Math 594. Algebra II.
Final Exam (April 14–23, 2002)
No time limit

Name: ____________________

Read all questions carefully. *Do any* 5 *out of the* 6 *questions.* You will not be given partial credit on the basis of having misunderstood a question, and please show all work. *Unless otherwise indicated*, you may use without proof all results which were discussed in lecture, homework, or the course text. Be clear and precise in stating what you use.

If you are unable to solve part of a problem, you may still use the conclusion from that part to do subsequent parts of the problem. If your solution does not fit in the indicated space, please use the back of the same page. This is an open-book, open-notebook exam. It is due in my office during 1:30–3:30pm on Wednesday, April 23. At 3:30pm the solution set will become available on the web, so late submission will be unacceptable. *You must turn in your exam to me personally; do not leave it in a mailbox or on an office door.*

You must sign below (indicating your agreement with) the following honor pledge: *I pledge my honor that I have not used calculators, electronic computing machines of any sort, the Internet, contact with other human beings, or any published book other than the course text for mathematical assistance in connection with my work on this exam.*

Question	Possible	Actual
1	20	
2	20	
3	20	
4	20	
5	20	
6	20	
Total	100	

1. (20 pts) Work out the Galois group of $X^4 - 7$ over each of the following fields: $\mathbf{Q}$, $\mathbf{Q}(\sqrt{7})$, $\mathbf{Q}(\sqrt{-7})$, $\mathbf{Q}(\sqrt{-1})$. Determine the lattice of subfields for the case of $\mathbf{Q}$ as the base field.

2. Recall from class that we have a natural isomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \simeq (\mathbf{Z}/n)^\times$ for any $n \geq 1$, where ζ_n is a primitive nth root of unity in some extension of $\mathbf{Q}$. In this problem, we work inside of a fixed algebraic closure $\overline{\mathbf{Q}}$.

(i) (10 pts) For n and m positive integers, with $n|m$, show that the natural diagram of groups

$$\begin{array}{ccc} \mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}) & \simeq & (\mathbf{Z}/m)^\times \\ \downarrow & & \downarrow \\ \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) & \simeq & (\mathbf{Z}/n)^\times \end{array}$$

commutes. Use this to show that $\mathbf{Q}(\zeta_a) \cap \mathbf{Q}(\zeta_b) = \mathbf{Q}$ if and only if $\gcd(a, b) = 1$ or 2. Hint: when $\gcd(a, b) = 1$, apply the commutative diagram with $m = ab$ and use the Chinese Remainder Theorem (Up to 3 points extra credit for determining exactly when $\mathbf{Q}(\zeta_n) \simeq \mathbf{Q}(\zeta_m)$).

(ii) (10 pts) Using the isomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}) \hookrightarrow (\mathbf{Z}/p^n)^\times$ for any prime p and any $n \geq 1$, along with the known structure of the group $(\mathbf{Z}/p^n)^\times$, show that $\mathbf{Q}(\zeta_{p^n})$ contains a unique subfield K of degree p^{n-1} over $\mathbf{Q}$ and that $K \cap \mathbf{Q}(\zeta_p) = \mathbf{Q}$.

3. (20 pts) The problem works out some examples with quadratic fields.

(*i*) (8 pts) Construct a finite Galois extension $L/\mathbf{Q}(\sqrt{2})$ with $\mathrm{Gal}(L/\mathbf{Q}(\sqrt{2})) \simeq \mathbf{Z}/2 \times \mathbf{Z}/2$ and L *not* Galois over $\mathbf{Q}$ (prove it!).

(*ii*) (12 pts) Using that $\mathrm{Gal}(\mathbf{Q}(\zeta_8)/\mathbf{Q}) \to (\mathbf{Z}/8)^\times$ is an isomorphism, find all quadratic subfields of $\mathbf{Q}(\zeta_8)$, writing each in the form $\mathbf{Q}(\sqrt{d})$ for an explicit squarefree integer d (possibly negative). Hint: first prove there are three such subfields.

4. (20 pts) Give examples for each of the following, or indicate that no such example exists. In each case, provide brief justification.
(*i*) (4 pts) A finite field of order 30.

(*ii*) (4 pts) A field F which is abstractly isomorphic to a proper subfield $F' \subsetneq F$.

(*iii*) (4 pts) A Galois extension of $\mathbf{Q}$ with Galois group C_{13} (hint: is this a quotient of $(\mathbf{Z}/p)^{\times}$ for some prime p?).

(*iv*) (4 pts) A Galois extension of $\mathbf{F}_3$ with Galois group $\mathbf{Z}/2 \times \mathbf{Z}/2$.

(*v*) (4 pts) A field of characteristic zero which cannot be embedded into $\mathbf{C}$.

5. (20 pts) If K/k is an extension fields, a k-*derivation* from K to K is a k-linear map $D : K \to K$ such that $D(xy) = xD(y) + yD(x)$ for all $x, y \in K$ (the *Leibnitz rule*).

(*i*) (5 pts) Prove that for any k-derivations $D_1, D_2 : K \to K$ and any elements $c_1, c_2 \in K$, $c_1D_1 + c_2D_2$ and $D_1 \circ D_2 - D_2 \circ D_1$ are k-derivations from K to K.

(*ii*) (5 pts) Applying the Leibnitz Rule to the identities $1 \cdot 1 = 1$ and $xx^{-1} = 1$ (for $x \neq 0$), conclude that $D(1) = 0$ and $D(x^{-1}) = -D(x)/x^2$ for any nonzero $x \in K$, and likewise show $D(x^n) = nx^{n-1}D(x)$ for all $n \geq 1$ and $x \in K$. Deduce that if $a \in K$ then two k-derivations $D_1, D_2 : K \to K$ coincide on $k(a) \subseteq K$ if and only if $D_1(a) = D_2(a)$.

(iii) (5 pts) If $K = k(T)$ for an indeterminate T, prove that the k-derivations $D : K \to K$ are precisely the operators $D_c : f \mapsto c\,f'(T)$ for varying $c \in K$ (hint: prove that $c \cdot \mathrm{d}/\mathrm{d}T$ is a derivation with value c on T, and use *(ii)*).

(iv) (5 pts) For any $a \in K$ and $f \in k[T]$, prove $D(f(a)) = f'(a)D(a)$ for any k-derivation $D : K \to K$. Conclude that if K/k is separable algebraic, then the only k-derivation $D : K \to K$ is $D = 0$ (this property turns out to *characterize* separable extensions among algebraic extensions, and is fundamental in more advanced field theory).

6. (20 pts) We say that a polynomial $f \in k[X]$ over a field k is *additive* if $f(U) + f(V) = f(U+V)$ in $k[U,V]$.

(*i*) (5 pts) If k has characteristic zero, prove that an additive polynomial in $k[X]$ is precisely one of the form $f = cX$ with $c \in k$.

(*ii*) (10 pts) If k has positive characteristic p, show that $f \in k[X]$ is additive if and only if $f = \sum c_j X^{p^j}$.

(iii) (5 pts) We say that a polynomial $f(X)$ is *multiplicative* if $f(U)f(V) = f(UV)$ in $k[U,V]$. In any characteristic, prove that the multiplicative polynomials are the zero polynomial and the monomials $f = X^n$ with $n \geq 0$.