Math 242 — Spring 2005
Final Exam, June 8. Time: 2 1/2 hours.

Remarks: Each problem on this exam is worth 12 points. Please make it clear in your exam booklet which problem you are answering on any given page. **If you cannot solve part (a) of a problem, you may assume the result and work on part (b), and so forth.** The exam is somewhat long; do as much of it as you can, and prioritize your time carefully.

Please communicate your ideas clearly and give all necessary justifications for your statements.

Good luck!

Problem 1. a) Let D be a domain, and $a, b \in D$ be nonzero elements. Carefully define what it means to say that c is a GCD (greatest common divisor) of a and b.

b) Show (from the definition) that if a GCD exists, then it is unique up to associates.

c) Assume that D is a UFD (unique factorization domain). Show that a GCD of a and b does indeed exist.

Problem 2. a) Let E be an algebraic extension of F. You may assume that $[E : F]$ is finite. Carefully define what it means for the extension E/F to be separable.

b) Give an example of an inseparable field extension.

c) Assume that F has characteristic zero. Sketch the proof of why the extension E/F is separable. (Hint: derivative.)

Problem 3. Use the Gauss Lemma (the one about primitive polynomials) to show that if $f(x) \in \mathbf{Z}[x]$ factors nontrivially in $\mathbf{Q}[x]$, then f also factors nontrivially in $\mathbf{Z}[x]$.

Problem 4. a) Find polynomials $a(x), b(x) \in \mathbf{Q}[x]$ such that

$$(x^2 - 2)a(x) + (x^3 - 3)b(x) = 1.$$

b) Find a polynomial $f(x) \in \mathbf{Q}[x]$ such that $f(\sqrt{2}) = 1$ and $f(\sqrt[3]{3}) = -1$. (The point is that $f(x)$ must have rational coefficients — the problem would become trivial if we allowed real or complex coefficients, since we would then be able to take f to be a linear polynomial.) **NOTE: you do not have to simplify your expression for f.**

Problem 5. Let $f(x) = x^4 + x + \overline{1} \in \mathbf{Z}_2[x]$, and let α be a root of f in the algebraic closure $\overline{\mathbf{Z}_2}$ of $\mathbf{Z}_2$.

a) Show that $f(x)$ is irreducible in $\mathbf{Z}_2[x]$.

b) Express all the roots of $f(x)$ in the form $a\alpha^3 + b\alpha^2 + c\alpha + d$, for $a, b, c, d \in \mathbf{Z}_2$. (Hint: we know that one of the roots is α. To find the others, use Galois theory of the extension $\mathbf{Z}_2(\alpha)/\mathbf{Z}_2$. You may use the result of Problem 6 for this exercise, even if you have not done Problem 6.)

Problem 6. Let E/F be a Galois extension, with $[E : F] = n$. Take an element $\alpha \in E$. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$ be the r conjugates of α.

a) Show that r is a factor of n.

b) Show that every conjugate α_i is of the form $\sigma(\alpha)$, for some $\sigma \in G(E/F)$.

c) Write $G(E/F) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Show that

$$(x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_n(\alpha)) = \mathrm{irr}(\alpha, F)^{n/r}.$$

Problem 7. Let $\zeta = e^{2\pi i/9}$, and consider the cyclotomic field $E = \mathbf{Q}(\zeta) = \mathbf{Q}(\mu_9)$.

a) Find $\mathrm{irr}(\zeta, \mathbf{Q})$. You may use all theorems stated in class, even if they were stated without proof. Why does this mean that the regular 9-gon is not constructible?

b) Show that $G(E/\mathbf{Q})$ is cyclic, and find a specific generator σ.

c) Let $K = \mathbf{Q}(\zeta + \zeta^{-1})$ and $L = \mathbf{Q}(\zeta^3)$. Show that K and L are the only intermediate fields between $\mathbf{Q}$ and E. (Hint: what subgroups do they correspond to?)

d) Find $[K : \mathbf{Q}]$ and $[L : \mathbf{Q}]$.

Problem 8. Define the two complex numbers $\alpha = \sqrt{3 + \sqrt{11}}$ and $\beta = \sqrt{3 - \sqrt{11}}$.

a) Find $f(x) = \mathrm{irr}(\alpha, \mathbf{Q})$.

b) Show that the splitting field of f is $\mathbf{Q}(\alpha, \beta)$. Call this field E.

c) Find $\mathrm{irr}(\beta, \mathbf{Q}(\alpha))$, and deduce that $[E : \mathbf{Q}] = 8$.

d) Make a table of all 8 elements of $G = G(E/\mathbf{Q}) = \{\sigma_1, \ldots, \sigma_8\}$, showing their effect on α, $\sqrt{11}$, and β (why is this enough to specify each σ_i?).

e) What subgroup $H < G$ corresponds to the intermediate field $K = \mathbf{Q}(\alpha)$? Is H a normal subgroup of G? Why?

f) What subgroup $H' < G$ corresponds to the intermediate field $K' = \mathbf{Q}(\sqrt{11})$? Is H' a normal subgroup of G? Why?

Problem 9. This problem gives you an idea of how a solvable Galois group allows one to solve a polynomial by radicals. We'll sketch the main ideas involved in solving a general cubic equation. We start with a field F in characteristic zero, and we **assume that F contains a primitive 3rd root of unity ζ.** Let y_1, y_2, y_3 be three "independent" transcendental elements, and let

$$K = F(s_1, s_2, s_3), \qquad L = F(y_1, y_2, y_3)$$

where $s_1 = y_1 + y_2 + y_3$, $s_2 = y_1y_2 + y_1y_3 + y_2y_3$, and $s_3 = y_1y_2y_3$ are the elementary symmetric polynomials, as usual. Recall that $\Delta = (y_1 - y_2)(y_1 - y_3)(y_2 - y_3) \in L$ is the discriminant.

a) By considering the action of S_3 (viewed as the Galois group $G(L/K)$), show that $\Delta^2 \in K$ but $\Delta \notin K$. Deduce that the field $M = K(\Delta)$ is an extension of K by radicals, with $[M : K] = 2$. (CAUTION: do not spend time trying to explicitly write Δ^2 in terms of s_1, s_2, s_3!! The expression is rather complicated.)

b) Now let $\beta = y_1 + \zeta y_2 + \zeta^2 y_3$. Show that $\beta^3 \in M$ but $\beta \notin M$, this time by considering the action of the subgroup $G(L/M)$ of S_3. (Do not calculate β^3 directly, but instead show that every $\sigma \in G(L/M)$ sends β to some simple multiple of β, which allows you to understand the action on β^3.) Deduce that $L = M(\beta)$ and that L is an extension of M by radicals.

Cultural note: this shows that we can get the roots y_1, y_2, y_3 of the polynomial $x^3 - s_1x^2 + s_2x - s_3 \in K[x]$ by taking a square root of an element of K to get Δ, then a cube root of an element of $K[\Delta]$ to get β, which we can use to express all the elements of L, in particular y_1, y_2, and y_3.