MATH 581 — SECOND MIDTERM EXAM

May 12, 2006

NAME: ______________________________

1. Do not open this exam until you are told to begin.
2. This exam has 9 pages including this cover. There are 9 problems.
3. Do not separate the pages of the exam.
4. Your proofs should be neat and legible. You may and should use the back of pages for scrap work.
5. If you are unsure whether you can quote a result from class or the book, please ask.
6. Please turn **off** all cell phones.

PROBLEM	POINTS	SCORE
1	12	
2	12	
3	5	
4	5	
5	16	
6	12	
7	12	
8	10	
9	16	
TOTAL	100	

1. (3 points each) **(a)** Give a basis of $\mathbb{Q}[\sqrt{5}]$ over $\mathbb{Q}$. What is $[\mathbb{Q}[\sqrt{5}] : \mathbb{Q}]$? You do not need to prove it is a basis.

(b) Prove that $\sqrt{7} \notin \mathbb{Q}[\sqrt{5}]$.

(c) Give a basis of $\mathbb{Q}[\sqrt{7}, \sqrt{5}]$ over $\mathbb{Q}[\sqrt{5}]$. What is $[\mathbb{Q}[\sqrt{7}, \sqrt{5}] : \mathbb{Q}[\sqrt{5}]]$? You do not need to prove it is a basis.

(d) Give a basis of $\mathbb{Q}[\sqrt{5}, \sqrt{7}]$ over $\mathbb{Q}$. What is $[\mathbb{Q}[\sqrt{5}, \sqrt{7}] : \mathbb{Q}]$? You do not need to prove it is a basis.

2. (3 points each) Let V be a vector space over a field F and $\{v_1, \ldots, v_n\}$ a subset of V.

(a) Define what it means for $\{v_1, \ldots, v_n\}$ to be linearly independent.

(b) Define what it means for $\{v_1, \ldots, v_n\}$ to span V.

(c) Give a basis of $\mathbb{R}^3$ as a vector space over $\mathbb{R}$. Be sure to prove your answer is actually a basis!

(b) Prove that if $\{v_1, v_2, v_3, v_4\}$ is linearly independent in V, then so is $\{v_1 - v_2, v_2 - v_3, v_3 - v_4, v_4\}$.

3. (5 points) Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree 5 with no roots in $\mathbb{Q}$. (Note, we do NOT assume $f(x)$ is irreducible!!!) Let α be a root of $f(x)$. What are the possible values of $[\mathbb{Q}[\alpha] : \mathbb{Q}]$?

4. (5 points) Prove either (a) OR (b). Indicate clearly which one you would like me to grade.
(a) Let R be a commutative ring. Prove that the ideal $\langle x \rangle$ in the polynomial ring $R[x]$ is a maximal ideal if and only if R is a field.
(b) Let $\phi : R \to S$ be a surjective homomorphism of commutative rings and let $\wp$ be a prime ideal in R. Prove that $\phi(\wp)$ is a prime ideal of S. (You may quote the homework problem that $\phi(\wp)$ is an ideal!)

5. (3+3+4+6 points) Consider the finite field $\mathbb{F}_{7^{36}}$.

(a) How many elements are in $\mathbb{F}_{7^{36}}$?.

(b) What is the dimension of $\mathbb{F}_{7^{36}}$ as a vector space over $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$?

(c) Is $\mathbb{F}_{7^{36}} \cong \mathbb{Z}/7^{36}\mathbb{Z}$? Justify your answer!

(d) Arrange the subfields of $\mathbb{F}_{7^{36}}$ into a diagram showing containment between the subfields. Be sure to label the diagram indicating the degrees of the extensions.

6. (4 points each) **(a)** Show that the number $\sqrt[7]{2}$ is not constructible with straightedge and compass.

(b) Show it is possible to construct a regular 12-gon with straightedge and compass.

(c) Show it is impossible to square the circle, i.e., show it is not possible to construct (with a straightedge and compass) a square that has the same area as a circle of radius 1.

7. (4 points each) Let $F \subseteq K$ be a finite field extension with $\alpha \in K$ but $\alpha \notin F$.

(a) Prove that $F[\alpha^2] \subseteq F[\alpha]$.

(b) Find a polynomial $f(x) \in F[\alpha^2][x]$ so that $f(\alpha) = 0$. What are the possibilities for $[F[\alpha] : F[\alpha^2]]$?

(c) Prove that if $[F[\alpha] : F]$ is odd, then $F[\alpha^2] = F[\alpha]$.

8. (5 points each) Let $F \subseteq K$ be a finite field extension such that $[K : F] = n$. Let $\alpha \in K$ so that $\alpha \notin F$. In this problem you will show that α is algebraic, i.e., there is a polynomial $f(x) \in F[x]$ so that $f(\alpha) = 0$. So do NOT assume such a polynomial exists to do any proofs in this problem!

(a) Prove that $\{1, \alpha, \ldots, \alpha^n\}$ must be linearly dependent over F. (Hint: How many elements are in this set?)

(b) Use part (a) to prove that there exists $f(x) \in F[x]$ so that $f(\alpha) = 0$.

9. (4 points each) Let p be a prime number and ω a p^{th} root of unity.

(a) Prove that $[\mathbb{Q}[\sqrt[p]{3}] : \mathbb{Q}] = p$.

(b) Prove that $[\mathbb{Q}[\omega] : \mathbb{Q}] = p - 1$.

(c) Prove that $[\mathbb{Q}[\omega, \sqrt[p]{3}] : \mathbb{Q}] = p(p-1)$. You are not allowed to quote any results that make this part trivial. (Hint: $\gcd(p, p-1) = 1$) (You may use the back of this page if you need more space)

(d) Use part (c) to conclude that $f(x) = x^p - 3$ is irreducible over $\mathbb{Q}[\omega]$. (This is a very difficult fact to prove by any other method!)