] (a) SHOW that any Euclidean domain is a PID. (b) Show that any two nonzero elements have a g.c.d. in R. (c) Find (systematically) m, n so that $421m + 1664n = 1$.

(5) [Jan 89 #6] Prove or disprove: Every UFD is a PID.

(6) [May 91 #2b] Prove or disprove: R Euclidean domain $\Longrightarrow R[x]$ Euclidean domain and/or any two nonzero elements of $R[x]$ have a g.c.d. in $R[x]$.

(7) [Fall 87 #2] Prove or disprove: R PID $\Longrightarrow R[x]$ is PID.

(8) [Jan 87 #5] If R is an integral domain, what are necessary and sufficient conditions that $R[x]$ be: (0) a domain, (1) a PID, (2) a UFD, (3) noetherian.

(9) [Jan 98 # 3] Let R be a PID. If a, b are two nonzero elements in R, show that they have a l.c.m. (an element $m \in R$ such that (1) $a, b \mid m$, (2) if $a, b \mid x$ then $m \mid x$.)

(10) [Aug 96 # 5] Let R be a PID. An ideal P of R is called *primary* if whenever $ab \in P$ and $a \notin P$ then $b^n \in P$ for some n (depending on b). Show that P is primary iff either $P = 0$ or $P = (p^m)$ form some prime $p \in R$ and some exponent m.

(11) [Aug 95 # 4] Show that $\mathcal{Z}[\sqrt{10}] = \mathcal{Z} + \mathcal{Z}\sqrt{10}$ is not a UFD. [Hint: show that a) $n^2 - 10m^2 \neq 2, 3$ for all $n, m \in \mathcal{Z}$, b) 2,3, and $4 \pm \sqrt{10}$ are primes in $\mathcal{Z}[\sqrt{10}]$.]

(12†) [Sept 93 # 5] (a) Let D be a Euclidean domain, with Euclidean function δ (but do not assume $\delta(ab) \geq \delta(a)$). Let $D_n = \{a \in D \mid a \neq 0 \text{ and } \delta(a) \geq n\}$. Show that (1) if $b \in D_0$ and there exists an $a \in D$ such that $a + Db \subseteq D_n$, then $b \in D_{n+1}$; (2) $\bigcap_n D_n = \emptyset$. (b) Conversely, show that if an integral domain D has a chain of subsets $D \backslash \{0\} = D_0 \supseteq D_1 \supseteq D_2 \supseteq \ldots$ satisfying properties (1) and (2), then D is Euclidean.

(13†) Let R be an integral domain, $N : R\backslash\{0\} \longrightarrow \{n > 0 \mid n \in \mathcal{Z}\}$ be a function for which (i) $N(1) = 1$ and (ii) $N(xy) = N(x)N(y)$ for all x, y in $R\backslash\{0\}$. (1) Let K be the field of fractions of R. Show that N can be extended in a unique way to a function from $K\backslash\{0\}$ into Q that still satisfies $(i), (ii)$. (b) Show that R is a Euclidean domain under N iff for each $x \in K\backslash\{0\}$ there is an element $r \in R$ for which $N(x - r) < 1$.

(14) [Jan 92 # 2] Show that a polynomial of degree n over F has at most n roots in F.

(15) [Jan 97 # 4] Give counterexamples for each of the following statements, with details. Then corect each statement by modifying the underlined part. (a) If R is a $\underline{\text{commutative ring}}$, then a polynomial in $R[x]$ of degree n has at

most n roots in R. (b) If R is a division ring, then a polynomial in $R[x]$ of degree n has at most n roots in R. (c) If R is a unique factorization domain, then the greatest common divisor d of two members a, b of R can be written as $d = ax + by$ for some x and y in R.

(16) [Aug 98 # 10] If F denotes a field and Z the ring of integers, decide which of the following rings are PIDs and which are UFDs (no proofs are necessary):

$$F,\ Z,\ Z[x],\ F[x,y],\ F[[x]]\ \text{(formal power series)}.$$

(17) [Jan 89 #3] Let $R = F[[x]]$ be the ring of formal power series in one variable x over the field F. (a) Find the units of R. (b) Show each nonzero $f \in R$ is an associate of a power x^n for some $n \geq 0$. (c) Find all irreducible elements of R. (d) Show all ideals of R have the form Rx^n for some n. (e) Describe all finitely generated R-modules.

(18) [April 77 #4] (a) If M is a maximal ideal, SHOW R/M is a field. (b) If R is a Euclidean domain, show every ideal generated by an irreducible element is maximal.

(19) [Sep 79 #7b] Given an example of a prime ideal in R which is *not* maximal; is there an example where R is a UFD?

(20) [Jan 95 # 6] Prove that any proper homomorphic image of a PID that remains an integral domain must actually be a field.

(21) [May 1990 #4] If P is a nonzero prime ideal in a UFD, show P is minimal among nonzero prime ideals iff P is a principal ideal.

(22) [August 98 # 5] The *Krull dimension* of a commutative ring R is the longest chain of prime ideals properly contained in R, i.e. the largest integer n such that there exists a chain $P_0 < P_1 < \ldots < P_n < R$ ($P_0 = 0$ allowed if prime) of *prime ideals* P_i in R. If R is a PID, find its Krull dimension.

(23) [Sep 83 #7] If $R \subseteq S$ are PIDs with $d = gcd_R(a,b)$, show $d = gcd_S(a,b)$ too.

(24) [Mar 83 #5] If D is a UFD whose units together with 0 form a proper subring U, show D has infinitely many (nonassociate) primes. Give an example of such a D.

(25†) [Sep 82 #2] If $a_1, \ldots, a_n$ in a PID R have gcd d, show that there exists an invertible $n \times n$ matrix Q of determinant 1 over R with $Q\,[a_1, \ldots, a_n]^T = [d, 0, 0 \ldots 0]^T$. (This is false if R is merely a UFD).

(26†) [Aug 89 #4] Show $R = \{f(x) \in \mathcal{Z}[x] \mid$ the coefficient of x in $f(x)$ is even $\}$ is a subring. Show that 2 and $2x$ have a g.c.d. in R, but not a l.c.m.

(27) [Mar 83 #8] Does 7 divide 1031 + 3110 ? Why?

(28) [Aug 94 # 3] Describe which polynomials in $\mathcal{R}[x]$ belong to the subring $\mathcal{R}[x^2, x^3]$, $\mathcal{R}$ the field of real numbers.

(29) [Feb 84 # 5] Factor $x^3 - y^3$ into irreducible factors in $Q[x,y]$.

(30) [Jan 94 # 3] Prove that $y^3 + x^2y^2 + x^3y + x$ is irreducible in $\mathcal{Z}[x,y]$.

(31) [1985 # 3a] Show $x^5 - 6x^3 + 12x^2 + 21x - 3$ is irreducible in $Q[x]$.

(32) [Aug 96 # 4] In $Q[x]$, let $f(x) = x^{m_1} + \ldots + x^{m_k}$ where $m_i \equiv i - 1 \pmod{k}$. Show that $f(x)$ is divisible by $x^{k-1} + x^{k-2} + \ldots + 1$.

(33) [Aug 95 Comp. # 5] Factor $x^9 - x$ in $F_3[x]$ into irreducible factors (F_3 the Galois field of three elements).

NONCOMMUTATIVE RING QUESTIONS

(R here is a not-necessarily-commutative ring with unit 1)

(1) [Aug 89 # 2] If $(a+b)^2 = a^2+b^2$ for all a, b in R, show R is commutative.

(2) [Sep 86 # 7] (a) Define the quaternions H over the reals. (b) Show that any homomorphism of H into the complex numbers is identically zero. (c) Prove that the equation $x^2+1=0$ has infinitely many solutions in H.

(3) [1985 # 3d] An element of R is nilpotent if $x^n = 0$ for some n. Show that if x, y are commuting nilpotent elements in R then so is $x+y$; give an example to show this is not true if x, y do not commute.

(4) [Sep 84 # 2] Let L be a left ideal in R. (a) Show $I(L) := \{a \in R \mid La \subseteq L\}$ is the largest subring S of R such that L is a 2-sided ideal of S. (b) Prove that R is a division ring iff $I(L) = L$ for all nonzero L.

(5)[Aug 98 #5] A *derivation* D of a ring R is a map of R into itself such that

$$\begin{array}{ll} D(a+b) & = D(a)+D(b) \\ D(ab) & = D(a)b + aD(b) \end{array}$$

for all elements a, b of R. Show that if D is a derivation, and in addition $D^2 = 0$ and R has no 2-torsion ($2a = 0$ implies $a = 0$), then the "exponential map" $Id + D$ is an *automorphism* of R.

(6*) [Nov 77 # 9] (a) Show that R satisfies the a.c.c. on left ideals iff all its left ideals are finitely generated. (b) Prove that any finitely generated left R-module satisfies the a.c.c. on (left) submodules if R does.

(7†) [Nov 77 # 10] Let F be a field of characteristic $p > 0$. A *p-polynomial* is a polynomial $f(x) = a_n x^{p^n} + \ldots + a_1 x^{p^1} + a_0 x^{p^0} = a_n x^{p^n} + \ldots + a_1 x^p + a_0 x$ which is a linear combination of p^e-th powers of x ($e = n, .., 1, 0$). If $a_n \neq 0$ then f has *degree n.* (a) Show that the set R of all p-polynomials becomes a non-commutative ring under the usual addition and the substitution product $f(x) * g(x) = f(g(x))$. Does R have a unit element? What are the zero divisors? (b) Show that every left ideal I in R is principal, $I = Rf$. (c) Show that every right ideal of R is principal iff the field F is perfect ($F^p = F$). (d) Are there any perfect fields F for which R is commutative?

(8) [May 89 # 2] Show that in a general rng (not necessarily commutative or with unit), all the elements that are not divisors of zero have the same additive order. What are the possible values for this order?

(9) [Jan 94 # 5] Give an example (and a proof that it works) of a ring R without identity and an ideal in the ring direct sum $R \oplus R$ that does *not* have the form $I_1 \oplus I_2$ where the I_k are ideals in R.

Handout # 5 July 23, 1999

5. MODULE QUESTIONS

GENERAL MODULE KNOWLEDGE

1) **Know basic definitions**: R-module: left, right, bi, sub, quotient, free, direct sum and product, cyclic, simple [irreducible], indecomposable, noetherian [a.c.c], artinian [d.c.c].

2) **Know: Fundamental Theorem of Homomorphisms**.

3) **Know**: Composition series, composition factors, Jordan-Hölder Theorem.

4) **Know**: $\{R$-module structure on an abelian group $(M,+)\} = \{$ ring homomorphism $R \longrightarrow End(M,+)\}$.

5) **Know**: All modules for $R = \mathcal{Z},\ F,\ F[x]$.

KNOWLEDGE OF MODULES OVER A PID

1) **Know basic definitions**: elementary divisors, invariant factors, torsion, torsion-free, annihilator ideal.

2) **Know the Fundamental Theorem of Finitely Generated Modules over a PID**. *Elementary Divisor Form* (longest decomposition into cyclics): $M = R/(p_1^{e_1})\oplus\ldots\oplus R/(p_r^{e_r})\oplus R^n$ where the rank n and the number of summands of type $R/(p^e)$ (the elementary divisors) are invariants [M is cyclic iff $n=1$, no elementary divisors or $n=0$, elementary divisors have distinct primes]. *Invariant Factor Form* (shortest decomposition into cyclics): $M = R/(d_1)\oplus\ldots\oplus R/(d_s)$ for $d_1 \mid d_2 \mid \ldots \mid d_s$ where the invariant factors d_i are invariants [$d=0$ is allowed (free summands) but not $d=$ unit; M is cyclic iff $s=1$].

3) **Find invariant factors of a matrix** B over a Euclidean domain: Do elementary row and column operations until reach diagonal form $Diag\{d_1,\ldots,d_N\}$ with $d_1 \mid d_2 \mid \ldots \mid d_N$.

4) **Know How to Decompose**: (I) Write $M = F/K$ for F free on N generators $\{x_1,\ldots,x_N\}$ with M relations $B\vec{x} = \vec{0}$ (ie. $b_{i1}x_1 + \ldots + b_{iN}x_N = 0$ for $i = 1,2,\ldots,M$). (II) Find invariant factors of relation matrix B: Rewrite equations $B \longrightarrow UB$ for elementary U (elementary row operations), change basis of free module F by $B \longrightarrow BV$ for elementary V (elementary column operations), until reach diagonal form $Diag\{d_1,\ldots,d_N\}$ with $d_1 \mid d_2 \mid \ldots \mid d_N$. (III) Then $F = \bigoplus Ry_i$, $K = \bigoplus Rd_iy_i$, $M = F/K = \bigoplus R/(d_i) = \bigoplus_{d_i\neq\text{unit}} R/(d_i)$.

PROBLEMS

Counting Problems : Describe (up to isomorphism) all R-modules over a specific R with given specific annihilator. [SEE ABELIAN GROUPS AND JORDAN CANONICAL FORM]

(1) [Sep 84 # 6] Find the invariant factors of the following 3×3 matrices over $\mathcal{Z}$, and decide if they are equivalent: $\begin{pmatrix} 10 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 6 \end{pmatrix}$, $\begin{pmatrix} 4 & 6 & 4 \\ 4 & 20 & 12 \\ 20 & 0 & 20 \end{pmatrix}$.

(2) [Aug 97 # 7] Let M be the free module over $Q[x]$ with basis $v_1, v_2, v_3,$ N a submodule with basis w_1, w_2, w_3 where $w_1 = (x^3-x^2-x+1)v_1+(2x^2+2x)v_2+(x^3+x^2)v_3,$ $w_2 = (2x^3-3x^2-3x+2)v_1+(5x^2+5x)v_2+(2x^3+2x^2)v_3,$ $w_3 = (x^3-x)v_1+(x^2+x)v_2+(x^3+x^2)v_3$. (a) There is a theorem which implies that M has another basis u_1, u_2, u_3 for which d_1u_1, d_2u_2, d_3u_3 are a basis for N for some $d_1, d_2, d_3 \in Q[x]$ such that $d_1 \mid d_2 \mid d_3$. Write a carefully worded statement of this theorem, giving all appropriate hypotheses and conclusions. (b) Find the values d_1, d_2, d_3 for the example given here.

(3) [May 91 # 6] Let $M = \mathcal{Z} \oplus \mathcal{Z}$ be the free module of rank 2 over the ring $\mathcal{Z}$ of integers. Let S be the submodule of M spanned by $x = (3,0),$ $y = (0,4),$ $z = (6,2)$. Find a $\mathcal{Z}$-basis for the submodule S.

(4) [Aug 98 # 4] Let a, b, c be distinct elements of an integral domain D. Show that there are *unique* elements x, y, z in D such that

$$\begin{array}{ll} x+y+z & = 0 \\ ax+by+cz & = 0 \\ a^2x+b^2y+c^2z & = 0 \end{array} .$$

(5) [Sep 83 # 2] Prove that if a module has a composition series, it satisfies both chain conditions.

(6) [Sept 86 # 5] If M is an artinian module over a general R, show that any injective endomorphism is surjective.

(7) [Sep 84 # 5] If A, B, C are submodules of a general R-module M, with $A \supseteq C$, show $A \cap (B+C) = (A \cap B) + C$.

(8) [Jan 87 # 6; Aug 88 # 6] If I is an ideal of a commutative ring R, show (a) R/I is simple as an R-module $\iff I$ is a maximal ideal, (b) I prime $\implies R/I$ is an indecomposable R-module; (3) if I is prime, what kind of *ring* is R/I?

(9) [Jan 98 # 4] Let M be a module over a ring. A *section* $A : B$ of M is a pair of submodules A, B of M with $B \subseteq A$; a *trivial section* is where $B = A$. A submodule C of M *covers* a section $A : B$ if $(A \cap C) + B = A$, and *avoids* $A : B$ if $A \cap C \subseteq B$. (a) Show that C covers $A : B$ iff $A \subseteq B + C$, and avoids $A : B$ iff $A \cap (B+C) = B$. (b) Show that every C simultaneously covers and avoids any trivial section; that any C with $C \supseteq A$ covers $A : B$; and that any C with $C \subseteq B$ avoids $A : B$. (c) Give an example of a $\mathcal{Z}$-module M and a submodule C that covers one nontrivial section $A : B$ and avoids another nontrivial section $A' : B'$ for which the two quotients A/B and A'/B' are isomorphic.

(10) [Aug 96 # 3] Let M be a finitely generated module over a ring R. Show that *any* generating set for M as R-module must contain a *finite* generating set. Conclude that M has a minimal generating set (no proper subset generates M), and that every minimal generating set of M is finite.

(11) [Aug 94 # 8] If the *annihilator* of a left R-module M is $Ann_R(M) = \{a \in R \mid aM = 0\}$, show that for submodules M_1, M_2 of M we have $Ann_R(M_1 + M_2) = Ann_R(M_1) \cap Ann_R(M_2)$. Show furthermore that we have $Ann_R(M_1) + Ann_R(M_2) \subseteq Ann_R(M_1 \cap M_2)$, but show that this inclusion could be strict.

Handout # 6 July 26, 1999

6. JORDAN CANONICAL FORM: COUNTING QUESTIONS

JCF KNOWLEDGE

$T : V \longrightarrow V$ is a fixed linear transformation on a finite-dimensional vector space V over a field F, M is an $n \times n$ matrix over F.

1) **Know basic definitions for** T (analogously for M, interpreted as a linear transformation on $V = F^n$ acting by left multiplication): *characteristic polynomial* ($\chi_T(t) = \det(tId - T)$), *characteristic root* (root of the characteristic polynomial, λ such that $\det(\lambda I - T) = 0$), *minimum polynomial* (monic polynomial of smallest degree satisfied by T); *eigenvalue* (scalar $\lambda \in F$ such that $T(v) = \lambda v$ for some vector $0 \neq v \in V$) and *eigenvector* (vector $0 \neq v \in V$ such that $T(v) = \lambda v$ for some $\lambda \in F$); λ-*eigenspace* V_λ ($= \{v \in V \mid T(v) = \lambda v\} = \{$ eigenvectors of T$\} \cup \{0\}$); *generalized eigenvector* of order k ($= \{v \in V \mid (T - \lambda I)^k(v) = 0$ but $(T - \lambda I)^{k-1}(v) \neq 0\}$; order 0 means $v = 0$, order 1 means v is a true eigenvector); *generalized* λ*- eigenspace* V^λ (all generalized eigenvectors); *determinant, trace, rank, nullity, Jordan canonical form* JCF, *rational canonical form* RCF for a tranformation T or matrix M. $r \times r$ *Jordan block* $J_r(\lambda)$.

2) **Know facts**: (1) *eigenvectors = characteristic roots in finite dimensions* ($\det(\lambda I - T) = 0 \iff \lambda I - T$ singular, kills some vector $v \neq 0$, $\iff \lambda v = T(v) \iff v$ is an eigenvector with eigenvalue λ); (2) *minimum polynomial divides all polynomials satisfied by* T (it is generator of the ideal in $F[t]$ of all polynomials satisfied by T); (3) $V_\lambda = \ker(T - \lambda I)$, $V^\lambda = \bigcup_k \ker(T - \lambda I)^k$. (4) V becomes a finitely-generated module for the P.I.D. $F[x]$ via the action $x.v = T(v)$, so $f(x).v := f(T)(v)$; then V^λ is just the $x - \lambda$-torsion submodule, and a Jordan block $J_r(\lambda)$ in JCF corresponds to a cyclic direct summand $F[x]/(x_\lambda)$, in the decomposition of V considered as $F[x]$-module; (5) every polynomial splits into linear factors in some extension field, for example the algebraic closure of F, so we may have to pass to an extension in order to get enough eigenvalues and eigenvectors.

3) **Know How to Count**: If a matrix M has characteristic polynomial $\chi(t) = \prod(t - \lambda_i)^{f_i}$ and minimum polynomial $\mu(t) = \prod(t - \lambda_i)^{e_i}$, then $f_i \geq e_i; e_i$ gives the **size of the largest** Jordan λ_i-block, f_i gives the **total sum of the sizes** of all Jordan λ_i-blocks. $\dim\ker(M - \lambda) =$ **number** of Jordan λ-blocks = **number of independent λ-eigenvectors** (exactly one for each Jordan block), $\dim\ker(M - \lambda)^e =$ number of independent generalized λ-eigenvectors (exactly e for each Jordan λ-block of size $\geq e$, but only r for a Jordan λ-block of size $r \leq e$). [Pray that you aren't asked to find the matrix Q that puts M in Jordan form, $Q^{-1}MQ = J$, equivalently find the Jordan basis of generalized eigenvectors for M.]

COUNTING PROBLEMS

Describe (up to isomorphism, using JCF or RCF) all $n \times n$ matrices M over a specific F with given characteristic polynomial $\chi(t)$ and/or minimum polynomial $\mu(t)$.

(1) [Jan 89 # 5] $n = 9, F = F,\ \mu(t) = t^2(t-1)^2(t+1)^3$.

(2) [May 92 # 4] $n = 6, F = \mathcal{C},\ \mu(t) = (t-1)^2(t-2)$ (JCF).

(3) [Feb 84 # 4] $n = 6, F = Q,\ \mu(t) = (t-1)^2(t^2+1)$ (RCF over Q, JCF over $\mathcal{C}$).

(4) [Sep 79 # 1] $n = 6, F = \mathcal{C},\ \mu(t) = (t+2)^2(t-1)$ (JCF).

(5) [Aug 95 Comprehensive # 6] $n = 10, F = \mathcal{R},\ \mu(t) = (t^4-1)^2$ (find all possible values of k, the maximum number of independent eigenvectors).

(6) [Jan 79 # 5] $n = n, F = F,\ \mu(t) =$ product of distinct linear factors (find JCF, find eigenvalues of any polynomial $f(M)$).

(7) [Jan 94 # 1] $n = 5, F = Q,\ \mu(t) = (t-2)^2(t+3)$ (find all RCFs; find two such matrices having the same characteristic polynomial but which are still not similar).

(8) [May 91 # 1ab] $n = 6, F = \mathcal{R},\ \mu(t) = t^4 + t^2$ (RCF over $\mathcal{R}$, JCF over $\mathcal{R}$).

(9) [Aug 88 # 2] $n = 6, F = \mathcal{C}, \mathcal{R},\ \chi(t) = t^6 - t^5 - t^2 + t$ (JCF over $\mathcal{C}$, RCF over $\mathcal{R}$).

(10) [Jan 87 # 7] $n = 5, F = \mathcal{C}, \mathcal{R},\ \chi(t) = t^5 - t$ (RCF over $\mathcal{R}$, JCF over $\mathcal{C}$).

(11) [Jan 82 # I; Jan 79 # 1] $n = 6, F = \mathcal{C},\ \chi(t) = (t+2)^4(t-1)^2$ (JCF).

(12) [Jan 81 # 1] $n = 8, F = \mathcal{C}, \mathcal{R},\ \chi(t) = t^2(t^4-1)(t^2-1)$ (RCF over $\mathcal{R}$, JCF over $\mathcal{C}$).

(13) [Aug 96 # 7] $n = 7, F = \mathcal{C}, \mathcal{R},\ \chi(t) = (t-1)^3(t^2+1)^2, \mu(t) = (t-1)(t^2+1)^2$ (RCF over $\mathcal{R}, \mathcal{C}$, JCF over $\mathcal{C}$).

(14) [Jan 82 # III] $n = 5, F = \mathcal{C},\ \chi(t) = (t-2)^3(t+7)^2, \mu(t) = (t-2)^2(t+7)$ (find trace, determinant, JCF, is it diagonalizable?)

(15) [Jan 95 # 4] $n = 8, F = \mathcal{C},\ \chi(t) = t^8 - t^4, \mu(t) = t^6 - t^2$ (JCF).

(16) [Sep 80 # 3] $n = 4, F = \mathcal{C}$, satisfies $f(t) = t^2 - 7t + 10$, trace 11 (find determinant, JCF).

(17) [Aug 94 # 4b] $n = n, F = \mathcal{C}$, satisfies $f(t) = t^d - 1$ (has order d, smallest positive exponent such that $M^d = I$) (JCF).

(18) [Sep 82 # 7] Show two idempotent $n \times n$ matrices are similar iff they are equivalent.

(19) [Jan 92 # 5] $n = n, F = F$, satisfies $f(t) = t^2 - t$ (is *idempotent*, $M^2 = M$) (show two such are similar iff they have the same rank).

(20) [Sep 93 # 1] $n = n, F = \mathcal{R}$, satisfies $f(t) = t^3 - t$ (is *tripotent*, $M^3 = M$) (show two such are similar iff they have the same rank and the same trace).

(21) [Sep 78 # 2] $n = 12, F = GF(3),\ \chi(t) =$ product of linear factors; find JCF given $\text{rank}(M) = 10$, $\text{rank}(M^2) = 9$, $\text{rank}(M^3) = 9$, $\text{rank}(M-1) = 12$, $\text{rank}(M-2) = 9$, $\text{rank}((M-2)^2) = 7$, $\text{rank}((M-2)^3) = 6$.

(22) [Aug 89 # 7] $n = 2, F = GF(2)$, ALL POSSIBLE RCFs.

(23) [Aug 98 # 6] Let V be an n-dimensional vector space over the complex numbers, and let T be a linear transformation from V to itself whose minimum polynomial $\mu(x)$ has degree 2. (a) Find all possible Jordan Canonical Forms for T. [Hint: consider the possible factorizations of $\mu(x)$ over K.] (b) Show that V is a direct sum of T-invariant subspaces, each of which has dimension less than or equal to 2. (c) Show that T has an eigenvalue λ such that the λ -eigenspace (the set of all eigenvectors for the eigenvalue λ, together with the zero vector) has dimension at least $n/2$.

Handout # 7 July 27, 1999

7. JORDAN CANONICAL FORM: FINDING QUESTIONS

KNOWLEDGE

$T : V \longrightarrow V$ denotes a fixed linear transformation on a finite-dimensional vector space V over a field F. For an eigenvalue λ we set $N_\lambda := T - \lambda I$

1) **Know: T diagonalizable iff minimum polynomial has distinct linear roots** (eg. if characteristic polynomial has n distinct linear factors).

2) **Know how to do**: Gaussian reduction (elementary row operations), read off answer to system of equations $Ax = 0$ ($x = t_1x_1 + \ldots + t_rx_r$ for free parameters t_i from non-leading-one variables, basic solutions x_i arise as coefficients of t_i in solution).

3) **Know how to find** Ker(T): Gaussian reduction on system $Tx = 0$ (so dim Ker(T) = # free parameters = # columns - # leading-one rows.

4) **Know how to count**: The number n_e of Jordan λ-blocks of size e is given by a formula

$$n_e = g_e - g_{e+1} = 2k_e - (k_{e-1} + k_{e+1}), \quad g_e = k_e - k_{e-1} = \dim_F \left(\ker N_\lambda^{k+1} / \ker N_\lambda^k \right)$$

$$\text{for } g_e := \text{ the number of Jordan } \lambda\text{-blocks of size } \geq e, \quad k_e := \dim \left(\ker(N_\lambda^e) \right).$$

Each Jordan λ-block of size $\geq e$ contributes exactly one dimension to g_e (exactly one basic vector killed by N_λ^e but not already by N_λ^{e-1}), so g_e is the number of blocks of size $\geq e$, hence $g_e - g_{e+1}$ is (# size $\geq e$) - (# size $\geq e+1$) = (# size = e) = n_e. Another way to see this is as follows: each block of size i contributes e independent vectors to $\ker(N_\lambda^e)$ as long as $i \geq e$, but for $i < e$ can only contribute all it's got, namely i vectors, so

$$k_e = \dim \left(\ker(N_\lambda^e) \right) = n_1 + 2n_2 + 3n_3 + \ldots + (e-1)n_{e-1} + e(n_e + \ldots + n_r),$$

$$k_{e-1} = \dim \left(\ker(N_\lambda^{e-1}) \right) = n_1 + 2n_2 + 3n_3 + \ldots + (e-1)(n_{e-1} + n_e + \ldots + n_r)$$

$$g_e = k_e - k_{e-1} = n_e + \ldots + n_r = \text{ total number of size } \geq e,$$

$$g_e - g_{e+1} = \left(n_e + n_{e+1} + \ldots + n_r \right) - \left(n_{e+1} + \ldots + n_r \right) = n_e.$$

5) **Know how to find JCF**: (1) Find characteristic polynomial, (2) factor it into irreducibles $x - \lambda_i$; FIND JCF FOR EACH EIGENVALUE λ_iSEPARATELY; (3) [for roots of multiplicity $m > 1$ only] compute $k_e = \dim(\ker \left(N_\lambda^e \right)$ for $e = 1, 2, \ldots m$ (stop when dimension reaches m; $k_1 = m$ is the condition that there are enough independent ordinary eigenvectors to diagonalize), (4) $n_e = 2k_e - k_{e-1} - k_{e+1}$.

6) **Know how to find JCF basis** (only if forced to!): Systematic method for Jordan λ-blocks starting from a basis for $\ker(Z^k) = \ker \left(N_\lambda^k \right)$ for each $k = 1, 2, \ldots, e$ [obtained from Gaussian reduction], throwing in basic vectors from the kth kernel to an existing independent set [coming from the $(k-1)$st kernel and things generated by previous Jordan basis vectors].

FINDING PROBLEMS

Find the JCF and/or RCF J of a particular matrix M over field F (if asked: find Q with $Q^{-1}MQ = J$).

(1) [Jan 97 # 1] $F = \mathcal{R}, \mathcal{C}: \ M = \begin{pmatrix} -1 & 3 & 0 \\ 0 & 2 & 0 \\ 2 & 1 & -1 \end{pmatrix}$ (find RCF over $\mathcal{R}$, JCF over $\mathcal{C}$).

(2) [May 89 # 1] $F = \mathcal{C}: \ M = \begin{pmatrix} 0 & 4 & 2 \\ -1 & -4 & -1 \\ 0 & 0 & -2 \end{pmatrix}$.

(3) [1985 # 2] $F = \mathcal{R}: \ M = \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}$ (find $\chi(t), \mu(t)$, JCF).

(4) [Sep 84 # 4] $F = \mathcal{R}, \mathcal{C}: \ D = d/dx$ on $V = span\{x\sin(x), x\cos(x), \sin(x), \cos(x)\}$ (find $\chi(t), \mu(t)$,invariant factors, RCF over $\mathcal{R}$, JCF over $\mathcal{C}$).

(5) [Sep 83 #6] $F = \mathcal{C}: \ M_1 = \begin{pmatrix} 0 & -1 & -1 & -1 \\ 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{pmatrix}, M_2 = \begin{pmatrix} 0 & -1 & 0 & -1 \\ 1 & 2 & 1 & 2 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$.

(6) [Mar 83 # 1] $F = \mathcal{C}: \ \begin{pmatrix} -1 & 3 & 0 \\ 0 & 2 & 0 \\ 2 & 1 & -1 \end{pmatrix}$.

(7) [May 80 # 3] $F = \mathcal{C}: \ M_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \ M_2 = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ (find JCF and eigenvalues).

(8) [May 78 # 8] $F = \mathcal{C}: \ M = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$ (find $\chi(t), \mu(t)$, eigenvalues, JCF).

(9) [Nov 77 # 6] $F = \mathcal{R}$ [resp. $\mathcal{C}$], $M = d/dx, V = C^{\infty}(\mathcal{R})$ [resp. $C^{\infty}_{\mathcal{C}}(\mathcal{R})$ complex-valued functions on $\mathcal{R}$]; find all eigenvalues, eigenvectors; find JCF of restriction to space V_n of polynomials of degree $< n$.

(10) [Aug 95 # 5] $F = \mathcal{R}: \ M = (a_{ij})$ with $a_{ij} = 1$ for $i \leq j$ and $a_{ij} = 0$ for $i > j$ (find JCF).

(11) [May 92 # 7] If a real 2×2 symmetric matrix M has $\lim_{n\to\infty} trace(M^n) = 0$, show $\lim_{n\to\infty} M^n = 0$ too. Does this hold for $n \times n$ real symmetric matrices?

(12) [May 91 # 1c] Suppose M has the property that $trace(M^k) = 0$ for all $k > 0$, and that its minimum polynomial divides $t^4 + t^2$. Show that M is nilpotent.

(13) [Jan 98 # 7] If the $n \times n$ real matrix P is the transition matrix for a regular Markov chain, then its powers converge to a matrix $T = \lim_{n \to \infty} P^k$ of the form $\begin{pmatrix} t_1 & t_1 & \dots & t_1 \\ t_2 & t_2 & \dots & t_2 \\ \dots & \dots & \dots & \dots \\ t_n & t_n & \dots & t_n \end{pmatrix}$ all of whose columns are the same probability vector $\vec{t}$ (it's entries t_i are all nonnegative and sum to 1). (a) What is the JCF of the limit T? (b) What are the possible complex eigenvalues of the original P? (c) What are the possible JCFs of P? If you cannot do the general case, do at least the 2×2 case.

(14) [Aug 97 # 1b] Let K be a field containing p distinct p-th roots of unity, L and extension field such that $Gal(L/K)$ is a cyclic group of order p with generator σ. Find the Jordan canonical form of σ.

RELATED PROBLEMS

(1) [May 1990 # 7] Explain which of these 8×8 matrices are similar.

$$M_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & -3 & 0 & -3 & 0 \end{pmatrix}, \; M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & i & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & i & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -i & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -i & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -i \end{pmatrix},$$

$$M_3 = \begin{pmatrix} i & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & i & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & i & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -i & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -i & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

(2) [May 89 # 9] If an $n \times n$ matrix M over F has an elementary divisor $\lambda - a$ $(a \in F)$ show there is an invertible $n \times n$ matrix Q over F with $Q^{-1}MQ =$ RCF(M) AND $\det(Q) = 1$.

(3) [Fall 87 # 6] Find RCF of the 9×9 matrix over R whose JCF is $M = Diag\{J_2(2), J_1(2), J_2(2), J_2(i), J_2(-i)\}$.

(4) [Sep 86 # 3] Show S, T on a finite-dimensional V are similar if (1) $\text{rank}(S^m) = \text{rank}(T^m)$ for all $m = 0, 1, \dots$, (2) $S^n = 0$ for some n.

(5†) [Sep 84 # 8] Find the determinant and inverse of the $n \times n$ real matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 2 & 2 & \dots & 2 \\ 1 & 2 & 3 & 3 & \dots & 3 \\ 1 & 2 & 3 & 4 & \dots & 4 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 2 & 3 & 4 & \dots & n \end{pmatrix}.$$

(6†) [Sep 83 # 5] If M is any 3×3 real matrix with characteristic polynomial $x^3 + ax^2 + bx + c$, define its adjoint to be $M^* := M^2 + aM + bI$ and show $M^* = \det(M)M^{-1}$ when M is invertible; show $(M^*)^* = \det(M)M$ for any M.

(7) [Sep 82 # 8] Give two complex 4×4 matrices that have the same minimum and characteristic polynomials, yet are not similar.

(8) [Sep 78 # 1] Show that the set of 3×3 rational matrices commuting with $M = \begin{pmatrix} 0 & 0 & 6 \\ 1 & 0 & 4 \\ 0 & 1 & 2 \end{pmatrix}$ form a field.

(9) [May 78 # 7] Find inverse of $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

(10) [April 77 # 1] Use JCF to show $\det(e^M) = e^{trace(M)}$ for any $n \times n$ complex matrix; find e^M for $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

(11) [April 77 # 7] If M is a $n \times n$ complex matrix which is *normal* ($MM^* = M^*M$), use the Spectral Theorem to show $M^* = f(M)$ for some polynomial f; conclude any matrix which commutes with M also commutes with M^*.

(12) [Aug 95 Comprehensive # 4] If T is a diagonalizable linear operator on a finite-dimensional vector space V and W is a T-invariant subspace of V, prove W has a T-invariant complement (a subspace U such that $V = W \oplus U$).

Companion Matrices of a Polynomial d(t)

$$d(t) = a_0 + a_1 t + a_2 t^2 + \ldots + a_{m-1} t^{m-1} + t^m$$

Let the vector space V over F be a cyclic T-module with cyclic generator v and minimum polynomial $d(t)$, so that the vectors $v, T(v), T^2(v), \ldots, T^{m-1}(v)$ form a basis for V with $T^m(v) = -\big(a_0 I + a_1 T + a_2 T^2 + \ldots + a_{m-1} T^{m-1}\big)(v)$.

Matrices written on the left of vectors

Upper Left Companion Matrix = left matrix of T with respect to ordered basis $\overleftarrow{\mathcal{B}} = \{T^{m-1}(v), T^{m-2}(v), \ldots, T^2(v)T(v), v\}$:

$$\begin{pmatrix} -a_{m-1} & 1 & 0 & 0 & \ldots & 0 \\ -a_{m-2} & 0 & 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ -a_1 & 0 & 0 & 0 & \ldots & 1 \\ -a_0 & 0 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

$\Longleftarrow$ **USE THIS FORM**
1's down the superdiagonal
negatives of coefficients of d
run UP the FIRST column.

Lower Left Companion Matrix = left matrix of T with respect to ordered basis $\overrightarrow{\mathcal{B}} = \{v, T(v), T^2(v), \ldots, T^{m-2}(v), T^{m-1}(v), \}$:

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & 0 & -a_1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 0 & -a_{m-2} \\ 0 & 0 & \ldots & 0 & 1 & -a_{m-1} \end{pmatrix}$$

1's down the subdiagonal
negatives of coefficients of d
run DOWN the LAST column.

Matrices written on the right of vectors

Upper Right Companion Matrix = right matrix of T with respect to ordered basis $\overrightarrow{\mathcal{B}} = \{v, T(v), T^2(v), \ldots, T^{m-2}(v), T^{m-1}(v), \}$ (transpose of Left Lower):

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ -a_0 & -a_1 & -a_2 & \ldots & a_{m-2} & -a_{m-1} \end{pmatrix}$$

1's down the superdiagonal,
negatives of coefficients of
d run LEFT across the
BOTTOM row.

Lower Right Companion Matrix = right matrix of T with respect to ordered basis $\overleftarrow{\mathcal{B}} = \{T^{m-1}(v), T^{m-2}(v), \ldots, T^2(v)T(v), v\}$ (transpose of Left Upper):

$$\begin{pmatrix} -a_{m-1} & -a_{m-2} & \ldots & -a_2 & -a_1 & -a_0 \\ 1 & 0 & \ldots & 0 & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 0 & 0 \\ 0 & 0 & \ldots & 0 & 1 & 0 \end{pmatrix}$$

1's down the subdiagonal,
negatives of coefficients of
d run RIGHT across the
TOP row.

FROM NOW ON WE WILL ONLY DEAL WITH LEFT MATRICES
(operators on left of vectors, $T(v)$, matrices constructed column-by-column)

Invariant Rational Canonical Form

$V = V_1 \oplus \ldots \oplus V_s$ for T-invariant subspaces V_i which are cyclic with generators v_i and the restrictions $T_i := T\mid_{V_i}$ have minimum polynomials $d_i(t)$ with $d_1(t) \mid d_2(t) \mid \ldots \mid d_s(t)$ (the *invariant factors* of T).

$$T \sim \begin{pmatrix} C_1 & & & & \\ & \bullet & & & \\ & & \bullet & & \\ & & & \bullet & \\ & & & & C_s \end{pmatrix}$$

BLOCK
DIAGONAL
FORM

UPPER form: C_i = upper left companion matrix of $d_i(t)$;
LOWER form: C_i = lower left companion matrix of $d_i(t)$.

Elementary Rational Canonical Form

$V = V_1 \oplus \ldots \oplus V_r$ for T-invariant subspaces V_i which are cyclic with generators v_i and the restrictions $T_i := T\mid_{V_i}$ have minimum polynomials $p_i(t)^{e_i}$ (the *elementary divisors* of T) with $p_i(t)$ irreducible.

$$T \sim \begin{pmatrix} B_1 & & & & \\ & \bullet & & & \\ & & \bullet & & \\ & & & \bullet & \\ & & & & B_r \end{pmatrix}$$

BLOCK
DIAGONAL
FORM.

Upper Elementary Form: if we let P_i = upper left companion matrix of $p_i(t)$, $N_i = \begin{pmatrix} 0 & \ldots & 0 \\ \ldots & \ldots & \ldots \\ 1 & \ldots & 0 \end{pmatrix}$ the square matrix of size $n_i \times n_i$ (n_i = degree of $p_i(t)$) with 1 in lower left corner and zeroes elsewhere, then

$$B_i \sim \begin{pmatrix} P_i & N_i & & & \\ & P_i & N_i & & \\ & & \bullet & & N_i \\ & & & \bullet & P_i \end{pmatrix}$$

$\Longleftarrow$ **USE THIS FORM**
e_i blocks down the diagonal.

Lower Elementary Form: if we let Q_i = lower left companion matrix of $p_i(t)$, $M_i = \begin{pmatrix} 0 & \ldots & 1 \\ \ldots & \ldots & \ldots \\ 0 & \ldots & 0 \end{pmatrix}$ the square matrix of size $n_i \times n_i$ (n_i = degree of $p_i(t)$) with 1 in upper right corner and zeroes elsewhere, then

$$B_i \sim \begin{pmatrix} Q_i & & & & \\ M_i & Q_i & \bullet & & \\ & M_i & & \bullet & \\ & & & M_i & Q_i \end{pmatrix}$$

e_i blocks down the diagonal.

The Upper and Lower Elementary RCF are the matrices of T with respect to slightly modified bases, designed to display the companion matrices of the individual irreducible factors $p_i(t)$ repeated e_i times (glued together by the matrices N_i or M_i), instead of just the companion matrix of the total product $p_i(t)^{e_i}$.

The elementary block B_i is the matrix of T with respect to a basis $\mathcal{B}_i$. For the Upper Elementary RCF we have

$$\mathcal{B}_i = \{\overleftarrow{\mathcal{B}}_{i,e_i-1}; \ldots ; \overleftarrow{\mathcal{B}}_{i,1}; \overleftarrow{\mathcal{B}}_{i,0}\}$$

where for each $j = e_i - 1, \ldots, 1, 0$ the ordered basis $\overleftarrow{\mathcal{B}}_{i,j}$ is given by

$$\overleftarrow{\mathcal{B}}_{i,j}= \{v_{i;j;m-1}, v_{i;j;m-2}, \ldots, v_{i;j;1}, v_{i;j;0}\} \quad \big(v_{i;j;k} := T^k p_i(T)^j(v_i)\big)$$

[Notice that the standard cyclic basis has been modified to use $v_{i;j;k}$ instead of $T^{k+jm}(v_i),\ m = \deg p_i(t)$; both have the same leading power of T, but the action of T on the top term $v_{i;j;m-1}$ in the j-th part of the basis $\overleftarrow{\mathcal{B}}_{i,j}$ does not merely boost to the next basis vector, it boosts to the first vector in the (next) $j+1$-st basis *minus* a combination of vectors from the j-th basis with the coefficients from $p_i(t)$:

$$\begin{aligned} T(v_{i;j;m-1}) \quad &= \big(T^m\big)p_i(T)^j(v_i) \\ &= \big(p_i(T) - a_0 I - a_1 T - \ldots - a_{m-1}T^{m-1}\big)p_i(T)^j(v_i) \\ &= v_{i;j+1;0} - a_0 v_{i;j;0} - a_1 v_{i;j;1} - \ldots - a_{m-1} v_{i;j;m-1}. \end{aligned}$$

The e_i-th basis collapses,

$$v_{i;e_i;k} = 0 \text{ since } \ p_i(T)^{e_i}(v_i) = 0$$

by definition of $p_i(t)^{e_i}$ as minimum polynomial on V_i.]

Similarly, the elementary block B_i for the Lower Elementary RCF is the matrix of T with respect to a basis

$$\mathcal{B}_i = \{\overrightarrow{\mathcal{B}}_{i,0}; \overrightarrow{\mathcal{B}}_{i,1}; \ldots ; \overrightarrow{\mathcal{B}}_{i,e_i-1}\}$$

where for each $j = 0, 1, \ldots, e_i - 1$ the basis $\overrightarrow{\mathcal{B}}_{i,j}$ is given by

$$\overrightarrow{\mathcal{B}}_{i,j}= \{v_{i;j;0}, v_{i;j;1}, \ldots, v_{i;j;m-2}, v_{i;j;m-1}\}$$

EXAMPLE:

Primary cyclic V with minimum polynomial $p(t)^3$ for $p(t) = t^2 + 2t + 3$.

INVARIANT RCF: $s = 1,\ d_1 = p(t)^3 = t^6{+}6t^5{+}19t^4{+}36t^4{+}43t^2{+}30t{+}9$

Upper Invariant RCF Block

$$\begin{pmatrix} -6 & 1 & 0 & 0 & 0 & 0 \\ -19 & 0 & 1 & 0 & 0 & 0 \\ -36 & 0 & 0 & 1 & 0 & 0 \\ -43 & 0 & 0 & 0 & 1 & 0 \\ -30 & 0 & 0 & 0 & 0 & 1 \\ -9 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Lower Invariant RCF Block

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -9 \\ 1 & 0 & 0 & 0 & 0 & -30 \\ 0 & 1 & 0 & 0 & 0 & -43 \\ 0 & 0 & 1 & 0 & 0 & -36 \\ 0 & 0 & 0 & 1 & 0 & -19 \\ 0 & 0 & 0 & 0 & 1 & -6 \end{pmatrix}$$

ELEMENTARY RCF: $r = 1,\ p(t) = t^2 + 2t + 3,$

$$P = \begin{pmatrix} -2 & 1 \\ -3 & 0 \end{pmatrix},\ N = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ Q = \begin{pmatrix} 0 & -3 \\ 1 & -2 \end{pmatrix},\ M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Upper Elementary RCF Block

$$\left(\begin{array}{cc|cc|cc} -2 & 1 & 0 & 0 & 0 & 0 \\ -3 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & -3 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 0 & -3 & 0 \end{array}\right)$$

Lower Elementary RCF Block

$$\left(\begin{array}{cc|cc|cc} 0 & -3 & 0 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & -3 & 0 & 0 \\ 0 & 0 & 1 & -2 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & -3 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{array}\right)$$

JORDAN CANONICAL FORM = UPPER ELEMENTARY RCF WHEN ALL IRREDUCIBLES ARE LINEAR, $p_i(t) = t - \alpha_i \in F$.

Companion matrix is 1×1 matrix $P = Q = \big(\alpha_i\big)$, and the glueing matrix is $N = M = \big(1\big)$.

Upper Jordan Block

$$\left(\begin{array}{c|c|c} \alpha & 1 & 0 \\ \hline 0 & \alpha & 1 \\ \hline 0 & 0 & \alpha \end{array}\right)$$

EVERONE
USES THIS
⟵

Lower Jordan Block

$$\left(\begin{array}{c|c|c} \alpha & 0 & 0 \\ \hline 1 & \alpha & 0 \\ \hline 0 & 1 & \alpha \end{array}\right)$$

Jordan Canonical Form (JCF) is the matrix of T with respect to a **Jordan basis**.

Jordan α-Block of Multiplicity e : $J_e(\alpha)$

$$\begin{pmatrix} \alpha & 1 & 0 & \dots & 0 & 0 \\ 0 & \alpha & 1 & \dots & 0 & 0 \\ 0 & 0 & \alpha & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \alpha & 1 \\ 0 & 0 & 0 & \dots & 0 & \alpha \end{pmatrix}$$

The basis for the (Upper) Jordan α-block of multiplicity e is

$$\overleftarrow{\mathcal{B}} = \{v_{e-1}, v_{e-2}, \dots, v_1, v_0\}$$

where

$$v_k = (T-\alpha)^k(v_0), \text{ so } (T-\alpha)v_i = v_{i+1}, (T-\alpha)v_{e-1} = v_e := 0.$$

The basis for the (seldom used) Lower Jordan α-Block is just the reverse of this, $\overrightarrow{\mathcal{B}} = \{v_0, v_1, \dots, v_{e-2}, v_{e-1}\}$.

It is important that the first basic vector v_{e-1} is the only eigenvector in the block, and that the cyclic generator v_0 has $(T-\alpha)^e(v_0) = 0$ but $(T-\alpha)^{e-1}(v_0) \neq 0$.

BASIC FACT:

THE JORDAN BASIS (hence the Jordan block)

FLOWS FROM THE GENERATING VECTOR v_0.

In the standard (upper) Jordan basis, the generator v_0 is at the far *right*, and the rest of the Jordan basis flows out of it *to the left*.

Finding a Jordan Basis

(Step 0) **Similarity Transform = Jordan Basis**: The *similarity matrix* P which transforms the matrix T into Jordan form by the *similarity transform* $P^{-1}TP = J$ is just the matrix $P = \begin{pmatrix} \uparrow & \cdots & \cdots & \uparrow \\ \vec{x}_1 & \cdots & \cdots & \vec{x}_n \\ \downarrow & \cdots & \cdots & \downarrow \end{pmatrix}$ whose columns are the vectors in a JORDAN BASIS $\mathcal{B} = \{x_1, \ldots, x_n\}$ ifor $V = R^n$. Thus the columns of P are *particular independent eigenvectors and generalized eigenvectors of T in a particular order.*

(Step 1) **Primary Decomposition**: Because generalized eigenvectors for distinct eigenvalues λ are automatically independent, we can BREAK THE PROBLEM INTO ITS PRIMARY COMPONENTS AND CONSTRUCT JORDAN BASES FOR EACH λ SEPARATELY: $V = V_{\lambda_1} \oplus \ldots \oplus V_{\lambda_r}$ for distinct eigenvalues $\lambda_1, \ldots, \lambda_r$ is the unique, canonical *primary decomposition* of V as $F[t]$-module into its p_i-primary components for primes $p_i = t - \lambda_i$. A Jordan basis $\mathcal{B} = \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_r$ is the union (in some order) of Jordan bases $\mathcal{B}_i$ for each primary component V_{λ_1}. (It is a convention, though not a rule, that in Jordan Canonical Form you always lump together all Jordan blocks going with the same eigenvalue λ_i.)

(Step 3) **The Primary Case**: We are thus reduced to finding a Jordan Basis for $V_\lambda = \ker(T - \lambda I)^e$ for a fixed eigenvalue λ, where $e \leq n$ is the exponent of $(t - \lambda)$ in the factorization of the *characteristic polynomial* $\chi_T(t)$. There is no trouble if $e = 1$, or more generally if the exponent $f \leq e$ of $t - \lambda$ in the *minimum polynomial* $\mu_T(t)$ is $f = 1$ (then V_λ is "diagonalizable", has a basis of eigenvectors, i.e. is a direct sum of e different Jordan λ-blocks $J_1(\lambda)$ of size 1. At the opposite extreme, there is no problem when $f = e$: then there is exactly one Jordan block $J_e(\lambda)$ of size e. THE TROUBLE COMES WHEN THERE ARE SEVERAL λ-BLOCKS FOR A GIVEN λ AND $1 < f < e$: YOU MUST BE CAREFUL TO CONSTRUCT BLOCKS WHICH DON'T GET TANGLED UP WITH EACH OTHER (i.e. all the various vectors remain independent). Recall that the Jordan basis $\mathcal{B}_i = \{N^{m-1}v_m, \ldots, N^2(v_m), N(v_m), v_m\}$ for each Jordan block $J_m(\lambda)$ flows from the cyclic generating vector v_m (with $N^m v_m = 0$) under $N = T - \lambda I$, but an independent family of vectors v_k from $\ker(N^k)$ need NOT generate an independent family of Jordan λ-blocks: we must make sure the v_k do not come from higher layer of generalized eigenvectors, $v_k = N(v_{k+1})$ (else the block determined by v_k would be part of a larger block), and we must make sure v_k does not fall into a lower layer $\ker(N^{k-1})$ (else the block would be a smaller block of size $k - 1$ or less). Thus our choice of independent generators v_k for blocks of size k must simultaneously dodge debris coming from higher blocks and stay independent modulo debris in lower blocks.

Layer-by-Layer Attack on V_λ

We replace V, T by $V_\lambda, T\mid_{V_\lambda}$ and assume from the start we are in a primary component. We define the **k-th level** of V to be subspace $V_k = \ker(N^k)$,

$$0 < V_1 < V_2 < \ldots V_{f-1} < V_f = V$$

(where the top level occurs the first time $V_f = V_{f+1}$, and the f is precisely the exponent of $(t-\lambda)$ in the minimum polynomial), and choose (e.g. via Maple or Mathematica) a basis $\mathcal{B}_{k,0}$ for V_k.

Level f: As with Jordan bases for Jordan blocks, *we must always start at the top.* We decompose the top level f into the level $f-1$ below plus a complement, the **f-layer** W_f, and choose corresponding bases:

$$V_f = V_{f-1} \oplus W_f, \text{ basis } \mathcal{B}_f = \mathcal{B}_{f-1,0} \cup \mathcal{J}_f$$

(for example, by adjoining the elements of $\mathcal{B}_{f,0}$ one at a time to $\mathcal{B}_{f-1,0}$, keeping at each step only those new elements that increase the rank).

Level $f-1$: We automatically have a subspace $V_{f-2} \oplus N(W_f) \subseteq V_{f-1}$, since if $0 = v_{f-2} + N(w_f)$ then applying N^{f-2} gives $0 = 0 + N^{f-1}(w_f)$, hence $w_f \in W_f \cap V_{f-1} = 0$. Thus we may decompose the level $f-1$ into the level $f-2$ below plus the debris from above plus a complement, the **$f-1$-layer** W_{f-1}, and again choose corresponding bases:

$$V_{f-1} = V_{f-2} \oplus N(W_f) \oplus W_{f-1}, \text{ basis } \mathcal{B}_{f-1} = \mathcal{B}_{f-2,0} \cup N(\mathcal{J}_f) \cup \mathcal{J}_{f-1}$$

(for example, by again adjoining the elements of $\mathcal{B}_{f-1,0}$ one at a time to $\mathcal{B}_{f-2,0} \cup N(\mathcal{J}_f)$).

Induction from Level $f-k$ to $f-(k+1)$: Given

$$V_{f-k} = V_{f-k-1} \oplus N^k(W_f) \oplus N^{k-1}(W_{f-1}) \oplus \ldots \oplus W_{f-k}$$

with corresponding basis

$$\mathcal{B}_{f-k} = \mathcal{B}_{f-k-1,0} \cup N^k(\mathcal{J}_f) \cup N^{k-1}(\mathcal{J}_{f-1}) \cup \ldots \cup N(\mathcal{J}_{f-(k-1)}) \cup \mathcal{J}_{f-k},$$

we again automatically have a subspace

$$V_{f-k-2} \oplus N^{k+1}(W_f) \oplus N^k(W_{f-1}) \oplus \ldots \oplus N(W_{f-k}) \subseteq V_{f-k-1},$$

since if $0 = v_{f-k-2} + N^{k+1}(w_f) + \ldots N(w_{f-k})$ then applying N^{f-k-2} gives $0 = 0 + N^{f-1}(w_f) + \ldots + N^{f-k-1}(w_{f-k})$, so $N^k(w_f) + \ldots + w_{f-k} \in \ker(N^{f-k-1}) = V_{f-k-1}$ forces $w_f = \ldots = w_{f-k} = 0$ by assumed independence, then $v_{f-k-2} = 0$ too. Thus we may decompose the level $f-k-1$ into the level $f-k-2$ below plus the debris from above plus a complement, the **$f-k-1$-layer** W_{f-k-1}, and again choose corresponding bases:

$$V_{f-k-1} = V_{f-k-2} \oplus N^{k+1}(W_f) \oplus N^k(W_{f-1}) \oplus \ldots \oplus N(W_{f-k}) \oplus W_{f-k-1}$$

$$\mathcal{B}_{f-k-1} = \mathcal{B}_{f-k-2,0} \cup N^{k+1}(\mathcal{J}_f) \cup N^k(\mathcal{J}_{f-1}) \cup \ldots \cup N(\mathcal{J}_{f-k}) \cup \mathcal{J}_{f-k-1}.$$

Bottom Level $1 = f - (f-1)$: Since $V_0 = 0 = W_0, \mathcal{B}_0 = \emptyset$, we finally end up with the true eigenspace

$$V_1 = N^{f-1}(W_f) \oplus N^{f-2}(W_{f-1}) \oplus \ldots \oplus W_1$$

with corresponding basis of eigenvectors

$$\mathcal{B}_1 = N^{f-1}(\mathcal{J}_f) \cup N^{f-2}(\mathcal{J}_{f-1}) \cup \ldots \cup N(\mathcal{J}_2) \cup \mathcal{J}_1.$$

Since we can replace any basis $\mathcal{B}_{i,0}$ for V_i by another basis $\mathcal{B}_i$, we do this successively starting from the bottom to get

$$\begin{aligned}
&\mathcal{B}'_1 = \mathcal{B}_1 = N^{f-1}(\mathcal{J}_f) \cup N^{f-2}(\mathcal{J}_{f-1}) \cup \ldots \cup N(\mathcal{J}_2) \cup \mathcal{J}_1\\
&\mathcal{B}'_2 = \mathcal{B}'_1 \cup N^{f-2}(\mathcal{J}_f) \cup N^{f-3}(\mathcal{J}_{f-1}) \cup \ldots \cup N(\mathcal{J}_3) \cup \mathcal{J}_2\\
&\vdots\\
&\mathcal{B}'_{f-1} = \mathcal{B}'_{f-2} \cup N(\mathcal{J}_f) \cup \mathcal{J}_{f-1}\\
&\mathcal{B}'_f = \mathcal{B}'_{f-1} \cup \mathcal{J}_f.
\end{aligned}$$

where each $\mathcal{J}_k$ **is a basis for the k-th layer**. Putting these together gives us a basis $\mathcal{B}' = \mathcal{B}'_f$ for all of $V_f = V$ which we can portray schematically by:

$\mathcal{B}'_f$	$\mathcal{J}_f$					
$\mathcal{B}'_{f-1}$	$N(\mathcal{J}_f)$	$\mathcal{J}_{f-1}$				
$\mathcal{B}'_{f-2}$	$N^2(\mathcal{J}_f)$	$N(\mathcal{J}_{f-1})$	$\mathcal{J}_{f-2}$			
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		
$\mathcal{B}'_2$	$N^{f-2}(\mathcal{J}_f)$	$N^{f-3}(\mathcal{J}_{f-1})$	$N^{f-4}(\mathcal{J}_{f-2})$	$\ldots$	$\mathcal{J}_2$	
$\mathcal{B}'_1$	$N^{f-1}(\mathcal{J}_f)$	$N^{f-2}(\mathcal{J}_{f-1})$	$N^{f-3}(\mathcal{J}_{f-2})$	$\ldots$	$N(\mathcal{J}_2)$	$\mathcal{J}_1$

The Final Jordan Basis is created *by generating one Jordan λ-block of size k out of each vector in $\mathcal{J}_k$*, for $k = f, f-1, \ldots, 2, 1$. In the above diagram, each block "hangs down" from its generator in $\mathcal{J}_k$, containing one vector in each of $\mathcal{J}_k, N(\mathcal{J}_k), N^2(\mathcal{J}_k), \ldots, N^{k-1}(\mathcal{J}_k)$. That is, for each $v_k \in \mathcal{J}_k$ we get a Jordan block basis $\{N^{k-1}(v_k), \ldots, N^2(v_k), N(v_k), v_k\}$. By stringing all these together we get a Jordan basis for $V = V_\lambda$, and doing the same thing for each λ and putting them all together gives a Jordan basis for V itself.

Clearly this construction is too time-consuming to appear on a General Exam except perhaps for one λ-block of size 1 and one of size 2. Even in this situation you will probably only be asked to describe the Jordan form, not actually find the Jordan basis.

Computing using Jordan Form

Example: A system of ordinary DE's which are *linear with constant coefficients* has solution given by the exponential of the matrix of coefficients,

$$\frac{d}{dt}\vec{y}(t) = A\vec{y}(t),\ \vec{y}(t_0) = \vec{y}_0 \Longleftrightarrow \vec{y}(t) = e^{(t-t_0)A}(\vec{y}_0).$$

Computing $f(A)$ for a function $f(t)$ which is analytic, or meromorphic with poles which don't include any eigenvalues of A:

(1) **Reduction to Jordan Form** $f(J)$: If $S^{-1}AS = J$ then $A = SJS^{-1}$ and $f(A) = Sf(J)S^{-1}$.

(2) **Reduction to Block Form**: If $J = \begin{pmatrix} B_1 & & & \\ & \bullet & & \\ & & \bullet & \\ & & & B_r \end{pmatrix}$ is in block-diagonal form, then it suffices to compute $f(B)$ for each block:

$$f(J) = \begin{pmatrix} f(B_1) & & & \\ & \bullet & & \\ & & \bullet & \\ & & & f(B_r) \end{pmatrix}.$$

(3) **Evaluation on a Jordan Block**: If $B = J_m(\lambda) = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \bullet & & \\ & & & \bullet & 1 \\ & & & & \lambda \end{pmatrix}$

then

$$f(J_m(\lambda)) = \begin{pmatrix} f(\lambda) & f'(\lambda) & \frac{f''(\lambda)}{2!} & \dots & \dots & \dots & \frac{f^{(m-1)}(\lambda)}{(m-1)!} \\ & f(\lambda) & f'(\lambda) & \dots & \dots & \dots & \dots \\ & & f(\lambda) & \bullet & \dots & \dots & \dots \\ & & & & \bullet & \dots & \frac{f''(\lambda)}{2!} \\ & & & & & f(\lambda) & f'(\lambda) \\ & & & & & & f(\lambda) \end{pmatrix}.$$

Reason: $f(t) = \sum_{k=0}^{\infty} \frac{f^{(k)}}{k!}(t-\alpha)^k$, so $f(J_m(\alpha)) = \sum_{k=0}^{\infty} \frac{f^{(k)}(\alpha)}{k!}N^k$ where $J = \alpha I + N$ with $N = J_m(0) = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \bullet & & \\ & & & \bullet & 1 \\ & & & & 0 \end{pmatrix}$, $N^k = \begin{pmatrix} 0 & & 1 & \\ & \bullet & & 1 \\ & & \bullet & \\ & & & 0 \end{pmatrix}$ having 1's down the k-th superdiagonal and 0's elsewhere, $N^m = 0$.

Important Example: $f(t) = e^t$, $e^{tJ_m(\alpha)} = e^{t\alpha}e^{tN} = e^{t\alpha}\left(\begin{array}{ccccccc} 1 & t & \frac{t^2}{2!} & \cdots & \cdots & \cdots & \frac{t^m}{(m-1)!} \\ & 1 & t & \frac{t^2}{2!} & \cdots & \cdots & \cdots \\ & & 1 & \bullet & \cdots & \cdots & \cdots \\ & & & & \bullet & \cdots & \frac{t^2}{2!} \\ & & & & & 1 & t \\ & & & & & & 1 \end{array}\right)$.

Example 1: An ODE with solution involving real exponentials is

$$y_1'(t) = \alpha y_2(t),\ y_2'(t) = \alpha y_1(t),\ y_1(0) = c_1,\ y_2(0) = c_2,$$

which be written $\vec{y}\,' = A\vec{y}$ for $A = \begin{pmatrix} 0 & \alpha \\ \alpha & 0 \end{pmatrix}$, $S^{-1}AS = J = \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}$ for $S = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $S^{-1} = \frac{1}{2}S$, $e^{tJ} = \begin{pmatrix} e^{t\alpha} & 0 \\ 0 & e^{-t\alpha} \end{pmatrix}$, $e^{tA} = Se^{tJ}S^{-1} = \frac{1}{2}\begin{pmatrix} e^{\alpha t} + e^{-\alpha t} & e^{\alpha t} - e^{-\alpha t} \\ e^{\alpha t} - e^{-\alpha t} & e^{\alpha t} + e^{-\alpha t} \end{pmatrix}$, $e^{tA}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = e^{\alpha t}\begin{pmatrix} \frac{1}{2}(c_1 + c_2) \\ \frac{1}{2}(c_1 + c_2) \end{pmatrix} + e^{-\alpha t}\begin{pmatrix} \frac{1}{2}(c_1 - c_2) \\ \frac{1}{2}(-c_1 + c_2) \end{pmatrix}$, leading to the general solution

$$y_1(t) = \frac{c_1 + c_2}{2}\,e^{\alpha t} + \frac{c_1 - c_2}{2}\,e^{-\alpha t},\ y_2(t) = \frac{c_1 + c_2}{2}\,e^{\alpha t} + \frac{-c_1 + c_2}{2}\,e^{-\alpha t}.$$

Example 2: An ODE leading to a solution involving *sin*, *cos* is

$$y_1'(t) = \alpha y_2(t),\ y_2'(t) = -\alpha y_1(t),\ y_1(0) = c_1,\ y_2(0) = c_2,$$

which be written $\vec{y}\,' = A\vec{y}$ for $A = \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix}$, $S^{-1}AS = J = \begin{pmatrix} \alpha i & 0 \\ 0 & -\alpha i \end{pmatrix}$ for $S = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$, $S^{-1} = \frac{1}{2}\bar{S}$, $e^{tJ} = \begin{pmatrix} e^{t\alpha i} & 0 \\ 0 & e^{-t\alpha i} \end{pmatrix}$, $e^{tA} = Se^{tJ}S^{-1} = \begin{pmatrix} \frac{1}{2}(e^{i\alpha t} + e^{-i\alpha t}) & \frac{1}{2i}(e^{i\alpha t} - e^{-i\alpha t}) \\ \frac{1}{2i}(-e^{i\alpha t} + e^{-i\alpha t}) & \frac{1}{2}(e^{i\alpha t} + e^{-i\alpha t}) \end{pmatrix} = \begin{pmatrix} cos(\alpha t) & sin(\alpha t) \\ -sin(\alpha t) & cos(\alpha t) \end{pmatrix}$, $e^{tA}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = cos(\alpha t)\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} + sin(\alpha t)\begin{pmatrix} c_2 \\ c_1 \end{pmatrix}$, leading to the general solution

$$y_1(t) = c_1 cos(\alpha t) + c_2 sin(\alpha t),\ y_2(t) = c_2 cos(\alpha t) - c_1 sin(\alpha t).$$

Example 3: An ODE with solution involving t times an exponential is

$$y_1'(t) = \alpha y_1(t) + y_2(t),\ y_2'(t) = \alpha y_2(t),\ y_1(0) = c_1,\ y_2(0) = c_2,$$

which can be written $\vec{y}\,' = A\vec{y}$ for $A = J = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$, $e^{tA} = e^{tJ} = e^{t\alpha}\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$, $e^{tA}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = e^{\alpha t}\begin{pmatrix} c_1 + tc_2 \\ c_2 \end{pmatrix}$, leading to the general solution

$$y_1(t) = c_1e^{\alpha t} + c_2te^{\alpha t},\ y_2(t) = c_2e^{\alpha t}.$$

Handout # 8 July 29, 1999

8. FIELD THEORY

KNOWLEDGE

1) **Know basic definitions**: Field extension E/F (simple, algebraic, transcendental, finite, normal, separable, inseparable; degree $[E : F]$). $F(S), F[S]$ for subsets S of E/F. Minimum polynomial of algebraic element $a \in E/F$; degree of a over F. Splitting field of a polynomial over F. Characteristic, prime field.

2) **Know**: Transitivity of degree $[K : F] = [K : E][E : F]$.

3) **Know how to construct field extensions of F**: simple algebraic extension $E = F[x]/(p(x))$ for irreducible polynomial $p(x)$ in $F[x]$: will be simple algebraic extension of degree $[E : F] = \deg(p)$, generated by image of x with minimum polynomial p. Simple transcendental extension: $E = F(x)$ rational functions = field of fractions of $F[x]$.

4) **Know how to**: construct all finite fields $GF(q)$ ($q = p^e$, split $x^{p^e} - x$ over $\mathcal{Z}_p$).

PROBLEMS (F is an arbitrary field)

(1) [Feb 84 # 6] If $[F(a) : F]$ is odd show $F(a^2) = F(a)$.

(2) [May 89 # 3] If a, b are algebraic over F of degrees m, n, show $[F(a, b) : F] \leq mn$, with equality if m, n are relatively prime. Give an example where the inequality is strict.

(3) [Aug 89 # 5] If $[E : F]$ is finite, show any ring endomorphism of E which fixes F is an automorphism of E.

(4) [Nov 77 # 4] Define *finite* extension and *algebraic* extension; does either imply the other?

(5) [Ap 77 # 4b] If $p(x) \in F[x]$ is irreducible, SHOW there is a finite extension E/F containing a root of $p(x)$.

(6) [Sep 83 # 3] (a) Show any finite subgroup of $F^\times$ (the multiplicative group of invertible elements of F) must be cyclic. (b) Give an example of a finite nonabelian group contained in $R^\times$ for a ring R.

(7) [Ap 77 # 2] If F is finite SHOW (a) $|F| = q$ is a power of a prime p, (b) F splits $x^q - x$ over $\mathcal{Z}_p$, (c) $F^\times$ is cyclic of order $q - 1$.

(8) [May 78 # 10] Give a polynomial whose splitting field is a field of 9 elements; repeat for 18 elements.

(9) [Sep 86 # 1] If $F = GF(7)$, show $p(x) = x^2 + 1$ and $p(x) = x^3 + x + 1$ are irreducible in $F[x]$, and show $F[x]/(p(x))$ are fields (give their cardinalities).

(10) [May 92 # 6] Show that $f(x, y) = x + x^3y + y^8 + x^7y^5 + x^2y^4$ is irreducible over the rational field.

(11) [Jan 98 # 6] The finite field $GF(32)$ of 32 elements can be constructed as the extension $GF(2)(\beta)$ where β is a root of the polynomial $x^5 + x^2 + 1$ in $GF(2)[x]$. Find the minimal polynomial of β^3 over $GF(2)$.

(12) [Aug 94 # 6] Show that $F = GF(2)[x]/(x^4 + x + 1)$ is a field of characteristic 2 containing a primitive 15-th root of unity. Exhibit such a root.

(13†) [Sep 84 # 7] Factor $x^8 - 1$ into irreducibles in $\mathcal{Z}_p[x]$ for all primes p.

(14) [Aug 89 # 3] Show the set of all 2×2 matrices $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ over $GF(5)$ form (under the usual matrix addition and multiplication) a field of size 25.

(15) [1985 # 3b] Show the set of all 2×2 matrices $\begin{pmatrix} a & b \\ \lambda b & a \end{pmatrix}$ over $GF(7)$ form (under the usual matrix addition and multiplication) a ring of size 49. For which $\lambda \in GF(7)$ is this a field?

(16) [Sep 82 # 4] If E/F is algebraic and each $a \in E$ belongs to a normal sub-extension E_a ($F \subseteq E_a \subseteq E$), show E/F is normal.

(17) [Nov 77 # 3] Give an example of an inseparable extension E/Q of degree 7.

(18) [Jan 95 # 3] Let K and L be finite extensions of a field F, both contained in a field E. Let KL be the set of finite sums of products of members of K and L. Explain why KL is a subring of E that is finite-dimensional over F. From that, show that KL is a field and, in fact, the smallest subfield of E containing K and L.

(19) [Jan 94 # 7] In a field, if $t^m = 1$ and $t^n = 1$ for two relatively prime exponents m and n, then $t = 1$. Explain how this implies the following result for an integral domain: if $a^m = b^m$ and $a^n = b^n$ for two relatively prime exponents m and n, then $a = b$.

(20) [Sep 93 # 4] Prove that the additive group $(F, +)$ of a field F can never be isomorphic to the multiplicative group $(F^\times, \cdot)$. [Hint: consider orders of elements in the two groups.]

(21) [Aug 97 # 3] Let $K(x)$ be the field of rational functions over the field K. Prove *Luroth's Theorem*: for any nonconstant function $f \in K(x)$ the degree $[K(x) : K(f)]$ is finite. Can you describe $[K(x) : K(f)]$ in terms of f?

Handout # 9 August 3, 1999

9. GALOIS THEORY

GALOIS KNOWLEDGE

Definitions

1) **Element Definitions**: An element of E/F is *algebraic, transcendental* (= not algebraic), *separable* (= minimum polynomial is separable, no repeated roots), *inseparable* (= not separable), *minimumum polynomial* of an algebraic element.

2) **Polynomial Definitions**: $f(x) \in F[x]$ is *separable* (irreducible factors have simple [non-repeated] roots), has *discriminant* d_f ($\prod_{i<j}(r_i - r_j)^2$ over roots r_i); f is *solvable by radicals*; *Galois group* G_f; *splitting field* $Split(f/F)$ of a polynomial over F.

3) **Extension Definitions**: A field extension E/F is *finite* (finite *degree* $[E : F] = \dim_F E$), *simple* ($E = F(a)$ has one generator), *algebraic* or *separable* (all its elements are algebraic or separable over F), *transcendental* or *inseparable* (= not algebraic or not separable; inseparable extensions exist only in characteristic p); *normal* (an irreducible $f \in F[x]$ which has one root in E splits entirely over E), *Galois* ($Gal(E/F)$ fixes precisely F), *Galois group* $Gal(E/F)$ (= $Aut(E/F)$ automorphisms of E fixing F pointwise).

4) **Field Definitions**: *finite* field, *Galois* field $GF(q)(q = p^n)$, *Frobenius automorphism* $\mathcal{F}$.

Consequences of Transitivity

1) **Transitivity of Degree**: $[E : F] = [E : K][K : F]$ for $E \supseteq K \supseteq F$.

2) **Constructibility Criterion**: A complex number z is *constructible by ruler and compass constructions* from Q iff $[Q(z) : Q] = 2^n$ is a power of 2 (ie. z is algebraic of degree 2^n).

3) **Applications**: 3 Problems of Classical Antiquity are Unsolvable: (1) Squaring the circle, (2) Trisecting the angle, (3) Duplicating the cube. (Gauss) Regular n-gon is constructible iff $n = 2^e p_1 \ldots p_s$ for distinct Fermat primes $p_i = 2^{2^{t_i}} + 1$.

Minimum Polynomials

1) **Simple Algebraic Extension**: (i) the minimum polynomial of any algebraic element u is irreducible; if u satisfies some irreducible $f(x)$ over F, then $f(x)$ MUST be the minimum polynomial; (ii) u is algebraic over F iff $F(u) = F[u]$ is a finite extension of F (in which case $F(u)$ is isomorphic to $F[x]/(f(x))$ for $f(x)$ the minimum polynomial; (iii) a polynomial $f(x)$ has distinct roots in any (hence all) extension iff $(f, f') = 1$.

Splitting Fields

1) **Existence and Uniqueness** of the splitting field $Split(f/F)$.

2) **Extension of Isomorphism** $F \to F'$ to isomorphism $E = Split(f/F) \to E' = Split(f'/F')$ in at most $[E : F]$ ways (exactly this many if $f(x)$ is separable).

3) **Characterization**: finite E/F is normal (resp. Galois) iff it is the splitting field of a (resp. separable) polynomial.

Galois Theory

1) **Fundamental Theorem of Galois Theory**: the Galois correspondence [subextension K of E/F corresponds to $H = Gal(E/K)$ in $G = Gal(E/F)$, subgroup H corresponds to fixed field of invariants $Fix(H) = Inv(H)$] is (1) an order-reversing bijection between all subextensions and all subgroups; (2) has $\mid H \mid = [E : K] = h$, $[G : H] = [K : F] = k$; (3) H is normal in G iff K/F is normal iff K is closed under the action of $Gal(E/F)$, and in this case $Gal(K/F)$ is isomorphic to G/H.

$$\begin{array}{rcrcrcr}
E & & 1 & \qquad & E & & 1 \\
h| & & h| & & H| & & | \\
K & (2) & H & & K & (3) & H \\
k| & & k| & & G/H\| & & \| \\
F & & G & & F & & G
\end{array}$$

2) **Galois' Criterion**: f is solvable by radicals iff G_f is a solvable group.

3) **Abel-Ruffini Theorem**: The general equation of degree $n > 4$ is not solvable by radicals (since its Galois group is S_n).

4) **Existence**: There exist degree 5 equations over Q which are not solvable by radicals.

5) **Galois Group as Permutations**: G_f imbeds in S_n (permutes n roots of f); it is transitive iff f is irreducible.

6) **Evenness**: The even permutations $G_f \cap A_n$ correspond to the extension $F(\sqrt{d_f})$, so G_f is contained in A_n iff $\sqrt{d_f}$ exists in F; an irreducible cubic has Galois group S_3 iff $\sqrt{d_f}$ not in F, has group A_3 iff $\sqrt{d_f}$ in F.

BE ABLE TO FIND EASY GALOIS GROUPS ON THE EXAM !!

(I) general equation of degree n over F (S_n).

(II) $x^p - a$ in characteristic p (irreducible iff $a \neq b^p$ for $b \in F$, single root b, $G_f = 1$).

(III) $x^p - x - a$ in characteristic p (irreducible iff $a \neq b^p - b$ for $b \in F$, roots $\{b, b+1, \ldots, b+p-1\}$, $G_f = (Z_p, +)$ abelian consisting of $\sigma_i(b) = b + i$, cyclic generated by σ_1).

(IV) $x^n - a$ in characteristic not dividing n WITH $\zeta \in F$ for primitive n-th root of unity ζ (irreducible only if $a \neq b^n$ for $b \in F$; this is sufficient if n

is prime), roots $\{b, b\zeta, b\zeta^2, \ldots, b\zeta^{n-1}\}$, G_f abelian subgroup of additive group $(Z_n, +)$ of integers mod n, consisting of $\sigma_i(b) = b\zeta^i$).

(V) $x^n - 1$ in characteristic not dividing n (roots $\{1, \zeta, \zeta^2, .., \zeta^{n-1}\}$ for primitive n-th root of unity ζ, G_f abelian subgroup of $(Z_n^\times, \cdot)$ multiplicative group of units in integers mod n), consisting of $\sigma_j(\zeta) = \zeta^j$ for $1 \leq j < n$ relatively prime to n, $\sigma_j \sigma_{j'} = \sigma_{jj'}$.

(VI) $x^n - a$ in characteristic not dividing n (roots $\{b, b\zeta, b\zeta^2, .., b\zeta^{n-1}\}$ for primitive n-th root of unity ζ, G_f subgroup of *semidirect product* $(\mathcal{Z}_n, +) \times (\mathcal{Z}_n^\times, \cdot)$ of additive group of integers mod n with multiplicative group of units of ring Z_n, consisting of $\sigma_{ij}(b\zeta^m) = b\zeta^{i+jm}$; USUALLY NONABELIAN if $\zeta \notin F$ with $\sigma_{i,j}\sigma_{i',j'} = \sigma_{i+ji',jj'}$.

Finite Fields

Finite Field Theorem: (1) A finite field F has order $q = p^n$ a power of a prime ($p =$ characteristic of F, $n = [F : Z_p]$); (2) There exists one and (up to isomorphism) only one finite field of order q for each $q = p^n$, namely $GF(q) = Split(x^q - x/Z_p)$; (3) $GF(q)$ is Galois over $\mathcal{Z}_p$ with Galois group $< \mathcal{F} > \cong \mathcal{Z}_n$ cyclic of order n; (4) $GF(p^n)$ contains a subfield $GF(p^m)$ iff $m \mid n$, in which case $Gal(GF(p^n)/GF(p^m)) \cong < \mathcal{F}^m > \cong Z_{\frac{n}{m}}$.

Groups

1) **Definitions**: *Solvable, nilpotent group; normal series, composition series, derived series; factors* of a normal series, *equivalence* of two normal series (have the same factors, up to order and isomorphism); *commutator* $[h, k]$ ($:= hkh^{-1}k^{-1}$), *commutator subgroup* $[H, K]$, *derived* or *commutator group* G', n-th *derived group* $G^{(n)} := [G^{(n-1)}, G^{(n-1)}]$; nilpotence chain $G^n = [G^{n-1}, G]$.

2) **Solvability Theorems**: G solvable iff some n-th derived group $G^{(n)} = 1$ (G nilpotent iff some $G^n = 1$); if K is a normal subgroup of G then G is solvable iff both G/K and K are solvable.

3) **Symmetric Group**: A_n is simple for $n \geq 5$, so S_n is not solvable for $n \geq 5$.

4) **Jordan-Hölder Theorem**: Any two composition series are equivalent.

5) **Schreier Refiniement Theorem**: Any two normal series have equivalent refinements.

TYPICAL PROBLEM

Given polynomial $f(x)$ or element β over F, find $G = Gal(f/F)$ or $Gal(F(\beta)/F)$, find all subgroups of G and subfields of $E = Split(f/F)$, and set up the Galois correspondence.

(1) [Jan 82 # II] $F = Q$, $f = x^3 + 5x - 5$ (show f is irreducible, find its real roots; is f solvable by radicals?)

(2) [Ap 77 # 6] $F = Q,\ f = x^3 + 5$ (show f is irreducible but G is not of order 3; is f solvable by radicals?)

(3) [Aug 88 # 5; Sep 80 # 7] $F = Q,\ f = x^4 - x^2 - 6$.

(4) [Jan 87 # 3] $F = Q,\ f = x^4 - x^2 - 2$.

(5) [Sep 86 # 4] $F = Q,\ f = x^4 + 1$.

(6) [Jan 95 # 7] $F = Q,\ f = x^4 - 2x^2 - 2$ (show f irreducible, describe G as permutations of roots).

(7) [May 91 # 5] $F = Q,\ f = x^4 - 2$ (find G, identify all subfields of degree 4 over Q with their corresponding subgroups).

(8) [Jan 94 # 2] $F = Q,\ f = x^4 - 2$ (show G isomorphic to the dihedral group of order 8).

(9) [Aug 95 Comprehensive # 3] $F = Q,\ f = x^4 - 4$ (describe G as automorphisms, find all subfields).

(10†) [Sep 82 # 5] $F = Q,\ f = x^4 + 2x^2 + 2$.

(11) [Jan 97 # 5] $F = Q,\ f = x^4 - 5$ (descibe G as a group of permutations of the roots).

(12) [March 83 # 2] $F = Q,\ \beta = (1 + \sqrt{2})/(1 + \sqrt{3})$.

(13) [Jan 98 # 5a] $F = Q,\ f = x^5 + 5x^3 - 20x + 10$.

(14) [Sep 93 # 6] $F = Q,\ f = x^5 - 6x + 3$ (prove f is (a) irreducible, (b) has exactly 3 real roots, (c) $G(E/L)$ contains a transposition of roots of f for any real subfield L of the splitting field E of f over Q, (d) $G(E/Q) = S_5$, (e) $0 < r \in Q, \sqrt{r} \notin Q \Longrightarrow \sqrt{r} \notin E$).

(15) [Jan 81 # 2] $F = Q,\ \beta =$ primitive 7-th root of unity (find the minimum polynomial of β, find $[Q(\beta) : Q]$, find all subfields).

(16) [Nov 77 # 8] Find $Gal(E/Q)$ if $E = Q(i, \beta)$ for β a primitive n-th root of unity for odd $n > 1$.

(17) [Jan 79 # 6; Sep 79 # 6] Find $Gal(E/Q)$ for $E = Q(\sqrt{2}, i)$ or $E = Q(i + \sqrt{2})$.

(18) [Aug 89 # 8] If $\beta = \sqrt{2 + \sqrt{2}}$, show $Q(\beta)/Q$ is Galois with G cyclic; set up the Galois correspondence.

(19) [May 78 # 11] Describe all intermediate fields of E/F if E/F is Galois with group $Gal(E/F) = S_3$.

(20) [Jan 89 # 4; Feb 84 # 2] (a) Find $Gal(x^3 - 2/Q)$. (b) Find $f(x) \in Q[x]$ with $Gal(f/Q) = \mathcal{Z}_2 \times S_3$.

(21) [1985 # 4] Let E_n be the splitting field of $x^n - 1$ over Q. (a) What is $[E_n : Q]$? (b) What is $\mid G_n \mid$ for $G_n = Gal(E_n/Q)$? PROVE G_n is abelian. (c) SHOW G_{16} is not cyclic.

(22†) [Sep 83 # 4] If $x^4 + ax^2 + 1$ is separable and irreducible over F, find all roots and their relationships, find G. Show that F must be infinite.

(23) [May 80 # 6] If $F = Q(\zeta)$ for a primitive n^{th} root of unity, and $b^n = a \in F$ where $a \notin F^n$ is not an n^{th} power in F, show $G(F(b)/F)$ is abelian.

RELATED PROBLEMS

(1) [Jan 92 # 3] If ω is a primitive cube root of 1, determine whether $Q(\omega^3\sqrt{2})$ is a Galois extension of Q. Give reasons.

(2) [May 90 # 3] If E/Q is a finite Galois extension inside $\mathcal{C}$ with $Gal(E/Q)$ simple of order > 2, show the imaginary unit i CANNOT belong to E.

(3) [May 89 # 6] If E/F is Galois with $Gal(E/F)$ simple, for any element $a \in E$ which is not in F show that E is a splitting field for the minimum polynomial of a over F.

(4) [May 80 # 6] If $F = Q(\beta)$ for a primitive n-th root of unity, and $b^n = a \in F$ where $a \notin F^n$ is not an n-th power in F, show $G(F(b)/F)$ is abelian.

(5) [Fall 87 # 8] If E/Q is a splitting field of an irreducible polynomial f of degree 8, and $a \in E$ is a root of f so that f splits over $Q(a)$ into 2 linear and 3 quadratic factors, find the possible orders of $Gal(E/Q)$ and show f is solvable by radicals.

(6) [Aug 97 # 1ac] Let p be a prime number and F a field containing p distinct p-th roots of unity. Let E/F be a Galois extension for which $[E : F] = p$. (a) Prove that the Galois group $Gal(E/F)$ is cyclic of order p. (b) Prove that there is an element $b \in E\backslash F$ with $b^p \in F$.

(7) [Aug 94 # 7] Let ζ_n be a primitive n-th root of unity in $\mathcal{C}$ for $n > 2$. (a) Show that the fixed field of $Q(\zeta_n)$ under complex conjugation is $Q(\zeta_n + \bar{\zeta}_n) = Q(\zeta_n) \cap \mathcal{R}$. [Hint: write $\bar{\zeta}_n$ as a power of ζ_n and find a polynomial of low degree satisfied by ζ_n over $Q(\zeta_n + \bar{\zeta}_n)$.] (b) For $n = 7$, find the Galois group of $Q(\zeta_7 + \bar{\zeta}_7)$, then find all subfields of $Q(\zeta_7)$ with their correponding groups.

(8) [Jan 87 # 4] If $F \subseteq K \subseteq E$ with K/F finite, show that if K/F is separable (resp. normal, Galois), then also $K(a)/F(a)$ is separable (resp. normal, Galois) for any $a \in E$.

(9) [Aug 95 # 6] Let E/Q be a splitting field of $x^3 - 9x + 12$. Show that there is a single normal extension F/Q with $E \neq F \neq Q$. Find $[F : Q]$.

(10) [Aug 98 # 7] Suppose that K is a finite Galois extension of the rational field Q which contains $\sqrt{3}$ and has cyclic Galois group $Gal(K/Q)$. Show that $L = Q(\sqrt{3})$ is the only quadratic extension of Q contained in K.

(11) Let E be a separable extension of the field F, with $[E : F] = n$. Use Galois theory to find an upper bound $B(n)$ for the number of intermediate fields K, $F \subseteq K \subseteq E$, that depends only on n. You don't need to make the bound $B(n)$ very tight!

(12) [Aug 96 # 6] Let E/F be a finite Galois extension with Galois group G. The *Normal Basis Theorem* states that there is an element u in E whose images under the elements of G form an F-basis of E. Prove that for any subgroup H of G, the subfield corresponding to H in the Galois correspondence is $F(u_H)$ for $u_H = \sum_{h\in H} h(u)$.

(13) [Jan 95 # 8] Give an example of a polynomial $f(x) \in Q[x]$ having all these properties: (1) degree 4; (2) no rational roots; (3) no repeated factors in $Q[x]$; (4) its Galois group over Q is cyclic of order 2.

(14) [Sep 78 # 4] (a) If f is irreducible of degree 5 over Q, show $G(f/Q)$ contains an element of order 5. (b) Show $G(x^4+1/Q)$ has NO element of order 4. (c†) Show $G(x^4+x^3+1/Q)$ HAS an element of order 4.

(15†) [Sep 84 # 3] If E/Q is Galois of degree 4, prove $E = Q(\beta)$ for a root β of a polynomial x^4+ax^2+b; show $Gal(E/Q)$ is cyclic iff b is NOT in Q^2.

(16) [Jan 98 # 5b] The Galois group G of F of a polynomial $f(x) \in F[x]$ of degree 4 is known to contain a subgroup isomorphic to the dihedral group D_4. (a) Show that $f(x)$ is irreducible. (b) If some root r_i of $f(x)$ lies in the subfield $F(r_j, r_k)$ generated by two other roots, show $F(r_j, r_k)$ is a splitting field for $f(x)$ and that $G = D_4$.

(17†) [Jan 97 # 4] Let $f(x)$ be a monic polynomial in $\mathcal{Z}[x]$. Let p be a prime and let $\bar{f}(x)$ be the image of $f(x)$ in $\mathcal{Z}_p[x]$ obtained by reducing the coefficients of $f(x)$ modulo p. A theorem of Kronecker says that if $\bar{f}(x)$ has distinct roots in its splitting field, and if $\bar{\sigma} \in Gal(\bar{f}/\mathcal{Z}_p)$ then there is a $\sigma \in Gal(f/Q)$ having the same cycle structure as a permutation of the roots of $f(x)$ as $\bar{\sigma}$ does as a permutation of the roots of $\bar{f}(x)$. (a) Use this theorem (for a couple of choices of p) to show that the Galois group of x^4+4x^2+x+3 is isomorphic to S_4. (b) Apply the theorem to show that if $f(x)$ has even degree and the discriminant of $f(x)$ is a perfect square in $\mathcal{Z}$, then $\bar{f}(x)$ is reducible for each prime p.

(18) [Sep 83 # 8] If E/Q is Galois and $B(x,y) := Tr_{E/Q}(xy)$ (you may assume this is a nondegenerate bilinear form on $E \times E$ to Q), find the adjoints σ^* of the elements σ of the Galois group $G(E/Q)$ with respect to the bilinear form B.

(19) [Mar 83 # 7] (a) SHOW $E = GF(p^6)$ is Galois over $F = GF(p)$. (b) Express the trace $Tr_{E/F}(x)$ as a polynomial in x, and show there is an x with $Tr_{E/F}(x) \neq 0$. (c) Show $B(x,y) := Tr_{E/F}(xy)$ is a nondegenerate bilinear form on $E \times E$ to F.

Handout # 10. Bilinear Forms

KNOWLEDGE (V a vector space over F)

1) **Vector Space Definitions**: *Linear functional*, *dual space* V^* (all linear functionals), *dual basis* $\mathcal{B}^*$ (to a basis $\mathcal{B}$ for V); dual (or *adjoint*) $T^* : W^* \to V^*$ of a transformation $T : V \to W$ (defined by $T^*(f) = f \circ T$ for $f \in W^*$); *Bilinear form* B on V (bilinear map $V \times V \to F$) *left* and *right duality maps* $B_L, B_R : V \to V^*$ (via $B_L(x) := B(x, \cdot)$, $B_R(x) := B(\cdot, x)$); *skew, alternate, symmetric, nondegenerate, anisotropic* ($B(x,x) = 0 \Rightarrow x = 0$) bilinear form. *Orthogonal direct sum* $V_1 \perp V_2$, *isometry* $V_1 \to V_2$ of spaces with bilinear forms, *orthogonal* T (isometry $V \to V$). *Symplectic plane* for an alternate bilinear form (basis u, v with $B(u,v) = 1$, hence $B(u,u) = B(v,v) = 0$, $B(v,u) = -1$).

2) **Definitions for a given Bilinear Form** B : *Matrix* $Mat_{\mathcal{B}}(B)$ of B relative to an ordered basis $\mathcal{B} = \{x_1, \ldots, x_n\}$ of V ($\beta_{ij} = B(x_i, x_j)$); *left* and *right annihilators* $U^{\perp,L}$, $U^{\perp,R}$ of a subspace U (the vectors x killing U from the left or right, $B(x,U) = 0$ or $B(U,x) = 0$), *left* and *right radical* $Rad_L(B) = \ker(B_L) = V^{\perp,L}$, $Rad_R(B) = \ker(B_R) = V^{\perp,R}$, *left, right orthogonality, orthosymmetric* ($B(x,y) = 0 \Rightarrow B(y,x) = 0$). *Isotropic vector* ($B(x,x) = 0$).

3) **Know Facts**: (1) $Bil(V) \cong Hom(V, V^*)$ linear map (L or R) $V \to V^*$ (B gives $L = B_L$, $R = B_R$; L or B gives $B(x,y) = L(x)(y)$ or $B(x,y) = R(y)(x)$; (2) IF V IS FIN. DIM., nondegenerate bilinear form on $V \cong$ isomorphism (L or R) $V \to V^*$; a bilinear form B is *nondegenerate* $\Leftrightarrow$ *left nondegenerate* (left radical zero) $\Leftrightarrow$ *right nondegenerate* (right radical zero) $\Leftrightarrow$ some/any matrix of B is invertible ($\det(\beta_{ij}) \neq 0$), $Mat_{\mathcal{B}}(B) = Mat_{\mathcal{B}^*,\mathcal{B}}(R_B) = Mat_{\mathcal{B}^*,\mathcal{B}}(L_B)^t$, $Mat_{\mathcal{B}'}(B) = P^t Mat_{\mathcal{B}}(B) P$ for the *change-of-basis matrix* $P = Mat_{\mathcal{B}',\mathcal{B}}((Id)$.

4) **Orthosymmetric Theorem**: if V is finite dimensional of characteristic $\neq 2$, then B orthosymmetric $\Leftrightarrow$ alternate or symmetric.

5) **Basic Splitting Lemma**: any finite-dimensional nondegenerate subspace U of V is an orthogonal direct summand, $V = U \perp U^\perp$.

6) **Basic Structure Theorem**: (I) Any space with **alternate** form is a direct sum $V = P_1 \perp \ldots \perp P_r \perp R$ for R the radical, P_i symplectic planes; thus the rank of V is even and the determinant of any matrix of B is a square. (II) Any space with **symmetric** form is a direct sum $V = L_1 \perp \ldots \perp L_r \perp R$ for R the radical, L_i anisotropic lines (Fu_i with $B(u_i, u_i) \neq 0$); thus there is an orthogonal basis $\{u_1, \ldots, u_r, z_{r+1}, \ldots, z_{r+s}\}$ relative to which B has diagonal matrix. Over an algebraically closed field, we can assume all $B(u_i, u_i) = 1$; over the reals, we can assume all $B(u_i, u_i) = \pm 1$ (with the number of +1's, -1's, and 0's an invariant of B).

4) **Gram-Schmidt Orthogonalization Process** for Symmetric Bilinear Forms: Converts any ordered basis (or even spanning set) into an orthogonal basis (throwing out linearly dependent vectors); by normalizing the resulting vectors you get an orthonormal basis. Recipe: if $v_1, .., v_{r-1}$ have been converted to

orthogonal $w_1, .., w_{s-1}$ $(s \le r)$, replace v_r by $w_s = v_r - \sum_{i=1}^{s-1} B(v_r, w_i)/B(w_i, w_i) w_i$ (if w_s is 0, throw it out) obtained from subtracting off the orthogonal projections of v_r on the span of the previous w's. The method always works for positive definite, even anisotropic, forms, and often works for general nondegenerate symmetric bilinear forms, as long as none of the resulting w's is isotropic.

QUADRATIC FORM PROBLEMS

(1) [May 89 # 4] Find P so that $PMP^T = D$ is diagonal when $M = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}$ over a field of characteristic $\neq 2$.

(2) [Fall 87 # 5] Are the real quadratic forms with matrices $M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}$, $M_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ equivalent (i.e., are the matrices cogredient)?

(3) [May 91 # 3] Given the two quadratic forms $Q_i(x) = xA_ix^t$ where $A_1 = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}$ and $A_2 = \begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix}$, (a) are they equivalent forms over the rational field? (b) are they orthogonally equivalent over the real field?

(4) [May 78 # 9] Show any two eigenvectors for distinct eigenvalues of the matrix $\begin{pmatrix} 1 & 9 & 7 & 8 \\ 9 & 0 & 0 & 0 \\ 7 & 0 & 0 & 0 \\ 8 & 0 & 0 & 0 \end{pmatrix}$ are orthogonal.

(5) [Aug 94 # 5] If $f(x, y)$ is an alternating bilinear form on a 25-dimensional real vector space, and A is its matrix with respect to some basis, show that $\det(A)^{25} = 0$.

(6) [Jan 97 # 7] Let V be a finite-dimensional vector space over a field F, and let λ and μ be two linear functionals on V. Define $B(x, y) = \lambda(x)\mu(y) - \lambda(y)\mu(x)$ for $x, y \in V$. Show that B is an alternating bilinear form on V, and determine the possible values for its rank.

(7) [Aug 95 # 7] Show that every element of $SO_5(\mathcal{R}) = \{A \in GL_5(\mathcal{R}) \mid (Ax, Ay) = (x, y) \text{ and } \det(A) = +1\}$ [where $(x, y) = x \cdot y = x^t y$ is the usual dot product on $\mathcal{R}^5$] has a nonzero fixed point $Ax = x \neq 0$.

(8) [Aug 95 Comprehensive # 10] It is known that the space $M_n(\mathcal{R})$ of $n \times n$ real matrices is a real inner product space with inner product given by: $< A, B >= trace(AB^t)$, where B^t denotes the transpose of the matrix B. Let P be an invertible matrix and T the linear operator on $M_n(\mathcal{R})$ defined by $T(A) = P^tAP$. Denote the adjoint of T relative to this inner product by T^*. Prove that $T^*(A) = PAP^t$ for all A, and find necessary and sufficient conditions on the matrix P that $T = T^*$. Justify your answer.