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

Professors Ryan Kinser and Muthu Krishnamurthy

Aug 18, 2020, 1.00 - 4:00 p.m. in S207 PBB

Instructions:

- Do exactly two problems from each of the four sections.
- 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, even if you have not solved them.
- Unless specified otherwise, each problem is worth 15 points with points equidistributed across all parts within a given problem.

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. 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 modules. For any set X, we write $|X|$ to denote its cardinality.

1 Groups

1. Suppose G is a group such that $|G| = 2k$ with k odd. Prove that G has a subgroup of order k.

2. Let p be a prime number and let $\mathbb{F}_p$ denote the finite field with p elements. Consider the group $G = GL_2(\mathbb{F}_p)$ consisting of all 2×2 invertible matrices with entries in $\mathbb{F}_p$.

   (i) Determine the order of the group G.

   (ii) Exihibit a Sylow p-subgroup of G.

   (iii) Determine the number of Sylow p-subgroups of G.

3. Prove that a finite simple group of even order can be generated by a set of elements of order 2. (A group G is said to be simple if it is non-trivial and has no normal subgroups besides $\{e\}$ and G itself.)

2 Rings

1. Let R be a commutative ring with 1. It is said to be Noetherian if it satisfies the ascending chain condition on ideals:

   (i) If $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_k \subseteq \cdots$ is an ascending chain of ideals in R, then $\mathfrak{a}_k = \mathfrak{a}_{k+1} = \cdots$ for a sufficiently large k.

   Alternately, if the following is satisfied:

   (ii) Every ideal of R is finitely generated.

   Show that (i)$\Longleftrightarrow$ (ii).

2. An *arithmetic function* is a complex valued function on the set of positive integers $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$. Let $\mathcal{A}$ be the set of all arithmetic functions. Define the sum in $\mathcal{A}$ to be the ordinary addition of functions, and define a product $\star$ by the formula

$$f \star g(m) = \sum_{xy=m} f(x)g(y).$$

   (a) (5 points) Show that $\mathcal{A}$ is a commutative ring whose unit element is the function δ such that $\delta(1) = 1$ and $\delta(x) = 0$ if $x \neq 1$.

   (b) (10 points) Show that an element $f \in \mathcal{A}$ is invertible if and only if $f(1) \neq 0$.

3. Consider the Gaussian ring $\mathbb{Z}[i]$ and the natural homomorphism

$$\phi : \mathbb{Z} \to \mathbb{Z}[i]/(6+i)$$

given by $a \mapsto a + (6+i)$.

(a) (7 points) Show that ϕ is surjective.

(b) (8 points) Prove that $\mathbb{Z}[i]/(6+i) \cong \mathbb{Z}_{37}$.

3 Linear Algebra and Module Theory

1. Let F be a field and consider the vector space V given by

$$V = F[x]/(x+1)^2 \oplus F[x]/(x^2-1) \oplus F[x]/(x-1)^2$$

as a direct sum of cyclic $F[x]$-modules.

(a) (8 points) Determine the invariant factors and elementary divisors of V as a $F[x]$-module.

(b) (7 points) Determine the rational canonical form of the linear transformation $T : V \longrightarrow V$ given by multiplication by x.

2. Let V be the vector space over $\mathbb{R}$ of real polynomials whose degree $\leq n$. Let $T : V \longrightarrow V$ be the linear map given by

$$T(p(x)) = p'(x).$$

Determine the Jordan canonical form and the rational canonical form of T.

3. Let R be a commutative ring, let M and N be R-modules, and $\mathrm{Hom}_R(M, N)$ denote the set of R-module homomorphisms $M \to N$.

(a) (5 points) Describe the natural R-module structure on $\mathrm{Hom}_R(M, N)$ with a short justification.

(b) (10 points) Now let $R = \mathbb{Z}$ and $M = \mathbb{Z}/(m)$ and $N = \mathbb{Z}/(n)$, where m, n are positive integers. Describe $\mathrm{Hom}_{\mathbb{Z}}(M, N)$ as a direct sum of cyclic $\mathbb{Z}$-modules, including a complete proof that your description is correct.

4 Field Theory

1. Suppose $f(x) \in \mathbb{Q}[x]$ is a monic polynomial of degree n and $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ are the roots of $f(x)$. Let G be the Galois group of f over $\mathbb{Q}$.

   (a) (9 points) Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if the action of G on $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is transitive.

   (b) (6 points) If $f(x)$ is irreducible in $\mathbb{Q}[x]$, then show that n divides $|G|$.

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

   (a) (9 points) Determine the Galois group of K over $\mathbb{Q}$.

   (b) (6 points) Find all quadratic subfields of K.

3. Let E/F be a finite extension of fields.

   (a) Give a detailed definition for the property that <u>E is Galois over F</u>.
   Note that different textbooks may use different definitions. Any definition which is equivalent to the standard one in Dummit and Foote (in the finite case) is acceptable here, but <u>you must include additional definitions</u> for any terminology from field theory that you use in your definition.

   (b) Let $\alpha = \sqrt[4]{2} \in \mathbb{R}$ be the real fourth root of 2. Using the definition you provided in part (a), demonstrate whether $\mathbb{Q}[\alpha]$ is Galois over $\mathbb{Q}$ or not.

   (c) Let F be a field of characteristic *not* equal to 2, and suppose E/F is degree 2. Use the definition you provided in (a) to prove that E is Galois over F.

   (d) Give an example of a tower of Galois extensions that is not Galois, meaning, a tower of fields $F \subset E \subset K$ so that E is Galois over F, K is Galois over E, but K/F is not Galois.