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

Professors Miodrag C. Iovanov and Ryan Kinser

January 17, 2020

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 and $q = p^k$ $(k \geq 1)$, then $\mathbb{F}_q$ denotes the finite field with q 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 p-group, with $p \geq 2$ a prime number.

   (i) Prove that $Z(G)$ is non-trivial.
   (ii) If $G/Z(G)$ is cyclic, prove that G is abelian.
   (iii) Show that if $|G| = p^2$, then G is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

2. Prove that a finite simple group of even order can be generated by a set of elements of order 2.

3. Let $p < q$ be prime integers.
   (i) Show that if p does not divide $q - 1$, then any group of order pq is cyclic.
   (ii) Give an example of a non-cyclic group of order pq when p does divide $q - 1$.

2 Rings

1. Show that there is an isomorphism of rings

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

2. Let R be a commutative ring with 1. Call ideals I, J *relatively prime* if $I + J = R$. Prove the following two statements independently (i.e., statement (i) is not used to prove statement (ii)).

   (i) Assume I, J are relatively prime and $I \cap J = 0$. Prove that $R \cong R/I \times R/J$.
   (ii) Prove that if I and J are relatively prime, so are I^m and J^n for any positive integers m, n.

3. Let R be a commutative ring with 1 and $a \in R$. Prove the following two statements independently (i.e., statement (i) is not used to prove statement (ii)).

   (i) If $P \subset R$ is a prime ideal such that $P \subsetneq (a)$, prove that $P = aP$.
   (ii) Suppose that (a) is a maximal ideal of R. Prove that there is no ideal I of R satisfying $(a) \supsetneq I \supsetneq (a^2)$.

3 Linear Algebra and Module Theory

1. Let $S, T\colon \mathbb{C}^n \to \mathbb{C}^n$ be linear operators such that $ST = TS$. Prove that S and T have a common eigenvector.

2. Let $d \geq 1$ be an integer and $V \subset \mathbb{C}[x]$ the complex vector space of polynomials of degree $\leq d$. Consider the linear transformation $T\colon V \to V$ sending a polynomial $P(x)$ to $P(x-1)$.

   (i) Find all eigenvectors and eigenvalues of T.
   (ii) Use part (i) to find the Jordan canonical form of T.

3. Let A be a $\mathbb{Z}$-module, n a positive integer, and define

$$A_n = \{a \in A \ \mid \ na = 0\},$$

   which you may assume is a $\mathbb{Z}$-module without proof. Construct (with proof) an isomorphism of $\mathbb{Z}$-modules $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z},\, A) \cong A_n$.

4 Field Theory

1. Let p be a prime integer and α a root of the polynomial $x^3 - p$.

   (i) Find (with justification) the degree of the field extension $\mathbb{Q}(\alpha, i)$ over $\mathbb{Q}$, where $i = \sqrt{-1}$ as usual.
   (ii) Prove that $x^3 - p$ is irreducible in the polynomial ring $\mathbb{Q}(i)[x]$.

2. Determine (with proof) the Galois group G of the splitting field F of the polynomial $x^{20} - 1$ over $\mathbb{Q}$. Use this to describe to describe all intermediate fields between $\mathbb{Q}$ and F, along with their degrees, and which are normal extensions of $\mathbb{Q}$.

3. Give an explicit description of all intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[3]{5}, \zeta)$, where ζ is a primitive 3rd root of 1.