QUALIFYING EXAMINATION
AUGUST, 2001
Math 553

When answering any part of a problem you may assume you have done the preceding parts and also the preceding problems.

The number of [points] *carried by a correct answer is indicated after each question. Each of the problems 1–4 has total value 20, while problem 5 has total value 30.*

NOTATION: The symbol $\mathbb{Z}$ (resp. $\mathbb{Q}$) denotes the ring of rational integers (resp. the field of rational numbers).

For a positive integer n, S_n (resp. A_n) is the *symmetric (resp. alternating) group* of permutations of $\{1, 2, \ldots, n\}$.

1. It is known (and you may assume) that up to isomorphism there are three distinct nonabelian groups of order 12—the alternating group A_4, the dihedral group D_{12}, and a group S with generators x, y satisfying $x^4 = y^3 = 1$ and $xyx^{-1} = y^2$.

(a) Calculate the order of each element of S. Deduce that every proper subgroup of S is cyclic, that there are three of order 4, and one each of orders 2, 3, and 6. [7]

(b) Show that D_{12} has a unique abelian subgroup of order 6. How many non-abelian subgroups of order 6 does D_{12} have? [6]

(c) Use the fact that every three-cycle is a square in A_4 to show that A_4 has no subgroup of order 6. [3]

(d) The unit cube has four "long" diagonals of length $\sqrt{3}$; their endpoints fall into four disjoint pairs of vertices. Take for granted that the group of distance-preserving maps of the cube onto itself (isometries) leaving one vertex A fixed has order 6. (It consists of rotations around the long diagonal through A, and reflections in planes joining an edge through A to the opposite edge.) Then the isometries taking one fixed pair of vertices to itself form a nonabelian group of order 12. To which one of A_4, D_{12}, and S is it isomorphic? (Justify your answer!) [4]

2. (a) Let G be a simple group having a subgroup H of index $n > 2$. Prove that G is isomorphic to a subgroup H' of A_n. (You may take for granted that there is a homomorphism $G \to S_n$ corresponding to the left-multiplication action of G on the left cosets of H.) Deduce that if $n \geq 5$ and $H' \neq A_n$ then $[A_n : H'] \geq n$. [5]

(b) Prove that in a simple group of order 180 there must be 144 elements of order 5. [6]

(c) Prove that in a simple group of order 180 there must be 10 subgroups of order 9, some two of which intersect in a subgroup T of order 3. Show further that the normalizer of T has order ≥ 36. [6]

(d) Prove that there is no simple group of order 180. [3]

(OVER)

3. Let R be an integral domain with field of fractions K, and let $x \in R$ be a nonzero prime element (that is, x is a nonunit such that if $x|ab$ then $x|a$ or $x|b$). You may assume the fact that R is a unique factorization domain (UFD) if and only if every nonunit in R is a product of (one or more) primes. Assume that $\cap_{i>0} x^i R = (0)$. Note that in K,

$$R[1/x] = \{\, y/x^n \mid y \in R,\ n \geq 0 \,\}.$$

(a) Prove that if R is a UFD then so is $R[1/x]$. [4]

(b) Prove that every nonzero $z \in R[1/x]$ is *uniquely* of the form $z = z'x^e$ with $z' \in R$ not divisible by x and $e \in \mathbb{Z}$; and that if z is prime in $R[1/x]$ then z' is prime in R. [6]

(c) Without assuming R to be a UFD, show that if $q \in R$ divides a product of primes $p_1 p_2 \dots p_n$, then there is a subset $I \subseteq \{1, 2, \dots, n\}$ such that q is an associate of $\prod_{i \in I} p_i$.
Hint: induction on n. [6]

(d) Prove: If $R[1/x]$ is a UFD then R is a UFD. [4]

4. Let $k[X, Y, Z]$ be a polynomial ring over a field k, let $f(Z) \in k[Z]$ be irreducible, of positive degree, and let n be a positive integer. Let π be the natural surjection from $k[X, Y, Z]$ onto the ring

$$R := k[X, Y, Z]/(X^n Y - f(Z)) = k[x, y, z] \qquad (x = \pi(X),\ \text{etc.})$$

(a) Show that R is an integral domain, in which x is prime (see problem 3). [6]

(b) Show that π induces an isomorphism from $k[X, Z]$ onto $k[x, z]$. [3]

(c) Show that in the field of fractions of R, $R[1/x] = k[x, z, 1/x]$. [5]

(d) Show that R is a UFD. (See problem 3. You may assume that $\cap_{i>0}\, x^i R = (0)$.) [6]

5. (a) Show that $K = \mathbb{Q}(\sqrt{5 + \sqrt{5}}\,)$ is a degree-4 *cyclic* galois extension of $\mathbb{Q}$.
Hint. Let $\alpha = \sqrt{5 + \sqrt{5}}$ and $\alpha' = \sqrt{5 - \sqrt{5}} = 2\sqrt{5}/\alpha \in K$. Show that an automorphism taking α to α' must take α' to $-\alpha$. [9]

(b) Take for granted that the polynomial $x^3 - 6x^2 + 2$ is irreducible, with discriminant $1620 = 2^2 3^4 5$. Let F be its splitting field. Show that $L = F(\sqrt{5 + \sqrt{5}}\,)$ is a galois extension of $\mathbb{Q}$, having degree 12 and galois group the group S in problem 1 above. [15]

(c) L has the following subfields: L, F, K, $\mathbb{Q}(\sqrt{5})$, the three subfields generated by the roots of $x^3 - 6x^2 + 2$, and $\mathbb{Q}$. Does it have any others? (Justify your answer!) [6]