Math 901-902 Comprehensive Exam
June 3, 2008

Do two problems from each of the three sections, for a total of *six* problems. If you have doubts about the wording of a problem, please ask for clarification. In no case should you interpret a problem in such a way that it becomes trivial.

Notation: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ signify the fields of rational, real and complex numbers, respectively.

Section I: Groups and Character Theory

(1) Let $p \geq 5$ be a prime number, $\mathbb{F}_p$ be the field with p elements, and π be a primitive element of $\mathbb{F}_p$; that is, π generates the multiplicative group $\mathbb{F}_p^\times$.

(a) Prove that the elements $x := \begin{bmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{bmatrix}$ and $y := \begin{bmatrix} 1 & \pi \\ 0 & 1 \end{bmatrix}$ in $SL_2(\mathbb{F}_p)$ generate a non-abelian subgroup G of order $p(p-1)$.

(b) In the case $p = 5$, give a presentation of G in the usual form of generators and relations.

(2) Let H be a simple group of order 60. Follow this argument to show $H \cong A_5$:

(a) Prove that H is isomorphic to a subgroup of A_6, the *alternating* group of permutations on 6 elements, using the action of H on its Sylow subgroups.

(b) Suppose now that H is a simple subgroup of A_6 of order 60. Prove that the action of A_6 on left cosets of H by left translation (i.e., for $a, g \in A_6$, $(a, gH) \mapsto agH$) gives an isomorphism of A_6 to the *alternating* group of permutations of A_6/H, the set of left cosets.

(c) Show that $H \cong A_5$ using (b). (*Hint*: Show that H can be identified in the isomorphism of (b) with the subgroup H_1 of A_6, where $H_1 = \{\sigma \in A_6 \mid \sigma(1) = 1\}$.)

(3) Let G be a finite group. Let $\mathrm{Irr}(G)$ denote the set of irreducible complex characters of G. Prove that

$$|G| = \sum_{\lambda \in \mathrm{Irr}(G)} \lambda(1)^2.$$

Section II: Fields and Galois Theory

(4) (a) Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree p, and assume that $f(x)$ has exactly two non-real roots in $\mathbb{C}$. Prove that the Galois group of $f(x)$ over $\mathbb{Q}$ is S_p.

(b) Find an example of an irreducible polynomial $g(x) \in \mathbb{Q}[x]$ of degree 4, such that $g(x)$ has exactly two non-real roots in $\mathbb{C}$ and the splitting field of $g(x)$ over $\mathbb{Q}$ has degree 8.

(5) Let K/F be an algebraic extension of fields of characteristic $p > 0$, and let $u \in K$. Prove that u^{p^n} is separable over F for some positive integer n.

(6) Let $K = \mathbb{Q}(i, \sqrt{2})$, an extension of $\mathbb{Q}$ of degree 4. For a field F, let $F^\times$ denote the multiplicative group of non-zero elements of F.

(a) List the three intermediate fields E_1, E_2, E_3 strictly between $\mathbb{Q}$ and K.

(b) Show that $\mathrm{Norm}_{\mathbb{Q}}^{K}(1 + i + \sqrt{2}) = 8$.

(c) Show that $1 + i + \sqrt{2} \notin E_1^\times E_2^\times E_3^\times$, that is, $1 + i + \sqrt{2}$ cannot be expressed in the form $\alpha_1\alpha_2\alpha_3$, with $\alpha_i \in E_i$. ((b) is useful here.)

(d) Prove that $\alpha^2 \in E_1^\times E_2^\times E_3^\times$ for each $\alpha \in K^\times$. (Hint: If E_j is the fixed field of the automorphism σ_j, then $\alpha\alpha^{\sigma_j} \in E_j$.)

Section III: Rings and Modules

(7) Let A be an algebra over the field $\mathbb{Q}$ of rational numbers, and let G be a finite group of $\mathbb{Q}$-algebra automorphisms of A. Let $B = A^G := \{x \in A \,|\, g(x) = x \text{ for every } g \in G\}$.

(a) Prove that $\varphi : A \to A$ defined by

$$\varphi(x) = \frac{1}{|G|} \sum_{g \in G} g(x)$$

is a B-module homomorphism and that $\varphi(x) \in B$ for every $x \in A$.

(b) Show that $A = B \oplus \ker(\varphi)$.

(8) Let R be a commutative ring. Suppose that $H_1, \ldots, H_n$ are pairwise co-maximal ideals of R; that is, $H_i + H_j = R$, for each pair of indices $i \neq j$ in $\{1, \ldots, n\}$.

(a) Prove (from scratch) the Chinese Remainder Theorem: If $x_1, \ldots, x_n \in R$, then there exists an $x \in R$ such that $x \equiv x_i \pmod{H_i}$.

(b) Prove that, if R has only finitely many maximal ideals $P_1, \ldots, P_n$, and M is a finitely generated R-module such that $M_{P_i} \neq (0)$ for every i, then there exists an element $x \in M$ such that $x \notin P_iM$ for every i.

(9) Let M be a flat module over a commutative ring R. Prove that the following statements are equivalent:

(i) $X \otimes_R M \neq (0)$, for every non-zero R-module X (i.e. M is *faithfully flat*).

(ii) $X \otimes_R M \neq (0)$, for every non-zero cyclic R-module X.

(iii) $M \neq \mathbf{m}M$, for every maximal ideal $\mathbf{m}$ of R.