Spring 2012 Algebra Comprehensive Exam
Georgia Tech Mathematics

Problems: Choose 5 out of 7.

1. Recall that two $n \times n$ matrices A and A' are similar if there exists an invertible matrix B such that $A' = BAB^{-1}$. Similarity is an equivalence relation. How many similarity classes of 3×3 complex matrices with characteristic polynomial $(x-1)^3$ are there?

2. Define what it means for a finite group to be solvable, and prove from first principles that the alternating group A_4 is solvable.

3. Suppose that a group G with 125 elements acts on a set X with 7 elements. What are the possibilities for the number of fixed points of the action (i.e., for the set $\{x \in X | gx = x \ \forall g \in G\}$)?

4. Let R be a commutative ring with identity and let $R^\times$ be the group of invertible elements of R. Prove that $R \setminus R^\times$ is an ideal if and only if R has a unique maximal ideal.

5. Prove from first principles that the polynomial $2x^3 + x + 2$ is irreducible over $\mathbb{Q}[x]$.

6. Let L/K be a finite extension of fields and suppose $a, b \in L$ are elements such that $[K(a) : K] = 3$ and $[K(b) : K] = 2$. What are the possibilities for $[K(a+b) : K]$? Prove that your answer is correct.

7. What is the cardinality of the splitting field of $x^3 - 1$ over $\mathbf{F}_{11}$ (the field of 11 elements)? Same question over $\mathbf{F}_{49}$.

Solution

1. Recall that two $n \times n$ matrices A and A' are similar if there exists an invertible matrix B such that $A' = BAB^{-1}$. Similarity is an equivalence relation. How many similarity classes of 3×3 complex matrices with characteristic polynomial $(x-1)^3$ are there?

   Two matrices are similar if and only if they have the same Jordan canonical form. For 3×3 matrices with characteristic polynomial $(x-1)^3$, the Jordan form must have 1's on the diagonal. The following are the possibilities:

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

2. Define what it means for a finite group to be solvable, and prove from first principles that the alternating group A_4 is solvable.

   A finite group G is *solvable* if there is a chain of subgroups $G = N_0 \supset N_1 \supset \cdots \supset N_n = \{1\}$ such that for each $i = 1, 2, \ldots, n$, N_i is normal in N_{i-1} and N_{i-1}/N_i is abelian.

   Let A_4 be the group of even permutations of the 4-element set $\{1, 2, 3, 4\}$. Then A_4 consists of the identity id, eight 3-cycles, and three permutations that are products of two disjoint transpositions. Let $N_1 = \{id, (12)(34), (13)(24), (14)(23)\}$, which can be checked explicitly to be an abelian subgroup of A_4. It is normal because conjugation preserves cycle types of permutations. The quotient A_4/N_1 has order 3, and hence abelian.

3. Suppose that a group G with 125 elements acts on a set X with 7 elements. What are the possibilities for the number of fixed points of the action (i.e., for the set $\{x \in X | gx = x \ \forall g \in G\}$)?

   For any element $x \in X$, the product of the size of the orbit of x and the order of the stabilizer subgroup of x is equal to the order of the group G, which is 125. In particular, the size of the orbit divides 125, so each orbit contains either 1 or 5 elements. Then only possibilities for the number of fixed points are 2 and 7.

4. Let R be a commutative ring with identity and let $R^\times$ be the group of invertible elements of R. Prove that $R \setminus R^\times$ is an ideal if and only if R has a unique maximal ideal.

   Let $I = R\setminus R^\times$. If I is an ideal in R, then it is the unique maximal ideal because any proper ideal U of R must be contained in I. Otherwise U would contain an invertible element and be equal to R.

   For the converse, let J be the unique maximal ideal of R, and let $a \in R\setminus J$. If a were not a unit, then there is a maximal ideal contianing a, which is not J, so we get a contradiction. Therefore $R \setminus J = R^\times$, and we conclude that $R \setminus R^\times = J$ is an ideal.

5. Prove from first principles that the polynomial $2x^3+x+2$ is irreducible over $\mathbb{Q}[x]$.

   Let $f = 2x^3 + x + 2$. Suppose f is not irreducible, then it has a root in $\mathbb{Q}$ because one of the factors must have degree 1. Let $\frac{a}{b}$ be a root of f, where a and b are relatively prime integers and $b \neq 0$. Then we have $2a^3 = b^2(-a - 2b)$. If b is divisible by an prime p, then $p^2|2a^3$, so $p|a$, contradicting the assumption that a and b are relatively prime. Thus b must be ± 1, and f has an integer root a. However, a must divide 2 because $a(-2a^2 - 1) = 2$, and we see that f has no such root.

6. Let L/K be a finite extension of fields and suppose $a, b \in L$ are elements such that $[K(a) : K] = 3$ and $[K(b) : K] = 2$. What are the possibilities for $[K(a + b) : K]$? Prove that your answer is correct.

   Since $[K(a, b) : K]$ is equal to $[K(a, b) : K(a)][K(a) : K]$ and $[K(a, b) : K(b)][K(b) : K]$, we have that $[K(a, b) : K]$ is divisible by both 3 and 2. Combining with $[K(a, b) : K(a)] \leq [K(b) : K]$, we get $[K(a, b) : K] = 6$. From $[K(a, b) : K] = [K(a, b) : K(a + b)][K(a + b) : K]$, it follows that $[K(a + b) : K]$ divides 6, so the possibilities are 1, 2, 3, and 6.

   If $[K(a + b) : K]$ is equal to 1 (resp. 2) then $K(a, b) = (K(a + b))(b)$ would have degree at most 2 (resp. 4) over K, so this is not possible.

   As a vector space over K, $K(a, b)$ has a basis $\{1, a, a^2, b, ab, a^2b\}$. Suppose there are elements $c_0, c_1, c_2, c_3 \in K$ such that $c_3(a + b)^3 + c_2(a + b)^2 + c_2(a + b) + c_0 = 0$. Expending the expression in the basis above, we see that c_3 is the coefficient of a^2b and must be 0. Hence $a + b$ is a root of a degree 2 polynomial over K, which is impossible as seen above.

Therefore the only possibility for $[K(a+b):K]$ is 6.

7. What is the cardinality of the splitting field of x^3-1 over $\mathbf{F}_{11}$ (the field of 11 elements)? Same question over $\mathbf{F}_{49}$.

   Since 3 does not divide the order of the multiplicative group $\mathbf{F}_{11}^{\times}$, which is $11-1$, no element of $\mathbf{F}_{11}$ other than 1 is root of x^3-1. Thus x^3-1 factors as $(x-1)(x^2+x+1)$, and x^2+x+1 is irreducible. The splitting field is $\mathbb{F}[x]/(x^2+x+1)$, which has cardinality 11^2.

   Since 3 divides $49-1$, there are two distinct elements in $\mathbf{F}_{49}$ other than 1 that satisfy $x^3=1$. Or, direct computation shows that we have $x^3-1=(x-1)(x-2)(x-4)$, so the splitting field is $\mathbf{F}_{49}$ itself, which has cardinality 49.