QUALIFYING EXAMINATION

JANUARY 1995

MATH 553

DO ANY FOUR OF THE QUESTIONS (1–5). BEGIN EACH ONE ON A NEW SHEET.

IN ANSWERING ANY PART OF A QUESTION, YOU MAY ASSUME THE PRECEDING PARTS.

1. $\mathbb{Z}$ denotes the ring of integers.

[8] (a) Let m and n be relatively prime positive integers. Show that there is a ring isomorphism

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

[8] (b) Let $\phi(x)$ be the number of positive integers $\leq x$ and relatively prime to x. Prove that if $p_1, p_2, \ldots, p_k$ are distinct positive primes, and $e_1, e_2, \ldots, e_k$ are positive integers ($k > 0$), then

$$\phi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = p_1^{e_1-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1) \cdots p_k^{e_k-1}(p_k - 1).$$

[9] (c) Let m be a positive integer such that every group of order m is cyclic. Prove that m and $\phi(m)$ are relatively prime.

The converse is also true, but don't try to prove that now.

2. Let G be a non-abelian group of order p^3 (p an odd prime), and let C be its center.

[7] (a) Show that G/C is isomorphic to $\mathbf{Z}_p \times \mathbf{Z}_p$, where $\mathbf{Z}_p$ is a group of order p.

[6] (b) Prove that the map $f\colon G \to G$ defined by $f(x) = x^p$ is a group homomorphism.

Hint: By (a), for any x, y in G there is a $z \in C$ such that $yx = xyz$.

[6] (c) Prove that $f(G) \subset C$, and deduce that G has at least $p^2 - 1$ elements of order p.

[6] (d) Prove that G has subgroups H and K of orders p^2 and p respectively, such that $H \cap K = \{e\}$.

3. Let R be a commutative integral domain in which any two non-zero elements x, y have a greatest common divisor (gcd), i.e., an element dividing both x and y, and divisible by any other element which divides both x and y. Abusing notation, we write $d = (x, y)$ for any d which is a greatest common divisor of x and y.

[5] (a) Prove that if $d = (x, y)$, then $e = (x, y)$ if and only if $e = ud$ where u is a unit in R.

[7] (b) Prove that for all nonzero x, y, z in R,

$$(xy, zy) = (x, z)y.$$

[7] (c) Prove that if $(x, z) = (y, z) = 1$ then $(xy, z) = 1$.

[6] (d) Prove that any irreducible element in R is prime (i.e., generates a prime ideal).

Recall that z is irreducible if z is a nonzero nonunit element such that $z = xy$ implies that either x or y is a unit.

4. $\mathbb{F}_n$ denotes the finite field of cardinality n.

[8] (a) Prove that the polynomial $X^5 - X - 1$ has no root in $\mathbb{F}_9$.

[9] (b) Using (a), or otherwise, show that $X^5 - X - 1$ is irreducible over $\mathbb{F}_3$.

[8] (c) For which values of n is $X^5 - X - 1$ reducible over $\mathbb{F}_{3^n}$? Justify your answer.

5. Let $f(X)$ be an irreducible polynomial of degree 5 with coefficents in the field of rational numbers $\mathbb{Q}$. Assume that f has at least one non-real root in the complex field $\mathbb{C}$. Assume further that the discriminant of f is a square in $\mathbb{Q}$.[1]

[8] (a) Prove that the galois group G of f is either the alternating group $\mathbf{A}_5$ or the dihedral group $\mathbf{D}_5$ (of order 10). (You may assume that $\mathbf{A}_5$ is a simple group.)

[8] (b) Let r be a root of f, and let K be the field $\mathbb{Q}[r]$, so that f factors in $K[X]$ as $f = (X - r)g$ with g of degree 4. Prove that f is solvable by radicals if and only if g is reducible in $K[X]$.

[9] (c) Does (a) hold if we drop the assumption about a non-real root?

Hint: Let ζ be a primitive 25-th root of unity, and consider subfields of $\mathbb{Q}[\zeta]$.

---

[1] Let $y_1, \ldots, y_5$ be the roots of f, and set $\delta := \prod_{1 \le i < j \le 5}(y_i - y_j)$. The *discriminant* of f is

$$\delta^2 = \prod_{i \neq j}(y_i - y_j).$$

You may assume that if θ is any automorphism of the splitting field of f then $\theta(\delta) = \epsilon\delta$ where $\epsilon = \pm 1$ is the *sign* of the permutation of the y_i induced by θ (i.e., $\epsilon = 1$ if the permutation is even, and -1 if odd).