QUALIFYING EXAMINATION
Math 553
August 2007 - Profs. Lipman and Ulrich

BEGIN EACH QUESTION (I-IV) ON A NEW SHEET OF PAPER.

IN ANSWERING ANY PART OF A QUESTION, YOU MAY ASSUME THE RESULTS IN PREVIOUS PARTS, EVEN IF YOU HAVEN'T DONE THEM.

[**Bold numbers**] INDICATE POINTS (**60** TOTAL).

I. (a) [**3**] Let a be a positive integer. Prove that in the cyclic group $\mathbb{Z}_n$ of order $n > 0$, the number of elements x satisfying $ax = 0$ is the gcd (a, n).

(b) [**7**] Let G be an abelian group of order n^r, and suppose that for each positive a dividing n, the number of elements $x \in G$ satisfying $ax = 0$ is a^r. Prove that G is isomorphic to $(\mathbb{Z}_n)^r$.

II. [**10**] Let G be a group of order ap^n where p is prime and $(a, p) = (a, p - 1) = 1$. Suppose that some Sylow p-subgoup $P < G$ is cyclic. Prove that P is contained in the center of its normalizer $N(P)$.

Hint. Begin by describing a homomorphism $N(P) \to \mathrm{Aut}(P)$ whose kernel is the centralizer of P.

III. [**15**] Let R be a unique factorization domain, with fraction field F. Let M be a multiplicatively closed subset of R, containing 1 but not 0. Prove that the ring of fractions

$$R_M := \{\, r/m \mid r \in R,\ m \in M \,\} \subset F$$

is also a unique factorization domain, whose prime elements are all the associates in R_M (that is, multiples by units) of prime elements $p \in R$ such that $(pR) \cap M$ is empty.

IV. (a) [**2**] Show that the polynomial $X^4 - 10X^2 + 1$ is irreducible in $\mathbb{Z}[X]$.

(b) [**6**] Determine the splitting field E of $X^4 - 10X^2 + 1$ over the field $\mathbb{Q}$ of rational numbers; and describe *all* the subfields of E. (Justify your answer).

(c) [**2**] Let F be a finite field. Show that at least one of 2, 3 or 6 is a square in F.

(d) [**3**] Show that the polynomial $X^4 - 10X^2 + 1$ is reducible in $(\mathbb{Z}/p\mathbb{Z})[X]$ for all primes p.

(e) [**3**] Let F be a field, and $g \in F[X]$ an irreducible separable polynomial of degree d whose Galois group G is cyclic. Show that, as a group of permutations of the roots of g, G contains a cycle of length d.

(f) [**6**] Let $f \in \mathbb{Z}[X]$ be a monic polynomial with integer coefficients, of even degree > 1. Prove that if the discriminant Δ_f of f is a square in $\mathbb{Z}$ then for every prime $p \in \mathbb{Z}$, the natural image of f in $(\mathbb{Z}/p\mathbb{Z})[X]$ is reducible. Does this condition on Δ_f imply that f itself is reducible? (Justify your answer).

(g) [**3**] Does the preceding assertion hold when f has odd degree? (Justify your answer).

Hint. Compute the discriminant of $X^3 - 3X + 1$.