Math 362 Final Exam; Monday, May 5 1997 4:15–6:15pm

Instructions. Answer questions 1–3. To receive full points, you must justify all your steps by either explicit argument or by briefly indicating which theorems from class you are using. On the other hand, you do not have to prove theorems which you quote unless specifically asked to.

1. *(45 points)* Let K be a field of characteristic zero.

(a) Explain what is meant by saying an extension field L of K is a radical extension of K.

(b) Define the Galois group of a polynomial $f \in K[t]$.

(c) Explain what is meant by saying that a polynomial $f \in K[t]$ is solvable by radicals.

(d) Explain what is meant by saying that a group G is solvable.

(e) For a normal subgroup N of a group G, what is the relationship between solvability of G, N and G/N? Give an example of a group of order 180 which is solvable and an example of one which is not solvable. Are there any infinite solvable groups?

(f) Carefully state the theorem giving the relationship between solvable groups and solvability of equations by radicals. For which natural numbers n is every polynomial of degree n over a field of characteristic zero solvable by radicals?

(g) State conditions on a polynomial f of prime degree p over the rational numbers which are sufficient to ensure that the Galois group of f is isomorphic to the symmetric group S_p.

(h) Use the result in (g) to show that the extension $L/\mathbf{Q}$ has S_3 as Galois group, where L is the subfield of $\mathbf{C}$ generated by the roots of $t^3 + 3t + 3$. **2.** *(45 points)* Let $K = \mathbf{Q}(\omega)$ where $\omega = e^{2\pi i/9} \in \mathbf{C}$.

(a) Let $f = t^6 + t^3 + 1 = (t^9 - 1)/(t^3 - 1) \in \mathbf{Q}[t]$. Applying Eisenstein's criterion to $f(t+1)$, deduce that f is irreducible over $\mathbf{Q}$. Conclude that f is the minimal polynomial of ω over $\mathbf{Q}$.

(b) Show that the distinct roots of f in K are the elements ω^i for $i = 1, 2, 4, 5, 7$ and 8, and conclude that for each such i, there is an automorphism σ_i of $\mathbf{Q}(\omega)$ with $\sigma_i(\omega) = \omega^i$. Show that the Galois group $G = \Gamma(K/\mathbf{Q})$ consists of these 6 automorphisms σ_i.

(c) Calculate $(\sigma_i\sigma_j)(\omega)$ and hence show that the map $\sigma_i \mapsto \bar{i}$ is a group isomorphism between G and the multiplicative group $\mathbf{Z}_9^*$ of units in $\mathbf{Z}_9$ (here, $\bar{i}$ denotes the congruence class of i in $\mathbf{Z}_9$).

(d) Show that G is a cyclic group of order 6 generated by σ_2.

(e) What conditions must a finite field extension satisfy to ensure that the Galois correspondence is bijective? Prove that these conditions are satisfied by $K/\mathbf{Q}$.

(f) For each of the non-trivial proper subgroups of G, find the corresponding fixed field in K, proving carefully that your answer is correct. Draw diagrams showing all subgroups of G and the corresponding intermediate fields, exhibiting the Galois correspondence.

3. *(60 points)*

(a) For which integers p and q does there exist a finite field $\mathbf{GF}(q)$ with q elements and characteristic p?

(b) For p, q satisfying the conditions you gave in (a), describe an explicit polynomial in $\mathbf{Z}_p[t]$ such that $\mathbf{GF}(q)$ is the splitting field (and also the set of roots) of f.

(c) Explain using the results mentioned in (b) why every extension of finite fields is separable and normal (for separability, you'll have to compute the formal derivative of the polynomial in (b)).

(d) For which integers q' does $\mathbf{GF}(q)$ have a subfield with q' elements? How many subfields with q' elements are there?

(e) Let E be a finite field, let F be the splitting field of an irreducible polynomial $f \in E[t]$ and let α be a root of f in F. Show that $F = E(\alpha)$. (hint: $E(\alpha)/E$ is normal, by (c)).

(f) For which of the finite fields $\mathbf{GF}(q)$ is it true that every non-identity element of the multiplicative group $\mathbf{GF}(q)^*$ is a generator? Give an example (with $q \geq 5$, to avoid trivialities) for which this holds, and an example (with $q \geq 5$) for which it doesn't hold.

Let $P = \mathbf{Z}_2$ and $f = t^2 + t + 1$, $g = t^3 + t + 1$ and $h = t^5 + t^2 + 1$ in the polynomial ring $P[t]$. The next parts (h)–(k) of this question will show that the splitting field F of the degree ten polynomial fgh over P is isomorphic to $\mathbf{GF}(2^{30})$.

(g) Draw a diagram showing all the subfields $\mathbf{GF}(q)$ of $\mathbf{GF}(2^{30})$ and the inclusion relations amongst them.

(h) Show that f is the unique irreducible quadratic polynomial over P, and that g and h are also irreducible (hint; note that a reducible quintic with no root must have an irreducible quadratic factor).

(i) Let α, β, γ be roots in F of f, g and h, respectively. Determine $[P(\alpha)\colon P]$, $[P(\beta)\colon P]$ and $[P(\gamma)\colon P]$, and show that $n := [F\colon P]$ is divisible by 30.

(j) Show that F has a subfield $\mathbf{GF}(2^{30})$ with 2^{30} elements. Then show that $P(\alpha)$, $P(\beta)$ and $P(\gamma)$ are all contained in $\mathbf{GF}(2^{30})$.

(k) Using (e), show that all roots of fgh are in $\mathbf{GF}(2^{30})$ and conclude that $F = \mathbf{GF}(2^{30})$.

(l) Suppose that the non-constant polynomial f over the finite field F has factorization $f = f_1 \dots f_n$ where the f_i are (not necessarily distinct) irreducible polynomials over F of degree n_i. What degree $[E : F]$ would you expect for the splitting field E of f over F? Justify your answer if you can.