MATH 581 — SECOND MIDTERM EXAM

May 12, 2006

NAME: Solutions

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.

A basis is given by $\{1, \sqrt{5}\}$ and $[\mathbb{Q}[\sqrt{5}] : \mathbb{Q}] = 2$.

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

Proof: Suppose $\sqrt{7} \in \mathbb{Q}[\sqrt{5}]$, i.e., there exists $a, b \in \mathbb{Q}$ such that $\sqrt{7} = a + b\sqrt{5}$. We then have $(\sqrt{7} - b\sqrt{5})^2 = a^2$. Rearranging this we have $2b\sqrt{35} = 7 + 5b^2 - a^2$. Note that $b \neq 0$ for otherwise we'd have $\sqrt{7} \in \mathbb{Q}$ which we know it is not ($x^2 - 7$ is irreducible by Eisenstein with $p = 7$). Thus we have $\sqrt{35} = \frac{1}{2b}(7 + 5b^2 - a^2) \in \mathbb{Q}$. However, $\sqrt{35} \notin \mathbb{Q}$ since $x^2 - 25$ is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 7$. Thus, it must be 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.

We know from part (b) that $[\mathbb{Q}[\sqrt{7}, \sqrt{5}] : \mathbb{Q}[\sqrt{5}]] = 2$. A basis is given by $\{1, \sqrt{7}\}$.

(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.

A basis is given by $\{1, \sqrt{5}, \sqrt{7}, \sqrt{35}\}$ and $[\mathbb{Q}[\sqrt{5}, \sqrt{7}] : \mathbb{Q}] = 4$.

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.

See your textbook.

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

See your textbook.

(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!

Proof: A basis of $\mathbb{R}^3$ is given by $\{(1,0,0), (0,1,0), (0,0,1)\}$. Let $(x, y, z) \in \mathbb{R}^3$. Then $(x, y, z) = x(1,0,0) + y(0,1,0) + z(0,0,1)$, so the set is a spanning set. To see it is linearly independent, suppose $a(1,0,0) + b(0,1,0) + c(0,0,1) = (0,0,0)$, i.e., $(a, b, c) = (0,0,0)$. It is now clear that $a = b = c = 0$ and thus the set is linearly independent as well. ■

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

Proof: Suppose there exists $a, b, c, d \in F$ such that $a(v_1 - v_2) + b(v_2 - v_3) + c(v_3 - v_4) + dv_4 = 0$. Rearranging this we have the equation

$$av_1 + (b - a)v_2 + (c - b)v_3 + (d - c)v_4 = 0.$$

Using that $\{v_1, v_2, v_3, v_4\}$ is linearly independent over F gives that $a = b - a = c - b = d - c = 0$. This gives $a = 0$, which in turn gives $b - 0 = 0$, i.e., $b = 0$. Similarly we get $c = 0$ and $d = 0$ and thus the set is linearly independent as claimed. ■

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 $[\mathbb{Q}[\alpha] : \mathbb{Q}]$?

Suppose we factor $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Q}[x]$. Since we assume that $f(x)$ has no roots in $\mathbb{Q}$ there are only two possibilities for the degrees of $g(x)$ and $h(x)$ if $f(x)$ is reducible. We could have $\deg g(x) = 2$ and $\deg h(x) = 3$ or $\deg g(x) = 3$ and $\deg h(x) = 2$. If either one had degree 1 we would have a root in $\mathbb{Q}$. If either one had degree 4 it would force the other to have degree 1 and give a root in $\mathbb{Q}$. Thus, the possibilities of $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ are 5 (if $f(x)$ is irreducible), 2, and 3 (if $f(x)$ is reducible).

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!)

Proof (a): Recall that $\mathfrak{m}$ is a maximal ideal in a ring S if and only if $S/\mathfrak{m}$ is a field. Applying this to this problem we see that $\langle x \rangle$ is a maximal ideal in $R[x]$ if and only if $R[x]/\langle x \rangle$ is a field. However, we know that $R[x]/\langle x \rangle$ is isomorphic to R under the First Isomorphism Theorem (use the map $R[x] \to R$ by $f(x) \mapsto f(0)$). Thus, $\langle x \rangle$ is a maximal ideal in $R[x]$ if and only if R is a field. ■

Proof (b): Let $ab \in \phi(\wp)$. Using that ϕ is surjective we have that there exists $c, d \in R$ such that $\phi(c) = a$ and $\phi(d) = b$. Thus we have that $\phi(cd) = \phi(c)\phi(d) \in \phi(\wp)$. Thus we have $cd \in \wp$ by definition of $\phi(\wp)$. Since $\wp$ is a prime ideal we have that $c \in \wp$ or $d \in \wp$. But then $\phi(c) \in \phi(\wp)$ or $\phi(d) \in \phi(\wp)$. Thus, $\phi(\wp)$ is a prime ideal. ■

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

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

There are 7^{36} elements in this finite field.

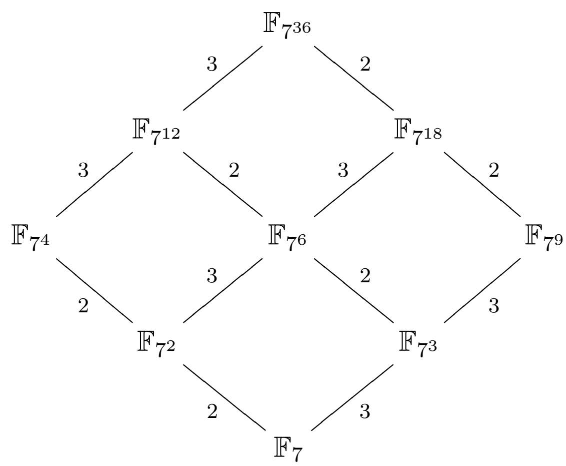
(b) What is the dimension of $\mathbb{F}_{7^{36}}$ as a vector space over $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$?

The dimension is 36.

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

They are NOT isomorphic. The ring $\mathbb{Z}/7^{36}\mathbb{Z}$ is not even a field as 7^{36} is NOT a prime number.

(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.

Proof: Note that $\sqrt[7]{2}$ is a root of $f(x) = x^7 - 2$, which is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 2$. Thus, $[\mathbb{Q}[\sqrt[7]{2}] : \mathbb{Q}] = 7$. Since 7 is not a power of 2, it must be that $\sqrt[7]{2}$ is not a constructible number. ■

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

Proof: Recall it is possible to construct a regular n-gon if and only if one can construct the angle $\frac{2\pi}{n}$ which is possible if and only if $\cos \frac{2\pi}{n}$ and $\sin \frac{2\pi}{n}$ are constructible numbers. Observe that $\cos \frac{2\pi}{12} = \cos \frac{\pi}{6} = \frac{\sqrt{3}}{2}$. Since all integers are constructible and we can take square roots of constructible numbers to get a constructible number, we use the fact that the constructible numbers form a field to conclude $\frac{\sqrt{3}}{2}$ is constructible. Similarly, $\sin \frac{2\pi}{12} = \frac{1}{2}$ so is constructible as well. Thus, it is possible to construct a regular 12-gon. ■

(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.

Proof: In order to construct such a square we would need to be able to construct a square with area π. Thus, we would need to be able to construct $\sqrt{\pi}$. However, $[\mathbb{Q}[\sqrt{\pi}] : \mathbb{Q}]$ is not finite, let alone finite and a power of 2! Thus, $\sqrt{\pi}$ is NOT a constructible number. ■

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

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

Proof: It is enough to show that $\alpha^2 \in F[\alpha]$, but this is clear as $\alpha \in F[\alpha]$ and so α^2 is as well since $F[\alpha]$ is closed under multiplication. ■

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

Note that $f(x) = x^2 - \alpha^2 \in F[\alpha^2][x]$ and $f(\alpha) = 0$. This shows that $[F[\alpha] : F[\alpha^2]] = 1$ or 2 depending on whether $f(x)$ is irreducible or not.

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

Proof: Observe that we have $F \subseteq F[\alpha^2] \subseteq F[\alpha]$. If $[F[\alpha] : F]$ is odd, this means that $[F[\alpha] : F[\alpha^2]]$ must divide an odd number. However, we showed in part (b) that $[F[\alpha] : F[\alpha^2]]$ must be 1 or 2. Since 2 cannot divide an odd number it must be that $[F[\alpha] : F[\alpha^2]] = 1$ and thus $F[\alpha] = F[\alpha^2]$. ■

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?)

Proof: There are $n + 1$ elements in this set. Since $[K : F] = n$, a basis contains exactly n elements. We know that a linearly independent set must have less elements then a basis, thus it must be that the set is linearly dependent. ■

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

Proof: We know that $\{1, \alpha, \ldots, \alpha^n\}$ is a linearly dependent set. Thus there exists $a_i \in F$ so that

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Set $f(x) = a_0 + a_1x + \cdots a_nx^n \in F[x]$. Then $f(\alpha) = 0$ by construction. ■

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

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

Proof: Let $f(x) = x^p - 3$. Then $f(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein with the prime 3. Thus, $[\mathbb{Q}[\sqrt[p]{3}] : \mathbb{Q}] = p$. ■

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

Proof: Here we use that ω is a root of the irreducible polynomial $g(x) = x^{p-1} + cdots + x + 1$. Thus, $[\mathbb{Q}[\omega] : \mathbb{Q}] = p - 1$. ■

(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)

Proof: Since $\mathbb{Q}[\sqrt[p]{3}]$ and $\mathbb{Q}[\omega]$ are both subfields of $\mathbb{Q}[\omega, \sqrt[p]{3}]$ we have that $p | [\mathbb{Q}[\omega, \sqrt[p]{3}] : \mathbb{Q}]$ and $p - 1 | [\mathbb{Q}[\omega, \sqrt[p]{3}] : \mathbb{Q}]$. Using that p and $p-1$ are relatively prime we have that $p(p-1)$ is the least common multiple of p and $p-1$ and thus $p(p-1)$ divides $[\mathbb{Q}[\omega, \sqrt[p]{3}] : \mathbb{Q}]$.
Now observe that since ω is a root of $g(x)$ with degree $p-1$, it must be that $[\mathbb{Q}[\sqrt[p]{3}, \omega] : \mathbb{Q}[\sqrt[p]{3}]] \leq p - 1$ since the extension can be at most $p-1$ if $g(x)$ is irreducible over $\mathbb{Q}[\sqrt[p]{3}]$ and is less if $g(x)$ factors. Thus, $[\mathbb{Q}[\omega, \sqrt[p]{3}] : \mathbb{Q}] \leq p(p-1)$. But we had the inequality in the other direction since $p(p-1) | [\mathbb{Q}[\omega, \sqrt[p]{3}] : \mathbb{Q}]$ above, thus we must have equality. ■

(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!)

Proof: Note our proof shows that we must have $[\mathbb{Q}[\omega, \sqrt[p]{3}] : \mathbb{Q}[\omega]] = p$. Thus, it must be that $x^p - 3$ remains irreducible over $\mathbb{Q}[\omega]$ or we would get a smaller extension. ■