MATH 553 QUALIFYING EXAMINATION  
January 6, 2012

PLEASE BEGIN YOUR ANSWER TO EACH PROBLEM I—IV ON A NEW SHEET.

WHEN ANSWERING ANY PART OF A PROBLEM, YOU MAY USE PRECEDING PARTS, EVEN IF YOU HAVEN’T SOLVED THEM.

I. [15 points] Let G be a finite group, let p be a prime divisor of the order |G|, and let P be a Sylow p-subgroup of G. Let N(P) be the normalizer of P, and C(P) ⊂ N(P) the centralizer of P (consisting of those elements of G which commute with every element of P).

(a) Show that the index [N(P) : C(P)] is the order of a subgroup of the automorphism group of P.
(b) Show that p divides [N(P) : C(P)] if, and only if, P is nonabelian.
(c) Show that if P is cyclic and the gcd ([G], p − 1) = 1 then C(P) = N(P).

II. [15 points] (a) Let R be an integral domain. Suppose there exists a function ν: (R \ {0}) → N such that (*) : for all b ≠ 0 in R and a ∉ bR, there exist x and y in R such that ax + by ≠ 0 and ν(ax + by) < ν(b).

Prove that R is a principal ideal domain.

(b). Let R be any principal ideal domain. Define ν: (R \ {0}) → N by ν(a) := 0 if a is a unit, and otherwise ν(a) := the total number of factors in any factorization of a into irreducible elements.

(i) Explain why this ν is well-defined.

(ii) Show that ν satisfies the condition (*) in (a).

III. [10 points] Let F be a finite field of odd cardinality q, and let L ⊃ F be an extension such that [L : F] = 2.

(a) Show that the roots in L of X^8 − 1 form a cyclic group G of order 8.

Hint: Consider the order of the multiplicative group L^∗.

(b) Let ζ be a generator of G. Show that (ζ + ζ^−1)^2 = 2.

(c) Show that ζ + ζ^−1 ∈ F ⇐⇒ (ζ + ζ^−1)^q = ζ + ζ^−1 ⇐⇒ q ≡ ±1 (mod 8).

IV. [20 points] (a) Prove: the galois group G of f(X) := (X^3 − 2)(X^3 − 3) ∈ Q[X] is isomorphic to the semi-direct product Z_2 ×_θ (Z_3 × Z_3), where θ takes the generator of Z_2 to the automorphism h → h^−1 of Z_3 × Z_3.

(b) Set ρ := e^{2πi/3}, so that L := Q[ρ, √2, √3] is a splitting field of f(X). (√ means real cube root.) Describe explicitly all the subfields of L that contain ρ. (One such field, for example, is Q[ρ, √12].)

Suggestions (fill in—and justify—the details!):

For (a), let E := Q[ρ] ⊂ Q[ρ, √2] := F. Show that X^3 − 2 is irreducible in E[X]. If X^3 − 3 were reducible in F[X] then for some d ∈ F, say d = a + b√2 + c√3 (a, b, c ∈ E), we’d have d^3 = 3, and so if ψ is the E-automorphism of F such that ψ(√2) = ρ√2 then ψ(d) = ρ^n d for some n = 1 or 2; deduce from this that a and one of b, c vanish, then take the (E/Q)-norm of d^3 to get a contradiction. Conclude that [L : E] = 9, and determine the galois group H of L/E.

Note also that complex conjugation is an automorphism of L, generating an order 2 subgroup G ⊂ G.