

**Algebra Qualifying Examination**  
**Outline of Solutions - August 1998**

1. Show that a group of order 72 is solvable. Hint:  $G$  acts by conjugation on the set of Sylow 3-subgroups of  $G$ .

Fact: If  $f : G \rightarrow H$  is a homomorphism and  $\text{im}(f)$  and  $\text{ker}(f)$  are solvable, then  $G$  is solvable.

By the Sylow theorems,  $G$  has one or four Sylow 3-subgroups. Let  $P$  be one such, and let  $N(P)$  be its normalizer.

If  $G$  has one Sylow 3-subgroup  $P$ , it is normal, and we apply the fact to the canonical homomorphism  $G \rightarrow G/P$ .

If  $G$  has four Sylow 3-subgroups, the action of  $G$  by conjugation gives a homomorphism  $f : G \rightarrow S_4$ , where  $S_4$  is the symmetric group on four letters, a solvable group. The kernel of  $f$  is a subgroup of  $N(P)$ , a group of order 18, so it is solvable too. Thus the fact applies again.

2. Let  $K = GF(81)$  be the field with 81 elements, and let  $F = GF(3)$  be the prime subfield of  $K$ . Determine the cardinalities of the following two sets.

(A) The set of elements of  $K$  which generate  $K$  as a field over  $F$ .

(B) The set of elements of  $K$  which generate  $K^* = K - \{0\}$  as an abelian group under multiplication.

(A) The subfields of  $K$  are  $GF(3) < GF(9) < GF(81)$ . An element of a finite field  $K$  generates it as a field if and only if it does not lie in any proper subfield. Hence the number of field generators is  $81 - 9 = 72$ .

(B) Since  $K^*$  is a cyclic group of order  $80 = 16 \times 5$ , the number of abelian group generators is  $\phi(80) = \phi(16) \times \phi(5) = 8 \times 4 = 32$ , where  $\phi$  is Euler's phi-function.

3. Let  $R$  be a commutative ring with unit 1. Show that an element  $r$  of  $R$  is nilpotent if and only if it belongs to every prime ideal of  $R$ .

Suppose  $r^n = r \times r \times \cdots \times r = 0$ . If  $P$  is a prime ideal, then  $0 \in P$ , so one of the factors belongs to  $P$ . I.e.,  $r \in P$ .

Suppose that  $R$  is not nilpotent. Then 0 does not lie in the multiplicative set  $\{1, r, r^2, r^3, r^4, \dots\}$ ,

so  $\{0\}$  is an ideal disjoint from this multiplicative set. By Zorn's lemma, the set of ideals of  $R$  which are disjoint from this multiplicative set contains a maximal element  $J$ . Now one shows that  $J$  is prime, and then it is a prime ideal of  $R$  which does not contain  $r$ .

4. Let  $S_4$  be the symmetric group on four letters, with elements of  $S_4$  expressed as products of disjoint cycles. (With multiplication  $(12)(23) = (123)$ ). Let  $H$  be subgroup of  $S_4$  generated by  $(12)$  and  $(34)$ . Express  $S_4$  as a disjoint union of  $H - H$  double cosets, and determine the number of elements in each double coset.

If  $H$  and  $K$  are subgroups of a finite group  $G$ , then  $|HaK| = |H||K|/|H \cap aKa^{-1}|$ . Thus, in the present problem, for any  $a$  in  $S_4$ ,  $|HaH| = 4, 8$ , or  $16$ . For  $a = (13)$ ,  $H \cap aHa^{-1} = \{1\}$ , so  $|HaH| = 16$ . For  $b = 1$  and  $c = (13)(24)$ , which normalize  $H$ ,  $HbH = H$  and  $HcH = Hc \neq H$ , so  $|HbH| = |HcH| = 4$ . Since we have a total of  $16 + 4 + 4 = 24$  elements in disjoint double cosets, we have the desired decomposition.

5. Let  $H$  and  $K$  be normal subgroups of a group  $G$  whose intersection is the trivial group. Show that each element of  $H$  commutes with each element of  $K$ .

Let  $h \in H$ ,  $k \in K$ . Then  $kh^{-1}k^{-1} \in H$  and  $hkh^{-1} \in K$ , so  $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) = (hkh^{-1})k^{-1}$  lies in both  $H$  and  $K$ , and so equals the identity. Thus  $h$  commutes with  $k$ .

6. Let  $p$  be an odd prime integer which has the property that all primes smaller than  $p$  divide  $p - 1$ . Show that  $p = 3$ . Hint: Consider  $p - 2$ .

If  $q$  is a prime divisor of  $p - 2$  it divides  $p - 1$ , a contradiction since  $p - 2$  and  $p - 1$  are relatively prime. Hence  $p - 2$  is a positive integer with no prime divisors, so  $p - 2 = 1$ , and  $p = 3$ .

7. For a  $3 \times 3$  matrix  $X$  over the complex numbers, let  $C(X)$  be the centralizer of  $X$ , the set of  $3 \times 3$  matrices which commute with  $X$ . Show that the vector space dimension of  $C(X)$  over the complex numbers is at least three.

We will prove the more general result that for an  $n \times n$  matrix  $X$ , the dimension of  $C(X)$  is at least  $n$ . Since  $C(UXU^{-1}) = UC(X)U^{-1}$  for any invertible matrix  $U$ , it suffices

to prove the theorem when  $X$  is in Jordan canonical form. Then  $X$  is a block diagonal matrix whose diagonal blocks  $X_1, \dots, X_k$  are elementary Jordan blocks. Note that if  $Z$  is an elementary  $r \times r$  Jordan block, then  $l, Z, Z^2, \dots, Z^{r-1}$  are linearly independent, so  $C(Z)$  has dimension at least  $r$ . Let  $Y_i$  be the  $n \times n$  matrix which has the  $r_i \times r_i$  block  $X_i$  in the same place it occurs in  $X$ , and zeros elsewhere, and let  $l_i$  denote the  $n \times n$  matrix with an  $r_i \times r_i$  identity matrix in that block and zeros elsewhere. Then the  $n$  matrices  $l_1, Y_1, \dots, Y_1^{r_1-1}, \dots, l_k, Y_k, \dots, Y_k^{r_k-1}$  are linearly independent and centralize  $X$ .

8. Let  $K$  be a splitting field for  $x^7 - 5$  over  $Q$ , the field of rational numbers. Determine the Galois group  $G = G(K/Q)$ .

If  $a$  is one root of  $f(x) = x^7 - 5$  and  $1, w, w^2, \dots, w^6$  are the seventh roots of unity, then the roots of  $f(x)$  are  $\{aw^i, i = 0, 1, \dots, 6\}$ . Any automorphism of  $K/Q$  is completely determined by what it does to  $w$  and  $a$ . Moreover, any map  $w \rightarrow w^i (i = 1, \dots, 6)$ ,  $a \rightarrow aw^k (k = 0, \dots, 6)$  extends uniquely to an automorphism of  $K/Q$ . Thus  $G$  has order 42. If we let  $\sigma$  and  $\tau$  be the automorphisms defined by  $\sigma(w) = w^3, \sigma(a) = a, \tau(w) = w, \tau(a) = aw$ , we see that  $\sigma^6 = 1, \tau^7 = 1$ , and  $\sigma\tau\sigma^{-1} = \tau^3$ . This information determines  $G$ .

9. Give an example of a polynomial with rational coefficients with splitting field  $L$  such that the Galois group of  $L$  over  $Q$  is cyclic group of order 3.

Let  $w$  and  $\sigma$  be as in problem 8 above. Then  $G(Q(w)/Q)$  is cyclic of order 6. We get a Galois extension of degree 3 by taking the fixed field of  $\sigma^3$ , which is generated by  $w + \sigma^3(w) = w + w^6$ . The orbit of  $w + w^6$  under  $\sigma$  is  $\{w + w^6, w^2 + w^5, w^3 + w^4\}$ . Thus one polynomial which does the job is

$$(x - w - w^6)(x - w^2 - w^5)(x - w^3 - w^4) = x^3 + x^2 - 2x - 1.$$

10. Let  $R$  be a ring and let  $M$  be a left Noetherian  $R$ -module. (I.e., There is no properly ascending chain  $M_1 < M_2 < M_3 < \dots$  of submodules of  $M$ .) Suppose that  $f : M \rightarrow M$  is an  $R$ -module homomorphism which is onto. Show that  $f$  is an isomorphism.

If  $f$  is not one-to-one then  $f^{-1}(0) < f^{-1}(f^{-1}(0)) < f^{-1}(f^{-1}(f^{-1}(0))) < \dots$  is a properly ascending chain of submodules of  $M$ .