Algebra general exam. January 13th 2012, 9am-2pm

Directions.

• Please show all your work and justify any statements that you make.
• State clearly and fully any theorem you use.
• Vague statements and hand-waving arguments will not be appreciated.
• You may assume the statement in an earlier part proven in order to do a later part.

DO EACH PROBLEM ON A SEPARATE SHEET OF PAPER, AND STAPLE THEM TOGETHER IN THE CORRECT ORDER BEFORE TURNING THE EXAM IN.

1. Let $F = \mathbb{F}_q$ be a finite field, where $q = p^r$ is a power of a prime $p$. Let $G = GL_n(F)$ be the group of all $n \times n$ invertible matrices with entries in $F$. Once you pick an ordered basis of $V := F^n$, you may find it useful to identify $G$ with the group of invertible linear operators on $V$.

(a) (6 pts) Calculate the order of $G$. Explain your answer carefully and write it in the simplest form as you can.

(b) (3 pts) Determine the order of a Sylow $p$-subgroup of $G$, and explicitly exhibit a Sylow $p$-subgroup $U$ of $G$.

(c) (2 pts) What is the normalizer in $G$ of the Sylow $p$-subgroup $U$ that you exhibited in (b)? An answer is sufficient.

(d) (3 pts) How many Sylow $p$-subgroups of $G$ are there? Explain how your answer in (d) is consistent with Sylow’s theorem.

2. Let $G$ be a subgroup of the symmetric group $S_n$ for some integer $n > 1$. Assume that $G$ acts transitively on $n := \{1, 2, \cdots, n\}$, that is, for any $i, j \in n$ there exists $g \in G$ s.t. $g(i) = j$.

A partition of $n$ is a decomposition $n = X_1 \cup \cdots \cup X_m$ into a disjoint union of nonempty subsets. There are two trivial partitions: $n = n$ and $n = X_1 \cup \cdots \cup X_m$ (so each $X_i$ has just one element). Otherwise the partition is said to be nontrivial. The group $G$ is called imprimitive if there is a nontrivial partition $n = X_1 \cup \cdots \cup X_m$ such that, for $g \in G$ and $1 \leq i \leq m$, $g(X_i) = X_j$ for some $j$. (That is, $G$ permutes the partition members among themselves.) The set $\{X_i\}$ is called a system of imprimitivity for the action of $G$ on $n$. The group $G$ is called primitive if it is not imprimitive.

(a) (3 pts) Let $n = 6$ and consider the cyclic subgroup $G := \langle 1, 2, 3, 4, 5, 6 \rangle$ of $S_6$. There are two non-trivial systems of imprimitivity for the action of $G$ on $n$. Find them.

(b) (3 pts) Prove that if $X_1 \cup \cdots \cup X_m$ is a system of imprimitivity for the action of $G$ on $n$, then all subsets $X_i$ have the same size $n/m$.

(c) (4 pts) $G$ is said to be doubly transitive if given elements $a, b, c, d \in n$, with $a \neq b$ and $c \neq d$, there exists $g \in G$ such that $g(a) = c$ and $g(b) = d$. Show that a doubly transitive group $G$ is primitive.
2

(d) (4 pts) Show that if \( n \geq 3 \), the alternating subgroup \( G = A_n \) of \( S_n \) is primitive.

3. Let \( R = \mathbb{Z} \sqrt{-2} \).

(a) (7 pts) Prove that \( R \) is a Euclidean domain. **Hint:** Use the square of the usual complex norm.

(b) (8 pts) Write 7 and 11 as products of irreducible elements of \( R \). Justify your answer.

4. Let \( R \) be a ring with 1. The **opposite ring** \( R^{op} \) is defined as follows: as a set \( R^{op} = R \), the addition on \( R^{op} \) coincides with the addition on \( R \) and the multiplication \( * \) on \( R^{op} \) is the multiplication on \( R \) in reverse order, that is, \( a * b = ba \) (where \( ba \) is the product in \( R \)). Let \( e \in R \) be an idempotent element, that is, \( e^2 = e \).

(a) (2 pts) Prove that \( eRe = \{ ere : r \in R \} \) is a subring of \( R \).

(b) (6 pts) Consider the left \( R \)-module \( M = Re \). Prove that its endomorphism ring \( \text{End}_R(M) = \text{Hom}_R(M, M) \) is isomorphic to \( (eRe)^{op} \), the opposite ring of \( eRe \).

5. (9 pts) Let \( F \) be a field, \( n \) a positive integer and \( M_n(F) \) the set of \( n \times n \) matrices over \( F \). Let \( A \in \text{Mat}_n(F) \) be such that \( A^2 = A \). Prove that \( A \) is diagonalizable and classify all such \( A \) up to similarity. (Recall that \( A, B \in \text{Mat}_n(F) \) are similar if there exists \( C \in \text{GL}_n(F) \) s.t. \( C^{-1}AC = B \).)

6. Let \( R \) be a commutative ring with 1. Recall that a left \( R \)-module \( M \) is called **Noetherian** if it satisfies the ascending chain condition on submodules and **Artinian** if it satisfies the descending chain condition on submodules. Assume that an \( R \)-module \( M \) is both Artinian and Noetherian. (For example, \( R \) might be a field, and \( M \) might be a finite-dimensional vector space over \( R \)). Let \( T : M \to M \) be an \( R \)-module homomorphism.

(a) (3 pts) Prove that there exists \( k \in \mathbb{N} \) s.t. \( \ker(T^k) = \ker(T^{2k}) \) and \( \text{im}(T^k) = \text{im}(T^{2k}) \).

(b) (4 pts) Prove that if \( k \) is as in part (a), then \( M = \ker(T^k) \oplus \text{im}(T^k) \).

(c) (2 pts) Deduce from (a) and (b) that there exist submodules \( M_0 \) and \( M_1 \) of \( M \) s.t. \( M = M_0 \oplus M_1, T|_{M_0} \) is nilpotent and \( T|_{M_1} \) is invertible (as a map from \( M_1 \) to \( M_1 \)).

(d) (5 pts) Now assume that \( R \) is a field of **characteristic zero**, \( M \) is a finite-dimensional vector space over \( R \) and \( \text{tr}(T^n) = 0 \) for every \( n \in \mathbb{Z}_{\geq 0} \). Prove that \( T \) is nilpotent. **Hint:** Apply (c), assume that \( M_1 \neq 0 \) and reach a contradiction by applying the Cayley-Hamilton theorem to \( T|_{M_1} \).

7. If \( q \) is a prime power, denote by \( \mathbb{F}_q \) a finite field of order \( q \).

(a) (6 pts) Find a monic irreducible polynomial of degree 3 over \( \mathbb{F}_5 \) and use it to construct a field of order 125. Justify your answer.

(b) (6 pts) Find all \( q \) for which the polynomial \( p(x) = x^2 + x + 1 \) is irreducible in \( \mathbb{F}_q[x] \). **Hint:** What can you say about roots of \( p(x) \) and what do you know about the multiplicative group \( \mathbb{F}_q^\times \)?
8. Let $F$ be a field of characteristic zero, let $K$ and $L$ be finite extensions of $F$ and $KL$ the compositum of $K$ and $L$.


(c) (4 pts) Give an example where $K \cap L = F$ but $[KL : F] \neq [K : F][L : F]$.

(d) (4 pts) Assume that $K/F$ and $L/F$ are both Galois. Prove that $Gal(KL/F)$ is isomorphic to a subgroup of $Gal(K/F) \times Gal(L/F)$.

(You need not prove that $KL/F$ is Galois).

Note: The assertions of (a),(b) and (d) remain valid for $F$ of positive characteristic, but part (a) has shorter proof in the case of characteristic zero.