Algebra qualifying exam

University of Hawai‘i at Mānoa

January, 2020

Instructions:

- You have 4 hours to complete this exam.
- There are 6 sections.
- You should answer 12 questions and answer at least one question in each of the 6 sections. If you have time, you may answer more than 12 questions—your entire paper will be read and taken into consideration.
- For every solution, please indicate clearly which problem you are working on. More generally, the more legible your writing is, the better it will be appreciated!

The following notations are used throughout:

- $\mathbb{Z}$ stands for the ring rational integers.
- $\mathbb{Q}$ stands for the field of rational numbers.
- $\mathbb{R}$ stands for the field of real numbers.
- $\mathbb{C}$ stands for the field of complex numbers.
- $\mathbb{F}_{p^n}$ stands for the field which consists of p^n elements, where p is a prime, and $n > 0$ is an integer.

1. Group theory

1. Let G be a group of order $|G| = 121$. Suppose that $G \not\simeq \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$. Assume that G acts on a finite set X which consists of 100 elements. How many elements $g \in G$ which satisfy

$$g \cdot x = x \quad \text{for every } x \in X$$

are there?

List all the possible options. Justify your answer.

2. Prove the following statement or give a counter-example (with a justification).

"Let G be a group, and let N be a normal subgroup of G. Then G must have a subgroup isomorphic to G/N."

3. Let G be a group with a normal subgroup H. Suppose that $G/H \simeq \mathbb{Z}$. Let $n > 1$ be an integer. Does G necessarily have a normal subgroup A_n such that $G/A_n \simeq \mathbb{Z}/n\mathbb{Z}$? Prove it or give a counter-example (with a proof).

4. Assume that, for positive integers n and m, the group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic. Does that imply that $\gcd(m, n) = 1$? Prove it or give a counter-example (with a proof).

2. Fields and Galois theory

1. Let p be a prime, and $n \geq 1$ an integer.

Prove that there are infinitely many irreducible polynomials in $\mathbb{F}_{p^n}[x]$.

2. Recall that a field is called *perfect* if every algebraic extension of F is separable (equivalently, every polynomial $f \in F[x]$ is separable). Also recall that if an irreducible polynomial $f \in F[x]$ is not separable, then its derivative vanishes: $f' = 0$.

Let F be a field, and assume that $\operatorname{char}(F) = p > 0$. Denote by $\varphi : F \to F$ the Frobenius endomorphism defined by

$$\varphi(a) = a^p.$$

Assume that φ is surjective. Prove that F is perfect.

3. Let $[K : \mathbb{Q}] = n > 1$ be a finite extension. It is tempting to think about elements of K as complex numbers. Prove that there are at most n pairwise distinct embeddings (i.e. ways to identify elements of K with complex numbers)

$$\sigma : K \hookrightarrow \mathbb{C}$$

which satisfy $\sigma(q) = q$ for every $q \in \mathbb{Q}$.

4. Is there an element $\alpha \in \mathbb{Q}(\sqrt[3]{2})$ such that $1 + \sqrt[3]{2} = \alpha^2$? Prove your answer.

3. Category theory

1. For a finite-dimensional vector space V over a field k, its dual V^* is defined as the linear space of all linear maps $V \to k$. Clearly (you do not need to prove that) the k-vector spaces V and V^* are always isomorphic (because their dimensions are equal).

(a) In the category of finite-dimensional vector spaces with inner product prove that V is naturally isomorphic to V^*.

(b) In the category of finite-dimensional vector spaces, prove that there is no natural isomorphism between V and V^*.

2. Suppose A is an object of category $\mathcal{C}$. For any object $C \in \mathcal{C}$, we have a set of morphisms $\mathrm{Mor}(C, A)$. If we have a morphism $f : B \to C$, we get a map of sets

$$(*) \quad \mathrm{Mor}(C, A) \to \mathrm{Mor}(B, A)$$

by composition. Suppose you have two objects A and A' in category $\mathcal{C}$, and maps

$$\iota_C : \mathrm{Mor}(C, A) \to \mathrm{Mor}(C, A')$$

for every object $C \in \mathcal{C}$ that commute with the maps $(*)$. Show that there is a unique morphism $g : A \to A'$ such that (as C ranges over the objects of $\mathcal{C}$)

$$\iota_C(u) = g \circ u.$$

4. Ring theory

1. In the ring $\mathbb{Z}[\sqrt{-5}]$, give an example of an element which is irreducible but not prime. Prove your claims about the element.

2. Suppose A is a commutative ring with identity $1_A \in A$. Recall that Jacobson radical $J \subset A$ is defined as the intersection of all maximal ideals in A. Let $a \in A$ be such that

$$a \equiv 1 \pmod{J}.$$

Is a necessarily a unit? Prove your claim.

3. Give an example, with a proof, of a commutative ring A with identity which is not Noetherian.

4. Let K be a field, and let $A \supset K$ be an integral domain which contains K, and is a finite-dimensional vector space over K.

An example of this situation is $K = \mathbb{R}$ and $A = \mathbb{C}$ (as a two-dimensional vector space over $\mathbb{R}$). As a more general example, any finite algebraic extension A of K satisfies these conditions. In all these examples, A is a field by construction.

Prove that A must be a field.

5. Modules and multilinear algebra

1. Consider the $\mathbb{R}$-module $A = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ as a ring with multiplication defined by

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'.$$

(This multiplication is well-defined, you do not need to prove that, and it makes A into an R-algebra; you do not need to prove that.)

Is A an integral domain? Prove your answer.

2. Is $\mathbb{Q}/\mathbb{Z}$ a flat $\mathbb{Z}$-module? Justify your answer.

3. Let R be commutative ring , and let M be a non-zero Noetherian R module. Assume that M is not simple. Does M necessarily have a submodule $N \subsetneq M$ such that the quotient M/N is simple?

4. Recall that an R-module M is called a torsion module if for every $x \in M$ there is a non-zero $r \in R$ such that $rx = 0$.

Let R be an integral domain, and let $I \subset R$ be a non-zero ideal in R. Is it true that $\bigwedge^3 I$ is a torsion R-module?

Justify your answer.

6. Commutative algebra

1. Is any U.F.D.integrally closed? Justify your answer.

2. Let R be a commutative ring with identity $1 \in R$. Suppose that there is a maximal ideal $M \subset R$ such that every element $1 + m$ with $m \in M$ is a unit. Prove that R is a local ring.

3. Let $\varphi : B \to A$ be a homomorphism of commutative rings (both with identities).
Let $I \subset B$ be an ideal.
Define the extension of I to A as the ideal I^e generated by the set $\varphi(I)$:

$$I^e := \langle \varphi(a) \rangle_{a \in A}$$

Prove (or provide a counterexample to) the isomorphism

$$A/I^e \simeq A \otimes_B (B/I).$$

4. Prove that for a prime ideal $\mathfrak{p} \subset R$ in a finite-dimensional domain R, the Krull dimension of $R/\mathfrak{p}$ is smaller than the Krull dimension of R