Comprehensive Exam Fall 2006

Proposed algebra questions (with solutions)

Matt Baker and Saugata Basu

1. Find all finite simple groups having a subgroup of index 3.

   Solution: Let G be a finite simple group having a subgroup H of index 3. Then G acts on the set S of left cosets of H in G by left-multiplication, and the kernel of this action is the largest normal subgroup of G contained in H. Since G is simple, the kernel must be trivial. Therefore, since $|S| = 3$, this action defines an injective homomorphism $G \to S_3$, i.e., G is a subgroup of the symmetric group on 3 letters. Since G is simple and has a subgroup of index 3, the only choice is $G \cong \mathbf{Z}/3\mathbf{Z}$.

2. Let p be a prime number, let k be a positive integer, and suppose that G is a group of order p^k acting on a finite set S. Show that the number of elements of S fixed by every $g \in G$ is congruent to $|S|$ (the cardinality of S) modulo p.

   Solution: If O is any orbit consisting of more than one element, then since $|O|$ divides $|G|$, it must be a multiple of p. The N elements of S fixed by G are precisely the orbits of size one. Partitioning S into the orbits of G and counting, we see that $|S| \equiv N \pmod{p}$ as desired.

3. If p and q are primes, prove that a group of order p^2q cannot be simple.

   Solution: Let G be a group with $|G| = p^2q$. If $|G| = p^3$, then by the structure theory for p-groups, G has a normal subgroup of index p. So we may assume that $p \neq q$.

   Assume that G is simple. Then the number of p-Sylow subgroups must be q, and hence $q \equiv 1 \pmod{p}$. In particular, $q > p$.

   The number of q-Sylow subgroups is either p or p^2. It cannot be p, because this would imply that $p \equiv 1 \pmod{q}$ and thus $p > q$, a contradiction.

   Hence, the number of q-Sylow subgroups must be p^2. Any two such subgroups can have only the identity as a common element. Hence, the total number of non-identity elements in the q-Sylow subgroups is $p^2(q-1)$.

On the other hand the intersection of any two distinct p-Sylow subgroups can have size at most p (the intersection has to be a subgroup of each). Thus, since $q \geq 2$, the number of elements in the p-Sylow subgroups is at least $2p^2 - p$. But then $p^2(q-1) + 2p^2 - p = p^2q + p(p-1) > |G| = p^2q$, which is a contradiction.

4. Give examples (with proof) of commutative ring R with identity such that:

   (i) R has exactly 10 ideals.

   (ii) R has exactly 10 maximal ideals.

   Solution: For (i), we may take $R = \mathbf{Z}/p^9\mathbf{Z}$ for any prime number p. Ideals of R correspond bijectively to ideals (a) of $\mathbf{Z}$ with $a \mid p^9$, and by unique factorization in $\mathbf{Z}$, there are exactly 10 such ideals: $(1), (p), (p^2), \ldots, (p^9)$. For (ii), we can use a direct product construction and take $R = (\mathbf{Z}/p\mathbf{Z})^{10}$. Ideals of a direct product are direct products of ideals in each factor, so a maximal ideal in $(\mathbf{Z}/p\mathbf{Z})^{10}$ must be (1) on all but one factor. Since each individual factor $\mathbf{Z}/p\mathbf{Z}$ is a field, and thus has only (0) and (1) as ideals, the maximal ideals of R are precisely the ideals

   $$(1) \times (1) \times \cdots (0) \cdots \times (1) \times (1) \ .$$

   There are clearly 10 such ideals.

5. Suppose R is a ring with identity having p^2 elements for some prime number p. Prove that R is commutative.

   Solution: By the structure theorem for finite abelian groups, the additive group $(R, +)$ of R is isomorphic to either $\mathbf{Z}/p^2\mathbf{Z}$ or $(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/p\mathbf{Z})$. In the first case, there is an element $x \in R$ which generates $(R, +)$, so that every element of R is of the form nx for some $n \in \mathbf{Z}$. Elements of this form clearly commute, so R is commutative in this case. In the second case, we can view $(R, +)$ as a 2-dimensional vector space over the field $\mathbf{F}_p$. If $1, x$ is a basis for $R/\mathbf{F}_p$, then $R = \{a + bx \ : \ a, b \in \mathbf{F}_p\}$. Since elements of the form $a+bx$ commute with one another, R is commutative in this case as well.

6. Let K be a field, and let $f, g \in K[x]$ be polynomials with f irreducible over K. If h is any irreducible polynomial dividing $f \circ g = f(g(x))$, prove that $\deg(f) \mid \deg(h)$.

Solution: Let α be a root of h in some splitting field, and let $\beta = g(\alpha)$. Then $\beta \in K(\alpha)$, so $[K(\beta) : K]$ divides $[K(\alpha) : K]$. Since $h(\alpha) = 0$ and $h \mid f \circ g$, it follows that $f(\beta) = f(g(\alpha)) = 0$. As f and h are irreducible over K, $\deg(h) = [K(\alpha) : K]$ and $\deg(f) = [K(\beta) : K]$, and the result follows.

7. Suppose A, B are commuting $n \times n$ matrices over the field $\mathbf{C}$ of complex numbers. Prove that A, B have a common eigenvector.

   Solution: Let λ be an eigenvalue of A, and let V_λ be the corresponding eigenspace. For any $v \in V_\lambda$, we have

   $$A(Bv) = B(Av) = b(\lambda v) = \lambda \cdot Bv \ ,$$

   so that $Bv \in V_\lambda$. Therefore V_λ is invariant under B. Let w be an eigenvector of the restriction of B to V_λ. Then w is a simultaneous eigenvector for both A and B.

8. Let M be a 3×3 matrix with integer entries and $\det(M) = -1$. Assume that every real eigenvalue of M is rational. What are the possibilities for the minimal polynomial of M ?

   Solution: The characteristic polynomial of M is $t^3 + at^2 + bt + 1 \in \mathbb{Z}[t]$, whose only integer roots are ± 1. If all eigenvalues are real, then they are all rational by hypothesis, and hence are all integers since rational roots of monic polynomials are integers (i.e., every rational algebraic integer is an integer). The possible eigenvalues in this case are $-1, 1, 1$ and $-1, -1, -1$, and the possible minimal polynomials for M are

   $$(t+1)(t-1),\ (t+1)(t-1)^2,\ (t+1),\ (t+1)^2,\ (t+1)^3 \ .$$

   If λ is a complex eigenvalue, then so is its complex conjugate $\overline{\lambda}$. The third eigenvalue μ is a real number, hence an integer, and is equal to $-1/\lambda\overline{\lambda} = -1/|\lambda|^2$. Since $\lambda\overline{\lambda}$ is both a rational number and an algebraic integer, it follows that both $|\lambda|^2$ and $-1/|\lambda|^2$ are integers, and therefore that $|\lambda|^2 = 1$ and $\mu = -1$. Therefore we have three distinct eigenvalues $-1, \lambda, \overline{\lambda}$. The minimal polynomial is then $(t+1)(t-\lambda)(t-\overline{\lambda})$ where λ is a complex number with $|\lambda| = 1$.