Ph.D. Qualifying Exam and M.S. Comprehensive Exam in Algebra

Wednesday, August 16, 2006
Professors Frauke Bleher and Fred Goodman

Instructions: Do exactly two problems from each section for a total of eight problems. Be sure to justify your answers. Good luck.

1. Groups:

We denote $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}_n$.

(1) Let G be a group acting on a set S, let $s \in S$. Define the orbit $G.s$ of s under G, define the stabilizer G_s of s in G. Prove that G_s is a subgroup of G and that $|G.s| = (G : G_s)$.

(2) Let G be a finite group of order pq where p, q are primes with $p < q$. Suppose that $q \not\equiv 1 \mod p$. Prove that G is cyclic.

(3) Show that two elements of the symmetric group S_n are conjugate if, and only if, they have the same cycle structure. Determine the number of conjugates in S_7 of the permutation

$$(1, 2, 3)(4, 5, 6)(7).$$

The following exercise may be counted either as a ring theory exercise or a group theory exercise. If you want it to count for ring theory, then you must say so, and you must do two other group theory exercises.

(4) Let $\mathbb{F}_p$ denote the field with p elements, where p is a prime, $p \geq 3$. Consider the ring $R = \mathbb{F}_p[x]/(x^3)$. This problem concerns the abelian group G of units in R. Let $\bar{x}$ denote the image of x in R.

(a) Show that R has p^3 elements.

(b) Show that the ideal generated by $\bar{x}$ is a proper ideal with p^2 elements. Conclude that the group G of invertible elements has at most $p^3 - p^2 = p^2(p-1)$ elements.

(c) Show that elements of the form $\alpha + \beta\bar{x} + \gamma\bar{x}^2$ with $\alpha \neq 0$ are invertible. Conclude that G has precisely $p^2(p-1)$ elements. *Hint:* Compute the p-th power of an element $\alpha + \beta\bar{x} + \gamma\bar{x}^2$.

(d) Referring to an appropriate general theorem, show that $G \cong A \times B$, where A has order p^2 and B has order $p-1$, and that A must be either cyclic, or isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

(e) By appropriate choices of α, β, and γ, exhibit $p^2 - 1$ elements of order p and at least one element of order $p-1$. Conclude that $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p-1}$.

2. Rings:

All rings are assumed to have a multiplicative identity 1.

(1) (a) Let K be an infinite field, and let $f(t), g(t) \in K[t]$. Prove that if $f(c) = g(c)$ for all $c \in K$, then $f(t) = g(t)$ in $K[t]$.
    (b) Is part (a) still true if we assume K is a finite field? If so, prove this; otherwise give a counter-example.

(2) Prove that every principal ideal domain is a unique factorization domain.

(3) (a) Show that every maximal ideal in a commutative ring is prime.
    (b) Give an example of a ring R and a prime ideal in R that is not maximal.
    (c) Show that a non-zero ideal in $\mathbb{Z}$ is maximal if, and only if, it is prime.

(4) A commutative ring is said to be Noetherian if every ideal is finitely generated.
    (a) Show that a commutative ring is Noetherian if, and only if, it satisfies the ascending chain condition for ideals.
    (b) Show that every non–zero non–unit element in a Noetherian integral domain has at least one factorization into irreducibles.

3. Fields:

(1) Let E/F be a finite field extension, and let F' be any extension of F. Suppose that E and F' are contained in a common field, and let EF' be the composite. Prove that $[EF' : F'] \leq [E : F]$. Give an example of E, F, F' so that you have a strict equality.

(2) Let $f(t)$ be an irreducible polynomial of degree p over the rationals, where p is an odd prime. Suppose that f has $p - 2$ real roots and two complex roots which are not real. Prove that the Galois group of $f(t)$ over $\mathbb{Q}$ is isomorphic to the symmetric group S_p.

(3) Let $f(x)$ be a separable polynomial with coefficients in a field K and let L denote the splitting field of $f(x)$. Show that the fixed field of $\mathrm{Aut}_K(L)$ in L is equal to K.

(4) Let $f(x)$ be a polynomial with coefficients in a field K and let L denote the splitting field of $f(x)$. Let A be the set of roots of $f(x)$ in L. Show that for every $\sigma \in \mathrm{Aut}_K(L)$, $\sigma(A) = A$. Show, moreover, that $\mathrm{Aut}_K(L)$ acts faithfully on A, and that the action is transitive if $f(x)$ is irreducible.

4. Linear algebra and modules:

We will let I denote the identity transformation of a vector space or the identity matrix of any size.

(1) Let R be a ring with 1, let E be a left R-module and let L be a left ideal of R. Define LE to be

$$LE = \{x_1 v_1 + \cdots + x_n v_n \mid n \in \mathbb{Z}^+,\, x_i \in L,\, v_i \in E\}\,.$$

(a) Prove that LE is an R-submodule of E.
(b) Assuming that E is simple, prove that $LE = E$ or $LE = \{0\}$.
(c) Assume that L and E are simple and that $LE = E$. Prove that L is isomorphic to E as R-modules.

(2) Let K be an algebraically closed field, let V be a nonzero finite dimensional vector space over K, and let $A \in \mathrm{End}_K(V)$. Let V_A be the corresponding $K[t]$-module. Assume that V_A is a cyclic $K[t]$-module which is generated by $v \in V$, and suppose the annihilator of V_A in $K[t]$ is generated by $(t-\alpha)^r$, where $\alpha \in K$ and $r \in \mathbb{Z}^+$. Prove that
$$\{(A-\alpha I)^{r-1}v, \ldots, (A-\alpha I)v, v\}$$
is a basis of V over K, and determine the matrix of A with respect to this basis. Please be sure to explain all your steps.

(3) Let $p(x), m(x)$ be polynomials with complex coefficients. Let n denote the degree of $p(x)$. State and prove necessary and sufficient conditions on the pair of polynomials so that there exists an n–by–n complex matrix whose characteristic polynomial is $p(x)$ and whose minimal polynomial is $m(x)$.

(4) Let F be an algebraically closed field of characteristic $\neq 2$. The purpose of this exercise is to show that every invertible n–by–n matrix A with entries in F has a square root B; that is, there is a matrix B such that $B^2 = A$.
(a) Show that for an n–by–n matrix T whose only eigenvalue is λ, the number of Jordan blocks of T is equal to $n - r$, where r is the rank of $T - \lambda I$. In particular, T has a single Jordan block if, and only if, the rank of $T - \lambda I$ is $n - 1$.
(b) To prove that A has a square root, show that you can reduce to the case that A is in Jordan form and has a single Jordan block with eigenvalue 1. *Hint:* Reduce successively to the case that A is in Jordan form and has a single (non-zero) eigenvalue, then to the case that A is in Jordan form and the only eigenvalue of A is 1, and finally to the case that A is in Jordan form and has a single Jordan block with eigenvalue 1.
(c) Suppose that A is in Jordan form and has a single Jordan block with eigenvalue 1. Show that the Jordan form of A^2 also has a single Jordan block with eigenvalue 1. Conclude that A is similar to A^2. Since A is similar to a matrix with square root, A itself has a square root.
(d) In case the characteristic of F is 2, give an example of an invertible square matrix A which does not have a square root. *Hint:* Look at 2–by–2 matrices.