MATH 427
Midterm exam
due Tuesday, December 14, 11:00am

Instructions: Solve each problem as completely as possible, justifying all your answers. You should not discuss the problems on the exam with anyone else. You can use your textbook, but no other resources (e.g., no other texts, the internet, etc.). You may freely assume any of the results from chapters 1–9, 13, 14, including any homework exercises that were assigned. We are following the honor system—it is up to you to be honest, and also to report any cheating to me.

Good Luck!!

1. Let $p \in \mathbb{Z}_+$ be prime. For all $i, j \in \mathbb{Z}_+$ with $i < j$ let $\phi_{ji} : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ denote the natural quotient ring homomorphisms

$$\phi_{ji}(a \mod p^j) = a \mod p^i.$$ 

Set

$$R = \{(a_1, a_2, a_3, \ldots) \mid a_i \in \mathbb{Z}/p^i\mathbb{Z} \text{ and } \phi_{ji}(a_j) = a_i \text{ for all } i < j\} \subset \prod_{i=1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}.$$ 

(i) From exercise 19, page 231 (which you may assume) we know that

$$(a_1, a_2, \ldots) + (b_1, b_2, \ldots) = (a_1 + b_1, a_2 + b_2, \ldots)$$

and

$$(a_1, a_2, \ldots) \cdot (b_1, b_2, \ldots) = (a_1b_2, a_2b_2, \ldots)$$

defines a commutative ring structure on $\prod_{i=1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$. Prove that $R$ is a subring with 1.

(ii) Consider the set of infinite series

$$S = \left\{ \sum_{k=0}^{\infty} c_k p^k \mid c_k \in \{0, \ldots, p-1\} \right\}$$

Given $c = \sum_{k=0}^{\infty} c_k p^k \in S$, we note that although this series may not converge, for all $i \in \mathbb{Z}_+$, we can formally make sense of the reduction $\mod p^i$, written $\psi_i : S \to \mathbb{Z}/p^i\mathbb{Z}$, by declaring

$$\psi_i(c) = \left( \sum_{k=0}^{\infty} c_k p^k \right) \mod p^i.$$ 

Now set

$$\psi(c) = (\psi_1(c), \psi_2(c), \ldots)$$

and prove that this defines a bijection from $S$ to $R$.

Hint: observe that any $x \in \{0, 1, \ldots, p^i - 1\}$ can be uniquely written in the form $x = \sum_{k=0}^{j-1} c_k p^k$. 

1
(iii) (nothing to prove here) Using the bijection \( \psi \), we may identify the two sets \( S \) and \( R \), and so freely refer to \( c = \sum_{k=0}^{\infty} c_k p^k \) as an element of \( R \). Note that ring operations take on a particularly natural form in this way. That is, the sum and products of elements

\[
c = \sum_{k=0}^{\infty} c_k p^k \quad \text{and} \quad d = \sum_{k=0}^{\infty} d_k p^k.
\]

are computed by simply adding and multiplying formally, then appropriately rewriting the series to have all coefficients in \( \{0, \ldots, p-1\} \).

(iv) Prove that \( R \) is an integral domain and that it contains an isomorphic copy of \( \mathbb{Z} \) (in particular, observe that the field of fractions of \( R \) has characteristic zero!).

(v) Prove that \( c = \sum_{k=0}^{\infty} c_k p^k \in R \) is a unit if and only if \( c_0 \neq 0 \).

2. Suppose \( f(x) \in \mathbb{Q}[x] \) is an irreducible polynomial of prime degree \( p \), and let \( K \subset \mathbb{C} \) denote a splitting field.

(i) Prove that if \( f(x) \) has exactly \( p - 2 \) roots in \( \mathbb{R} \), then \( [K : \mathbb{Q}] = p! \) and \( \text{Aut}(K/\mathbb{Q}) \cong S_p \).

Hint: Prove that \( \text{Aut}(K/\mathbb{Q}) \) contains a \( p \)-cycle and a transposition.

(ii) Construct a degree \( 4 \) polynomial \( f(x) \in \mathbb{Q}[x] \) with exactly \( 2 \) real roots in the splitting field \( K \subset \mathbb{C} \) (so the assumption that \( p \) is prime should be used in your proof).

3. Let \( ch(F) = p < \infty \), \( a \in F \) and consider the polynomial \( f(x) = x^p - x + a \in F[x] \). Let \( K/F \) be the splitting field of \( f \).

(i) Show that \( K/F \) is Galois.

(ii) Show that if \( \alpha \in K \) is a root of \( f \), so is \( \alpha + c \) for \( c \in F_p \), and that this gives all the roots of \( f \).

(iii) Let \( G = \text{Aut}(K/F) \). Fix a root \( \alpha \in K \) of \( f \), and show that the function \( \phi: G \to K \) defined by \( \phi(\sigma) = \sigma(\alpha) - \alpha \) has image in \( F_p \), and is an injective homomorphism of groups (where \( F_p \) is viewed as the additive group \( \mathbb{Z}/p\mathbb{Z} \)).

(iv) Use (iii) to describe the group \( G \) up to isomorphism. (There is more than one possibility depending on \( [K : F] \).) Use this to prove that \( f \) is either irreducible over \( F \), or splits completely over \( F \).

Note: Since \( ch(F) = p \), we have \( F_p \subseteq F \), but we are not assuming they are equal.

4. Let \( p_1, p_2, \ldots, p_n \) be distinct primes in \( \mathbb{Z}_+ \). For concreteness, let \( \sqrt{p_i} \in \mathbb{R}_+ \) be the positive square root. In this problem you will analyze the extension \( \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q} \), which is the splitting field of the polynomial

\[
f(x) = (x^2 - p_1)(x^2 - p_2) \cdots (x^2 - p_n).
\]
(i) Prove that $[Q(\sqrt{p_1}, \ldots, \sqrt{p_k}) : Q] \leq 2^k$ for any $1 \leq k \leq n$.

(ii) Assuming $[Q(\sqrt{p_1}, \ldots, \sqrt{p_k}) : Q] = 2^k$ for some $1 \leq k \leq n$, prove that the following is a basis for $Q(\sqrt{p_1}, \ldots, \sqrt{p_k})/Q$

$$\{1\} \cup \bigcup_{r=1}^{k} \{\sqrt{p_{i_1} \cdots p_{i_r}}\}_{i_1 < i_2 < \ldots < i_r}.$$

Hint: write the extension as an iterated extension

$$Q \subseteq Q(\sqrt{p_1}) \subseteq Q(\sqrt{p_1}, \sqrt{p_2}) \subseteq \cdots \subseteq Q(\sqrt{p_1}, \ldots, \sqrt{p_k}).$$

(iii) Continuing to assume $[Q(\sqrt{p_1}, \ldots, \sqrt{p_k}) : Q] = 2^k$, prove

$$\text{Aut}(Q(\sqrt{p_1}, \ldots, \sqrt{p_k})/Q) \cong (\mathbb{Z}/2\mathbb{Z})^k.$$ 

Further, if $\sigma_1, \ldots, \sigma_k \in \text{Aut}(Q(\sqrt{p_1}, \ldots, \sqrt{p_k})/Q)$ are generators corresponding under the isomorphism to generators of the factors $\mathbb{Z}/2\mathbb{Z}$, describe the effect of each $\sigma_i$ on the basis from part (ii).

(iv) Prove that $[Q(\sqrt{p_1}, \ldots, \sqrt{p_k}) : Q] = 2^k$ for all $1 \leq k \leq n$.

Hint: Use induction. If there is $1 \leq k \leq n$ with $\sqrt{p_k} \in Q(\sqrt{p_1}, \ldots, \sqrt{p_{k-1}})$, pick the smallest $j \leq k-1$ so that $\sqrt{p_k} \in Q(\sqrt{p_1}, \ldots, \sqrt{p_j})$. Write $\sqrt{p_k}$ in terms of the basis from part (ii), and consider the product $\sqrt{p_k} \cdot \sigma_j(\sqrt{p_k})$. 

3