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

Professors Frauke Bleher and Miodrag Iovanov

August 17, 2018, 9:00 a.m. - 12:00 p.m. in 105 MLH

Instructions:

- Do EXACTLY TWO problems from EACH of the four sections.
- Please start a new page for every new problem and put your name on each sheet.
- Justify your answers and show your work.
- Please write legibly.
- In answering any part of a question, you may assume the results in previous parts of the SAME question, even if you have not solved them.
- Please turn in the exam questions with your solutions.

Notations:

We adopt standard notations. Namely:

- We write $\mathbb{C}, \mathbb{R}$ and $\mathbb{Q}$ to denote the field of complex numbers, real numbers and rational numbers, respectively. We write $\mathbb{Z}$ to denote the ring of rational integers. If p is a prime number then $\mathbb{F}_p$ denotes the finite field with p elements.
- Throughout this exam, R denotes a ring with identity $1 \neq 0$; R is called an integral domain if it is commutative with no zero divisors.
- All R-modules are assumed to be unital left R-modules.

1 Groups

1. Let G be a finite group, let p be a prime number, and let P be a Sylow p-subgroup of G. Suppose N is a normal subgroup of G.
   (a) Prove: $P \cap N$ is a Sylow p-subgroup of N, and PN/N is a Sylow p-subgroup of G/N.
   (b) Prove that the number of distinct Sylow p-subgroups of G/N is less than or equal to the number of distinct Sylow p-subgroups of G.
2. Show that any group with 255 elements is cyclic.
3. Let G be a group, N a normal subgroup of G, and let $\mathrm{Aut}(N)$ be the set of group automorphisms of N. Show that if $|G|$ and $|\mathrm{Aut}(N)|$ are two relatively prime numbers, then N is contained in the center of G.

2 Rings

1. Let R be a ring (recall that we assume that R has a multiplicative identity $1 \neq 0$). Show that if the polynomial ring $R[X]$ is a PID, then R is a field.
2. Let P be a prime ideal of the polynomial ring $\mathbb{Z}[X]$, which is not a maximal ideal.
   (a) Show that $P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, and that, in fact, $P \cap \mathbb{Z} = 0$. (Here, 0 represents the ideal consisting only of the polynomial $0 \in \mathbb{Z}[X]$.)
   (b) Show that the ideal $I = P\,\mathbb{Q}[X]$ (i.e., the ideal generated by the elements of P inside $\mathbb{Q}[X]$) is equal to the set $\{h(X)/a \mid h(X) \in P, a \in \mathbb{Q} \setminus \{0\}\}$.
   (c) Show that I is a prime ideal of $\mathbb{Q}[X]$ which can be generated by an element $f(X) \in P$, such that the content of f is 1, and possibly using this, prove that P is a principal ideal of $\mathbb{Z}[X]$.
3. Prove that there is an isomorphism of rings

$$\frac{\mathbb{Z}[X]}{\langle X^3 - 1, X^3 + 1\rangle} \cong \mathbb{Z}/2\mathbb{Z} \times \frac{\mathbb{Z}[X]}{\langle 2, x^2 - x - 1\rangle}.$$

3 Linear Algebra and Module Theory

1. Let M be a left R-module (recall that we assume R has a multiplicative identity $1 \neq 0$ and that R-modules are unital). We say M is a *simple* R-module if $M \neq \{0\}$ and the only submodules of M are $\{0\}$ and M.

   (a) Prove: M is simple if and only if $M \neq 0$ and $M = Rm$ for all $m \in M - \{0\}$.

   (b) Prove: If M is simple, then $\mathrm{End}_R(M)$ is a division ring (i.e., a skew field).

2. Let V be a complex vector space of dimension 7 with basis $v_1, \ldots, v_7$. Let $H : V \to V$ be the linear map defined as $H(v_k) = v_{k+1}$ for $k = 1, \ldots, 6$ and $H(v_7) = 0$. Find the Jordan canonical form of the map $T = I + H^2 + H^4$, where $I : V \to V$ is the identity map.

3. Suppose $A \in M_5(\mathbb{Q})$ is such that $A^9 = I$, where I is the identity matrix. Show that $A^3 = I$.

4 Field Theory

1. Let $K = \mathbb{Q}(\sqrt[8]{7}, i)$, let $F_1 = \mathbb{Q}(\sqrt{7})$ and let $F_2 = \mathbb{Q}(\sqrt{-7})$.

   (a) Prove that K is Galois over F_1 and over F_2, and determine $[K : F_1]$ and $[K : F_2]$.

   (b) Determine $\mathrm{Gal}(K/F_1)$ and $\mathrm{Gal}(K/F_2)$.

2. Let K be the splitting field of the polynomial $f(x) = x^4 - x^2 - 1$ over $\mathbb{Q}$.

   (a) Determine $[K : \mathbb{Q}]$, compute the Galois group of f over $\mathbb{Q}$ and identify it up to isomorphism among known groups with a small number of elements.

   (b) Determine, if any, all the intermediate extensions $\mathbb{Q} \subseteq L \subseteq K$ such that $\mathbb{Q} \subset L$ is *not* normal.

3. Let F be a finite field, and $F \subseteq L$ an extension of degree n.

   (a) Show that any irreducible polynomial in $F[X]$ of degree n is the minimal polynomial of exactly n elements of L.

   (b) If $|F| = q$, determine, in terms of q, the number of irreducible polynomials in $F[X]$ of degree 3, and the number of irreducible polynomials in $F[X]$ of degree 9, respectively.