**Qualifying Review Examination: Algebra**
**May 6, 2004**

Morning

Explain all of your answers. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ are the integers, rationals, reals, and complex numbers, respectively.

**1.** Let $p > 0$ be a prime number, $G$ a finite $p$-group, and $H$ a subgroup of $G$.

(a) Prove that there is a chain of subgroups $\{1\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_n = G$ where for all $i$, $1 \leq i \leq n$, $G_i$ has order $p^i$ and $H$ is one of the $G_i$.

(b) Prove that if $H$ is normal then there is a chain as in part (a) such that every $G_i$ a normal subgroup of $G$.

**2.** Let $p$ be a prime number and $A$ a $2 \times 2$ matrix of integers. Suppose that $\det(A) = p$. Determine the possible Smith normal forms for $A$ and $A^2$ (Smith normal forms of size $2 \times 2$ over $\mathbb{Z}$ will be diagonal matrices with nonnegative integer diagonal entries $d_1, d_2$ such that $d_1 \mid d_2$). You must show that every form on your list for $A^2$ actually occurs as a form for some $A^2$.

**3.** Let $L$ be the splitting field of a fifth degree polynomial $f$ over the rational numbers $\mathbb{Q}$, and assume that the Galois group of $L$ over $\mathbb{Q}$ is the alternating group $A_5$. You may use without proof that $A_5$ is a simple group of order 60.

(a) What is the dimension of $L$ as a $\mathbb{Q}$-vector space?

(b) Prove that no subfield of $L$ can have degree 2, 3, or 4 over $\mathbb{Q}$.

(c) Determine the number of subfields of $L$ of degree 12 over $\mathbb{Q}$.

(d) Are the roots of the equation $f(x) = 0$ expressible in terms of radicals over $\mathbb{Q}$?

**4.** Prove that a group of order $3^2 \cdot 17 \cdot 19$ is not simple. You may not quote the theorem that groups of odd order are solvable.

**5.** Let $B$ be a bilinear form on a finite dimensional vector space $V$ over the field $K$.

(a) Prove that the following three properties are equivalent:

(i) For some pair of bases $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$ of $V$, $\det(B(v_i, w_j)) \neq 0$.

(ii) For every pair of bases $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$ of $V$, $\det(B(v_i, w_j)) \neq 0$.

(iii) For every subspace $W$ of $V$, the natural linear map $V \to \mathrm{Hom}(W, K)$ is onto (the map takes $v \in V$ to the linear functional $x \mapsto B(v, x)$, $x \in W$).

(b) Suppose that the equivalent properties of (a) apply to $B$ and $V$. Assume that $B$ is alternating, i.e., $B(x, x) = 0$ for all $x \in V$ (so that $B(x, y) = -B(y, x)$ for all $x, y \in V$ as well). Let $u$ be any nonzero vector of $V$. Prove that there exists a vector $v \in V$ such that $B(v, v) = 0$ and $B(u, v) = 1$. Show that $V$ contains a subspace $Z$ such that

(1) $B(x, y) = 0$ for all $x \in P = Ku + Kv$, $y \in Z$ and

(2) $V$ is the direct sum of the subspaces $Z$ and $P$.

**Qualifying Review Examination: Algebra**
**May 6, 2004**

Afternoon

Explain all of your answers. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ are the integers, rationals, reals and complex numbers, respectively.

**1.** Prove from first principles that in a principal ideal domain, an irreducible element is prime. Prove also that a least common multiple of a pair of nonzero elements $a, b$ in a principal ideal domain is a generator of $(a) \cap (b)$.

**2.** Let $g \in S_{2n}$ (the symmetric group on $2n$ letters) be the product of $n$ mutually disjoint 2-cycles, and let $H = \{h \in S_{2n} : hg = gh\}$ be the centralizer of $g$. Show that $H$ has a normal abelian subgroup $N$ of order $2^n$ in which every element except 1 has order 2, and that $H/N \cong S_n$.

**3.** Suppose that the vector space $V$ of dimension $n$ over the field $K$ has a nilpotent endomorphism $S$ whose Jordan canonical form is just a single block, necessarily with zeros down the main diagonal and ones on the superdiagonal (or subdiagonal, if you prefer). Let $W \subseteq V$ be an $S$-invariant subspace of dimension $d$. Prove that the minimal polynomial for the map $S$ induces on $W$ is $x^d$, and that the the minimal polynomial for the map $S$ induces on $V/W$ is $x^{n-d}$. Prove also that if $U$ is any $S$-invariant subspace of dimension $d$, then $U = W$. Explicitly, what is the $K[x]$-module corresponding to $S$?

**4.** Let $K$, $L$ be finite fields, with $|K| = q$. For each of the statements below, indicate whether the statement is true or false, with a brief explanation of your answer.

(a) If $K \subseteq L$ is a field extension, then the extension is normal.

(b) If $K \subseteq L$ is a field extension, then the extension is Galois, and the Galois group is cyclic.

(c) For every positive integer $n$, $K$ has an extension field $L$ of degree $n$, unique up to $K$-isomorphism, and $|L| = q^n$.

(d) If one adjoins one root $\theta$ of a $K$-irreducible polynomial to $K$, then the polynomial splits over the extension field $K(\theta)$.

(e) If $|K| = p^m$ and $|L| = p^n$, where $p, m, n$ are positive integers and $p$ is prime, then $K$ is isomorphic with a subfield of $L$ if and only if $m|n$.

**5.** Let Tr denote the trace of a square matrix, and let $\beta(A, B) = \mathrm{Tr}(AB)$, a real-valued symmetric bilinear form on the ring $M_n$ of $n \times n$ real matrices. Find the signature of this bilinear form on the $n^2$-dimensional real vector space $M_n$.

## **Solutions**

Morning

**1.** (a) The existence of the part of the required chain within $H$ follows from the nilpotence of $p$-groups (or use part (b) with $H$ replacing $G$). To get the chain from $H$ to $G$ use induction on $|G|$. If $G$ is non-trivial, there is an element $z$ of order $p$ in its center, since it is nilpotent (and this is proved in part (b)), and, hence, a normal subgroup $< z >$ of order $p$. If $z \in H$, we may take a chain from $H/ < z >$ to $G/ < z >$ and take inverse images in $G$. If $z \notin H$, then $< H, z >$ has order $p|H|$ and the rest of the chain from $< H, z >$ to $G$ may be constructed working mod $< z >$. $\square$

(b) Use induction on $|G|$. The result is trivial if $|G| = \{1\}$. Consider the decomposition of $H$ into conjugacy classes under the action of $G$ on $H$ by conjugation. The number of elements in a class is the index of the stabilizer of an element in the class, and, hence, a power of $p$. If $H$ is non-trivial, there must be a class of size 1 other than the class of 1, or else $|H| \equiv 1 \bmod p$, and so $H$ meets the center of $G$. An element of order $p$ in the center of $G$ and in $H$, if $H$ is non-trivial, will generate a normal subgroup $G_1$ of $G$ (and of $H$, if it is non-trivial). Apply the induction hypothesis to $G/G_1$ and form a chain there as required: the inverse images in $G$ together with $\{1\}$ have the required property. $\square$

**2.** The product of the diagonal entries will be the determinant, up to sign. Therefore the only possibility for the diagonal entries of the Smith normal form for $A$ is 1, $p$. The only possibilities for the diagonal entries of the Smith normal form for $A^2$, which has determinant $p^2$, are 1, $p^2$ and $p$, $p$. The first clearly occurs for $A = \text{diag}\{1, p\}$ and the second occurs for $A = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}$.

**3.** The dimension of $L$ over $K$ is the same as the order of the Galois group $G = A_5$, and therefore it is 60. Subfields of degree $d$ correspond bijectively to subgroups of $G$ of index $d$. If $G$ had a proper subgroup $H$ of index $e \leq 4$, its action by left multiplication on the left cosets of $H$ is transitive, and would give a non-trivial homomorphism of $G$ into $S_e$, which has order $< 60$. The kernel would be a non-trivial proper normal subgroup of $G$, a contradiction. Subfields of degree 12 correspond to subgroups of order 5, and each of these is generated by a 5-cycle. The number of 5-cycles on 5 elements is $5!/5 = 24$, and there are four in each subgroup of order 5, so there are 6 subgroups of order 5, and six subfields of degree 12. (Alternate: by the Sylow theorems, the number is 1 mod 5 and divides 12: hence, since, since there cannot be a normal subgroup, the number is 6.) The roots cannot be expressed by radicals since the Galois group is not solvable.

**4.** More generally, consider a group of order $p^2qr$ where $p, q, r$ are distinct primes and $q = 2p^2 - 1$, $r = 2p^2 + 1$. The number of Sylow $q$-subgroups is congruent to 1 mod $q$ and divides $p^2r = (q + 1)(q + 2)/2 = 1 + q(q + 3)/2 \equiv 1 \bmod q$. It follows that the number is 1 or $p^2r$, since it is clear that $p$, $p^2$, and $r$ are not 1 mod $q$, and $pr \equiv 1/p$ (since $p^2r \equiv 1$). If the $q$-Sylow subgroup is not normal, this implies that there are $p^2r(q - 1)$ elements of order $q$, and hence only $p^2r$ of other orders. Similarly, the number of $r$-Sylow subgroups divides $p^2q$ and is 1 mod $r$, and $p^2q = (r - 1)(r - 2)/2 = 1 + r(r - 3)/2$, and so is 1 mod $r$.

It follows similarly that the number of Sylow $r$-subgroups is 1 or $p^2q$, and in the latter case that leaves only $p^2q$ elements of other orders. But then $p^r(q-1) < p^2q$, and $rq < r+q$, a contradiction. Thus, either the Sylow $q$-subgroup or the Sylow $r$-subgroup is normal. $\square$

**5.** (a) If $x_1, \dots, x_n$ and $y_1, \dots, y_n$ are any bases, and $S$, $T$ are nonsingular linear maps (giving changes of basis), then $\det\big(B(Sx_i, Ty_j)\big) = \det(S)\det(T)\det\big(B(x_i, y_j)\big)$. So, $\det\big(B(x_i, y_j)\big) \neq 0$ if and only if any $\det\big(B(Sx_i, Ty_j)\big) \neq 0$. Thus, (i) $\Rightarrow$ (ii). and (ii) $\Rightarrow$ (i) is obvious.

Assume (ii). Given $W$ and any basis of $W$, expand it to a basis $X$ of $V$. Choose a second basis $Y$ of $V$ which is dual to $X$ with respect to $B$. Row (or column) operations reduce this to the identity matrix. The corresponding new pair of bases is therefore in duality with respect to $B$. The restriction to $W$ of the first $\dim_K(W)$ of these gives the basis in $\mathrm{Hom}_K(W, K)$ dual to the original basis of $W$, whence the surjectivity of the natural linear map. Thus, (ii) $\Rightarrow$ (iii).

Assume (iii). Then (ii) follows trivially by taking $W = V$. We now have (i) $\Leftrightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (ii). $\square$

(b) Use (a) to get $x \in V$ so that $B(u, x) = 1$. Since $B$ is alternating $B(x, x) = 0$ and $B(x, u) = -B(u, x)$. Take $Z$ to be the kernel of the natural map to $Ku + Kx$. It has codimension 2 and meets $Ku + Kx$ in 0 since this 2-space is nonsingular. So $V$ is their direct sum. Orthogonality of the sum follows from the definition of $Z$. $\square$

Afternoon

**1.** Let $x$ be an irreducible element that divides $ab$. We must show that $x|a$ or $x|b$. Let $d$ be a generator of $(x, a)$. Then $d|x$ and $d|a$, and we may write $d = xr + as$. If $d$ is unit times $x$, then $x|a$ and we are done. If not, then, since $x$ is irreducible, $d$ is a unit, and we may assume that $d = 1$. Then $b = b(xr + as) = xbr + (ab)s$, and since $x$ divides both $xbr$ and $(ab)s$, $x$ divides $b$. $\square$[Alternate: $(x)$ must be contained in a maximal ideal $(y)$ and since $(y)$ is maximal it is prime, meaning that $y$ is prime. Since $y|x$ and $x$ is irreducible, $y$ is a unit times $x$. $\square$]

A common multiple of $a$ and $b$ is precisely the same thing as an element of $(a) \cap (b)$. A generator of the principal ideal $(a) \cap (b)$ is a common multiple, and every other common multiple is a multiple of the generator. $\square$

**2.** The effect of the action of $h$ on $g$ by conjugation in terms of the cycle decomposition may be seen by letting $h$ act directly, by permutation, on the elements of the cycle decomposition. Thus, $h$ is in the centralizer if and only if it permutes the $n$ two element sets that occur in the cycle decomposition of $G$. We therefore have a surjection of $H$ onto $S_n$, thought of as the permutations of these $n$ two element sets. The kernel may be thought of as permutations that map each of these two element sets into itself, which is the same as the group generated by the $n$ mutually disjoint 2-cycles that occur in the cycle decomposition of $g$. $\square$

**3.** The corresponding module over $K[x]$ is the cyclic $K[x]$-module $K[x]/x^n$. Invariant subspaces correspond to submodules, which are necessarily cyclic modules generated by powers of $x$: any element with nonzero constant is a unit, since the image of $x$ is nilpotent in the ring $K[x]/(x^n)$, and so every element is a power of $x$ times a unit. The submodule generated by $x^i$ has basis $x^i, x^{i+1}, \dots, x^{n-1}$, and so has dimension $n-i$ as a $K$ vector space. Thus, the $K$-vector space dimension of a submodule determines it uniquely. The cyclic module generated by $x^i$ is killed by $x^{n-i}$ and no lower power of $x$, and so is isomorphic with $K[x]/(x^{n-i})$, while the quotient by it $\cong K[x]/(x^i)$. Take $d = n-i$. Since the minimal polynomial of the matrix corresponds to the monic generator of the annihilator ideal in $K[x]$ of corresponding module, all of the statements follow.

**4.** All of the statements are true. A finite field with $q = p^N$ elements, where $p$ is the characteristic, is a splitting field of $x^q - x$ over $\mathbb{Z}/p\mathbb{Z}$, and so is normal even over $\mathbb{Z}/p\mathbb{Z}$. The derivative of $x^q - x$ is $-1$, which shows separability. Therefore a finite field is a normal and separable (i.e., Galois) extension of any subfield. Separability also follows because finite fields are perfect (the $p$th power map is injective since the nonzero elements form an abelian group of order relatively prime to $p$, and therefore bijective). By a theorem, the Galois group is cyclic, and generated by a suitable power of the Frobenius automorphism $F$ of the finite field. (If the smaller field has $p^m$ elements, the generator is $F^m$.) The unique field with $q^n$ elements is a degree $n$ extension of the unique field with $q$ elements, and is evidently the only degree $n$ extension. Adjoining one root of an irreducible polynomial produces the splitting field, because the extension is normal, as noted earlier. The final statement is true because if the smaller field has $q = p^m$ and the degree is $k$, the larger field is a $k$-dimensional vector space over the smaller and has $q^k = p^{mk}$ elements. The converse holds because a splitting field of $x^{q^k} - x$ obviously contains a splitting field of $x^q - x$.

**5.** Let $E_{ij}$ be the matrix with a 1 in $i, j$ positions and 0 elsewhere. These give a basis for $M_n$. Then $E_{ij}E_{h,k} = 0$ unless $j = h$, and then it is $E_{ik}$, which has trace 0 unless $i = k$. Group the basis into the $n$ elements $E_{ii}$, and the $n(n-1)/2$ pairs of elements $E_{ij}, E_{ji}$ for $j \neq i$. The $n^2 \times n^2$ matrix of the bilinear form is then the direct sum of $n$ one by one identity matrices and $n(n-1)/2$ matrices of the form $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ each of which has eigenvalues $1, -1$. Thus the signature, as a triple, is $(n + n(n-1)/2, n(n-1)/2, 0)$ (and the rank is $n^2$). If one uses the number of positive diagonal matrices minus the number of negative diagonal entries of an equivalent diagonal matrix, the signature is $n$. [Alternate: Call the signature, as a triple, $(p, q, r)$, where $p + q + r = n^2$. $M_n$ is the direct sum of the $n(n+1)/2$-dimensional space $S$ of symmetric matrices, on which the form is positive definite since each nonzero such $A$ is similar to a nonzero real diagonal matrix, and the $n(n-1)/2$-dimensional space $Q$ of skew symmetric matrices, on which the form is negative definite, since each nonzero such $A$ is similar to a nonzero diagonal matrix with pure imaginary entries. Thus, $p \geq n(n+1)/2$ and $q \geq n(n-1)/2$. Since $n(n+1)/2 + n(n-1)/2 = n^2$, we must have $p = n(n+1)/2$, $q = n(n-1)/2$ and $r = 0$. One may actually see that $S$ and $Q$ are orthogonal under $\beta$: they are the eigenspaces for the two eigenvalues $1, -1$ of the transpose map $T : M_n \to M_n$, and $T$ preserves $\beta$.]