Qualifying Review Examination: Algebra
September 11, 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 $p \geq 3$ be a prime integer. Let $G = \mathrm{Sym}_p$ be the group of all permutations of the integers $\{1, 2, \ldots, p\}$. Let $g \in G$ be the p-cycle $(1\ 2\ \cdots\ p)$. Determine explicitly the centralizer C of g in G and the normalizer H of $\langle g \rangle$ in G. In particular, what are the orders of C and H? Is H ever an abelian group?

2. For a field, F, let $F^\times$ be the multiplicative group of nonzero scalars and let $F^{\times n} := \{x^n | x \in F^\times\}$.
(a) Prove that $\mathbb{Q}^\times/\mathbb{Q}^{\times n}$ is an infinite group, for all $n > 1$.
(b) For a finite field, F, prove that $F^\times/F^{\times 2}$ has order 1 if $\mathrm{char}(F) = 2$ and has order 2 if $\mathrm{char}(F) > 2$.
(c) In a finite field, prove that any element is a sum of two squares (possibly including 0). *Hint:* Consider the possibility that the set of squares is a subfield.

3. Let f be a polynomial of degree 5 over $\mathbb{Q}$. Let L be its splitting field over $\mathbb{Q}$ and let G be the Galois group of L over $\mathbb{Q}$.
(a) Show that $[L : \mathbb{Q}] \neq 40$.
(b) Show that G contains no element of order 10.
(c) Show that the order of G is divisible by 5 if and only if f is irreducible.

4. Consider the bilinear form B defined on the vector space $Q = \{ax^2 + bx + c : a, b, c, \in \mathbb{R}\}$ of real quadratic polynomials define by $B(F, G) = \frac{d}{dx}(xFG)|_{x=1}$. For example, we have $B(x^2+1, x) = \frac{d}{dx}(x^4 + x^2)|_{x=1} = (4x^3 + 2x)|_{x=1} = 6$. Determine the rank and signature of B. Is it non-degenerate? Is it positive or negative definite or semi-definite?

5. (a) A linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^3$ as $\mathbb{R}$-vector spaces has matrix

$$A = \begin{pmatrix} 1 & 2 \\ -2 & 3 \\ 3 & -1 \end{pmatrix}$$

with respect to the standard bases. Find a matrix for $\bigwedge^2 T : \bigwedge^2 \mathbb{R}^2 \to \bigwedge^2 \mathbb{R}^3$. Specify the bases you use.
(b) Let V be a vector space over a field K. Explain carefully why there is a K-linear map $T : V \otimes V \to \bigwedge^2 V$ that sends $v_1 \otimes v_2 \mapsto v_1 \bigwedge v_2$. Is this map necessarily surjective? Show that this map is injective if and only if $V \cong 0$.

Qualifying Review Examination: Algebra
September 11, 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. Let G be the Galois group of the splitting field of $x^{420} - 1$ over the rational numbers $\mathbb{Q}$. Note that $420 = 4 \cdot 3 \cdot 5 \cdot 7$. In answering the questions below, state carefully any theorems you are using.

(a) What is the order of G? Explain the relation of G to the ring $\mathbb{Z}/420\mathbb{Z}$.

(b) Is G abelian? If so, express it as a direct product of cyclic groups of prime power order. Is G cyclic?

2. Let M be the complex vector space of $r \times r$ matrices over the complex numbers, where $r \geq 1$. Let S and T be $\mathbb{C}$-linear transformations from M to M, such that $S^r = T$, $T^r = S$, and S has r^2 mutually distinct eigenvalues. Prove that S and T are conjugate.

3. A group G of order 81 acts on a set S with 30 elements.

(a) Show that some element of S is fixed by at least 27 elements of G.
(b) How many elements of S are fixed by precisely 3 elements of G, assuming that there is at least one such element of S?

4. (a) Show that the Sylow 2-subgroup G of of Sym_4, the symmetric group on 4 elements, is generated by two involutions (elements of order 2), and so is a dihedral group of order 8.

(b) Show that G is a semidirect product of a normal subgroup K which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and a complement which is a subgroup R of G of order 2.

(c) Show that G has a subgroup S so that S is not the semidirect product of $S \cap K$ with some other subgroup of S.

5. Let E be a finite degree Galois extension of the field F such that E is the splitting field of a polynomial $p(x) \in F[x]$. We have an embedding of the Galois group $G := Gal(E/F)$ in the symmetric group Sym_n on n elements by action on the set of n distinct roots of $p(x)$. Assume that $n = 8$ and G is generated by $(1\ 2\ 3)(4\ 5\ 6)$, $(3\ 7\ 8)$ and $(1\ 2)(4\ 6)$. Prove that

(a) $p(x)$ is reducible.

(b) E is infinite.

Solutions

Morning

1. A p-cycle has $(p-1)!$ conugates, and its centralizer must have $p!/(p-1)! = p$ elements. Thus, $C = \langle g \rangle$. The subgroups of order p are disjoint except for the identity, and so there are $(p-1)!/(p-1) = (p-2)!$ of them. It follows that $H \supseteq C$ has order $p!/(p-2)! = p(p-1)$. an element $h \in H$ not in C must conjugate g to yield g^i, $2 \le i \le p-1$. g^i is represented by the cycle $h_i = (1\ \ 1+i\ \ 1+2i\ \ \cdots\ )$ (where the entries may be replaced by their least positive representative mod p). Thus, the permutation that sends k to the kth entry of h_i is in H, and these elements together with those in C generate H. H is never abelian.

2. (a) By unique factorization in the integers, the multiplicative group of $\mathbb{Q}$ is the direct sum of $\mathbb{Z}/2\mathbb{Z}$ and infinitely many copies of $\mathbb{Z}$. The subgroup, in additive notation, is the direct sum of $n(\mathbb{Z}/2\mathbb{Z})$ and infinitely many copies of $n\mathbb{Z}$, and the quotient will have a direct summand consisting of infinitely many copies of $\mathbb{Z}/n\mathbb{Z}$.

(b) If the finite field has order q its multiplicative group is cyclic of order $q-1$, and the quotient is $G/2G$, where $G \cong \mathbb{Z}/(q-1)\mathbb{Z}$. This is $\mathbb{Z}/2\mathbb{Z}$ if q is odd, and 0 if q is even.

(c) We continue the notation of (b). If q is even every element is a square and we are done. If q is odd, half the elements are squares. We have $(q-1)/2$ nonzero squares, and, so $(q+1)/2$ squares, which are clearly closed under multiplication. If these are closed under $+$ they will form a field (0 and 1 are among them, and the additive inverse of any element is an integer multiple of it while the multiplicative inverse of any element is a power of it). This is impossible, since $(q+1)/2$ does not divide q. Thus, we can choose $a^2 + b^2 = c$, a non-square, and necessarily nonzero. Its multiples by the nonzero squares d^2 give $(q-1)/2$ distinct non-squares, each of the form $(ad)^+(bd)^2$, and so give the remaining nonzero elements.

3. The group so generated is nonabelian, so G can not be the Galois group of a finite field, which is cyclic. Since G is not transitive on the roots of p, p is reducible.

4. If we use the basis $1, x, x^2$ and note that $B(x^i, x^j)$ is the value of $(i+j+1)x^{i+j}$ at 1, or $i+j+1$, we find that the matrix of B is

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix}.$$

The congruence (or cogredience) class of the matrix is unaffected if we perform an elementary row operation **and** the corresponding elementary column transformation. We subtract twice the first row from the second and twice the first column from the second. Then we subtract three times the the first row from the third and three times the first column from the third. This produces

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -2 \\ 0 & -2 & -4 \end{pmatrix}.$$

Subtracting twice the second row from the third and twice the second column from the third produces

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

Then B has rank 2 and signature $(1, 1, 1)$ (if given as a triple showing the number of diagonal entries that are positive, that are negative, and that are 0) or 0 (number of positive diagonal entries $-$ number of negative diagonal entries). B isn't non-degenerate, and is neither positive nor negative definite, nor semi-definite.

5. (a) Since e_1 maps to $e_1 - 2e_2 + 3e_3$ and e_2 maps to $2e_1 + 3e_2 - e_3$, $e_1 \bigwedge e_2$ maps to $(e_1 - 2e_2 + 3e_3) \bigwedge (2e_1 + 3e_2 - e_3)$ which simplifies to $((-2)(-1) - 3 \cdot 3)e_2 \bigwedge e_3 + (1(-1) - 3 \cdot 2)e_1 \wedge e_3 + (1 \cdot 3 - (-2)2)e_1 \bigwedge e_2 + = -7e_2 \bigwedge e_3 - 7e_1 \bigwedge e_3 + 7e_1 \bigwedge e_2$, and so the matrix is $(-7 \ \ -7 \ \ 7)$ with respect to the basis $e_1 \bigwedge e_2$ for $\bigwedge \mathbb{R}^2$ and the basis $e_2 \bigwedge e_3, e_1 \bigwedge e_3, e_1 \bigwedge e_2$ for $\bigwedge \mathbb{R}^3$. The simplification used that $e_i \bigwedge e_i = 0$ and $e_j \bigwedge e_i = -e_i \bigwedge e_j$.

(b) The map $V \times V \to \bigwedge^2 V$ that sends $(v_1, v_2) \mapsto v_1 \bigwedge v_2$ is K-bilinear by the basic properties of $\wedge$ and so there is an induced map $V \otimes_K V \to \bigwedge^2 V$ that sends $v_1 \otimes v_2 \mapsto v_1 \bigwedge v_2$. This map always surjective, since its image contains all the vectors $v_1 \bigwedge v_2$ for $v_1, v_2 \in V$, and these span $\bigwedge^2 V$. If $v \in V - \{0\}$ then $v \otimes v \neq 0$ and maps to 0 in $\bigwedge^2 V$, and so the map in injective if and only if $V = 0$.

Afternoon

1. (a) By a theorem, the Galois group of the splitting field of $x^n - 1$ over the rational numbers is isomorphic to the multiplicative group of units in the ring $\mathbb{Z}/n\mathbb{Z}$, and therefore has order $\Phi(n)$, where Φ is the Euler Φ-function. In this case $\mathbb{Z}/420\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, and so the multiplicative group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ (for the latter three factors note that the multiplicative group of a finite field is cyclic). It has order 96.

(b) Since the last factor is also $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, we may also write this as $(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. This group is abelian, but not cyclic, since there are repeated factors of prime power order for the prime 2.

2. Let $n = r^2$. $S^n = (S^r)^r = T^r = S$, and so S satisfies $x^n - x = 0$, as do all of its n distinct eigenvalues. The roots of this equation are 0 along with the root of $x^{n-1} - 1 = 0$, which are distinct, since the derivative is $(n-1)x^{n-2}$ and has no common root with $x^{n-1} - 1$. It follows that the eigenvalues of S must be exactly the n roots of $x^n - x = 0$, and so S is diagonalizable and has a diagonal matrix A with the n roots of $x^n - x$ on the diagonal. It suffices to see that A^r, which will be a matrix of T, has the same eigenvalues, and this simply means that the map $\lambda \mapsto \lambda^r$ maps the roots of $x^n - x$ to themeselves bijectively. Clearly, 0 is fixed, and so it suffcies to show that the map is bijective on the roots G of $x^{n-1} - 1$: these form an abelian group of order $n - 1$, and the map is a group endomorphism θ of G. The kernel is 1, for if $\lambda^r = 1$ and $\lambda^{n-1} = 1$, the order of λ divides both r and

$r^2 - 1$, and, hence, $r(r) - (r^2 - 1) = 1$. Since the map $\theta : G \to G$ is injective, it must be bijective. $\square$

3. The set S breaks up into orbits under the action of G: the length of the orbit of $s \in S$ is the index of the stabilizer H of s in G and so divides 81 and must be 1, 3, 9, 18, 27, or 81, and 81 is obviously not possible.

(a) 30 cannot be expressed as a sum of the numbers 9, 18, 27 even if repetitions are allowed, and so there is either an orbit of length 1 or of length 3. The stabilizer is then of order 81 or 27, and so an element in such an orbit is fixed by at least 27 elements.

(b) If s is fixed by exactly 3 elements of G its stabilizer has order 3, and its orbit has length 27. There can only be one such orbit, and so there are precisely 27 such elements, assuming that there is at least one.

4. (a) The Sylow 2-subbgroup is the same as the group of symmetries of a square whose consecutive vertices, numbered, say. clockwise, are given the numbers 1, 2, 3, 4. This group of order 8 is generated is generated, for example, by a reflection in a line bisecting two opposite sides such as $(1\ 2)(4\ 3)$ and and a reflection in a diagonal, such as $(1\ 3)$. Since these elements of order 2 do not commute, they cannot generated a subgroup of order 4, and so must generate the whole group.

(b) First solution. One definition of a dihedral group is a group generated by two involutions. Let t, u be such a pair of elements for G. Neither is equal to z, the unique involution in $Z(G)$, which has order 2. Therefore, one can take K to be generated by t, z, as t and z commute. Since K is proper in G, K fails to contain u (since t, u generate G). So, we take R to be the subgroup generated by u. Trivially, $R \cap K = 1$ and $G = RK$.

Second solution. A dihedral group is generated by a maximal cyclic subgroup (generator c) and an involution (say x) which inverts it under conjugatation. In the case of dihedral group of order 8, one computes that x and $c^{-1}xc$ commute and generate a normal subgroup, K. Since K has order 4, it is maximal. It suffices to find an involution outside K to generate a complementing subgroup. Use cx.

(c) Let S be the cyclic subgroup of order 4 used in the definition of a dihedral group of order 8. Then $S \cap K$ is cyclic (subgroups of cyclic groups are cyclic). Also, $SK = G$ (since K has index 2 and S is not contained in K, because K has exponent 2 and S has an element of order 4). Therefore, $S \cap K$ has order 2.

We seek a subgroup T of order 2 in S so that $S = T(S \cap K)$ and $1 = T \cap (S \cap K) = T \cap K$. However, there is only one subgroup of S of order 2, by cyclicity, which must be $S \cap K$. So, T is in $S \cap K$. Therefore, such T fails to exist and so S fails to be a semidirect product in the specified way.

5. The group so generated is nonabelian, so G cannot be the Galois group of a finite field, which is cyclic. Since G is not transitive on the roots of p (1,2,3,7, and 8 are in one orbit while 4,5,6 are in a different orbit), p is reducible.