QUALIFYING EXAMINATION
JANUARY, 1999
MATH 553 - PROFS. AVRAMOV/LIPMAN

When answering any part of a problem you may assume the answers to the preceding parts.
The number of points carried by a correct answer is indicated after each question.

NOTATION: The symbols \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C} \) stand for, respectively, the ring of integers and the fields of rational, real, and complex numbers.

1. Let \( G \) be a finite group, \( p > 0 \) a prime number, and \( H \) a normal \( p \)-subgroup of \( G \).
Prove the following assertions.

(1) \( H \) is contained in each Sylow \( p \)-subgroup of \( G \). [5]
(2) If \( K \) is any normal \( p \)-subgroup of \( G \), then \( HK \) is a normal \( p \)-subgroup of \( G \). [5]
(3) The subgroup \( O_p(G) \) generated by all normal \( p \)-subgroups of \( G \) is equal to the intersection of all the Sylow \( p \)-subgroups of \( G \). [5]
(4) \( O_p(G) \) is the unique largest normal \( p \)-subgroup of \( G \). [5]
(5) \( O_p(G) = \{1\} \) where \( \overline{G} = G/O_p(G) \). [5]

2. Let \( K \) be a field and let \( p > 0 \) be a prime number. Prove the following assertions.

(1) If \( a, b \in K \) satisfy \( a^n = b^p \) for some \( 0 < n < p \), then \( a = c^p \) for some \( c \in K \). [5]
(2) The polynomial \( x^p - a \) is reducible in \( K[x] \) if and only if \( a = c^p \) for some \( c \in K \). [5]
(3) If \( K \subseteq \mathbb{R} \) and \( \xi \in \mathbb{R} \) is such that \( \xi^p \in K \), then an irreducible polynomial \( f(x) \) of degree 3 in \( K[x] \) is also irreducible in \( K(\xi)[x] \). [10]

[Hint: After replacing \( K \) by \( K(\sqrt{\Delta}) \), where \( \Delta \) is the discriminant of \( f(x) \), one may assume that \( \sqrt{\Delta} \in K \), and that the splitting field of \( K \) over \( F \) has degree 3.]

3. For a fixed negative integer \( m \equiv 1 \mod (4) \) set \( \mu = \frac{1 + \sqrt{m}}{2} \) and \( \overline{\mu} = \frac{1 - \sqrt{m}}{2} \).
Prove the following assertions.

(1) \( \mathbb{Z}[\mu] = \{p + q\mu \in \mathbb{C} \mid p, q \in \mathbb{Z}\} \) is a ring and \( \mathbb{Q}[\sqrt{m}] = \{s + t\sqrt{m} \in \mathbb{C} \mid s, t \in \mathbb{Q}\} \) is its field of fractions. [5]
(2) \( \mathbb{Z}[\mu] \) is euclidean with respect to the norm

\[
N(s + t\mu) = (s + t\mu)(s + t\overline{\mu}) = \left(s + \frac{t}{2}\right)^2 - m \left(\frac{t}{2}\right)^2
\]

if and only if for all \( s, t \in \mathbb{Q} \) there exist \( p, q \in \mathbb{Z} \) with \( N(s + t\mu - p - q\mu) < 1 \). [10]
(3) \( \mathbb{Z}[\mu] \) is euclidean for this norm if and only if \( m = -3, -7, -11 \). [5]
4. Let \( F \) be a finite field with \( q \) elements. Prove the following assertions.

(1) Polynomials \( f(x), g(x) \in F[x] \) have the property that \( \varphi(c) = g(c) \) for all \( c \in F \) if and only if \( g(x) \equiv f(x) \mod (x^q - x) \).

(2) If \( \varphi: F \to F \) is any map of sets, then there is a unique polynomial \( f(x) \in F[x] \) of degree \( \leq q - 1 \) such that \( \varphi(c) = f(c) \) for all \( c \in F \), namely

\[
f(x) = \sum_{c \in F} \varphi(c) \left( 1 - (x - c)^{q-1} \right)
\]

(3) Fix \( a \in F \) and make the convention that \( 0^0 = 1 \). The polynomial of degree \( \leq q - 1 \) corresponding to the map \( \delta_a : F \to F \) given by \( \delta_a(c) = \begin{cases} 1 & \text{if } c = a \\ 0 & \text{if } c \neq a \end{cases} \) is equal to

\[
d_a(x) = 1 - \sum_{j=0}^{q-1} a^{q-1-j} x^j
\]

(4) Elements \( a_0, a_1, \ldots, a_{q-1} \) in \( F \) are pairwise distinct if and only if

\[
\sum_{j=0}^{q-1} a_i^n = \begin{cases} 0 & \text{if } n = 0, 1, \ldots, q - 2 \\ -1 & \text{if } n = q - 1 \end{cases}
\]

[HINT: Consider the map \( \delta = \sum_{j=0}^{q-1} \delta_{a_i} : F \to F \).]