FINAL EXAM
MATH 200B, UCSD, WINTER 17

You have three hours.

There are 11 problems, and the total number of points is 170. Show all your work. *Please make your work as clear and easy to follow as possible.*

Name:____________________________

Signature:____________________________

Section instructor:________________________

Section Time:__________________________

Problem	Points	Score
1	30	
2	10	
3	10	
4	10	
5	15	
6	15	
7	20	
8	15	
9	25	
10	10	
11	10	
12	10	
13	10	
14	10	
15	10	
Total	170	

1. (30pts) (i) *Give the definition of a symmetric multilinear map.*

If M and N are R-modules, a function

$$f\colon M^d \longrightarrow N$$

is multilinear if it is linear in each variable. It is symmetric if it is invariant under switching any two entries.

(ii) *Give the definition of the algebraic closure of a field K.*

The field extension L/K is the algebraic closure of K, if L/K is algebraic and if every polynomial with coefficients in K, splits in L.

(iii) *Give the definition of a normal extension.*

An algebraic extension L/K is normal if every polynomial with coefficients in K and one zero in L splits in L.

(iv) *Give the definition of a separable polynomial, a separable element and a separable extension.*

A polynomial is separable, if each irreducible factor has no repeated roots. An element $\alpha \in L/K$ is separable, if its minimum polynomial over K is separable. An extension L/K is separable, if every element $\alpha \in L$ is separable over K.

(v) *Give the definition of the Galois group of an extension.*

The set of automorphisms of L that fix the groundfield K, considered as a subgroup of the set of all permutations of L.

(vi) *Give the definition of a character.*

A character is a group homomorphism

$$\chi\colon G \longrightarrow K^*$$

from a group G to the multiplicative group K^* of a field K.

2. (10pts) *Let M be a Noetherian R-module. If $\phi\colon M \longrightarrow M$ is a surjective R-linear map, prove that ϕ is an automorphism.*

Let M_n be the kernel of ϕ^n. Note that we have an ascending chain,

$$M_1 \subset M_2 \subset M_3 \subset \dots.$$

Suppose that $M_1 \neq 0$. We will define $m_n \in M_n - M_{n-1}$ recursively, so that $\phi(m_n) = m_{n-1}$. By assumption, there is $m_1 \in M_1$, such that $m_1 \neq 0$. Suppose we have defined $m_1, m_2, \dots, m_n$. As ϕ is surjective, there is an $m_{n+1} \in M$ such that $\phi(m_{n+1}) = m_n$. As $m_n \in M_n$, it is immediate that $m_{n+1} \in M_{n+1}$ but not in M_n. Thus we have a strictly increasing sequence of submodules of M. This contradicts the fact that M is Noetherian.

Thus M_1 is the trivial module and ϕ must be injective. In this case ϕ must be a bijection, so that it is an automorphism.

3. (10pts) *Let M, N and P be R-modules over a ring R. Show that there is a natural isomorphism*:

$$\mathrm{Hom}_R(M \underset{R}{\otimes} N, P) \simeq \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)).$$

By the universal property of the tensor product, an element of $\mathrm{Hom}_R(M \underset{R}{\otimes} N, P)$ is the same as a bilinear map

$$M \times N \longrightarrow P.$$

If we fix $m \in M$ this gives us an R-linear map $N \longrightarrow P$, an element of $\mathrm{Hom}_R(N, P)$. Varying m gives us a function

$$M \longrightarrow \mathrm{Hom}_R(N, P),$$

which it is not hard to see is R-linear. Thus we get an element of $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$. It is straightforward to check that this assignment is R-linear.
Now suppose that we have an element of $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$. For every $m \in M$ we get an R-linear map $N \longrightarrow P$. This defines a function $M \times N \longrightarrow P$ which is bilinear, so that we get an element of $\mathrm{Hom}_R(M \underset{R}{\otimes} N, P)$. It is not hard to see that this is the inverse of the first assignment, so that we get an isomorphism:

$$\mathrm{Hom}_R(M \underset{R}{\otimes} N, P) \simeq \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)).$$

4. (10pts) *How many conjugacy classes of* 5×5 *matrices over* $\mathbb{Q}$ *with minimum polynomial* x^3 *are there?*

Two matrices are conjugate if and only if they have the same rational canonical form. So we just need to count the number of 5×5 matrices with minimal polynomial x^3 in rational canonical form.
To guarantee the minimal polynomial is x^3 we must have a block of the form

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

and no bigger blocks. There are then two possibilities:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

5. (15pts) (i) *Show that every finite subgroup of the multiplicative group of a field is cyclic.*

Let G be a finite subgroup of K^*, where K is a field. Then G is a finite abelian group, and so, by the Fundamental Theorem of finitely generated abelian groups, G is isomorphic to

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3} \times \cdots \times \mathbb{Z}_{m_r},$$

where $m_i | m_{i+1}$, for every $i \leq r - 1$. Thus the exponent e of G is equal to m_r and this is equal to the order of G if and only if G is cyclic. On the other hand, by definition of the exponent, every element of G is a root of

$$x^e - 1 \in K[x].$$

As this has at most e roots, it follows that $e \geq |G|$, so that G is indeed cyclic.

(ii) *Let $\mathbb{F}$ be a finite field with q elements. Show that $\mathbb{F}$ is the splitting field of the polynomial $x^q - x$.*

By (i), G the set of non-zero elements of $\mathbb{F}$, is cyclic of order $q - 1$. Thus the elements of G are precisely the roots of the polynomial

$$x^{q-1} - 1 \in \mathbb{F}_p[x].$$

But then the elements of L are precisely the q roots of

$$x^q - x.$$

In particular L is the splitting field of $x^q - x$.

6. (15pts) (i) *State a simple criterion for a finite field extension L/K to be normal.*

L/K is normal if and only if it is the splitting field of some polynomial $f(x) \in K[x]$.

(ii) *Which of the following fields extensions are normal?*
(a) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

Normal, as the splitting field of $(x^2 - 2)(x^2 - 3)$.

(b) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Not normal. $x^3 - 2$ has a root in L, but $x^3 - 2$ does not split in L. Indeed if $\alpha = \sqrt[3]{2}$, then the other roots are $\omega\alpha$ and $\omega^2\alpha$, and ω is not an element of $L \subset \mathbb{R}$.

7. (20pts) *(i) Let $f(x) \in K[x]$ be a polynomial and let L/K be a splitting field for $f(x)$.* Prove that $\alpha \in L/K$ is a repeated root of $f(x)$ if and only if α is a common root of $f(x)$ and $Df(x)$ (where Df denotes the formal derivative).

Suppose that α is a repeated root of $f(x)$. Then we may write

$$f(x) = (x - \alpha)^2 g(x),$$

where $g(x) \in L[x]$. Then

$$Df(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 Dg(x),$$

so that α is also a root of $Df(x)$.
Conversely suppose that α is a root of $f(x)$ and $Df(x)$. Then we may write

$$f(x) = (x - \alpha)g(x),$$

where $g(x) \in L[x]$. Then

$$Df(x) = g(x) + (x - \alpha)Dg(x).$$

Thus α is a root of $g(x)$. But then α is a repeated root of $g(x)$.

(ii) *Prove that every field extension in characteristic zero is separable.*

It suffices to prove that every irreducible polynomial $f(x)$ over a field of characteristic zero does not have a repeated root. Let $g(x)$ be the formal derivative of $f(x)$. Then $g(x)$ is not the zero polynomial, as the characteristic is zero. Let α be a root of $g(x)$ in some splitting field. Then the minimum polynomial $m(x)$ of α divides $g(x)$ and so it is of degree less than the degree of $f(x)$. As $f(x)$ is irreducible, $m(x)$ cannot divide $f(x)$ and so α cannot be a root of $f(x)$. Thus $f(x)$ and $g(x)$ do not have a common root and so $f(x)$ does not have a repeated root.

(iii) *Prove that every extension of finite fields is separable.*

Let $\mathbb{F}$ be a finite field. We proved that every element of $\mathbb{F}$ is a root of the polynomial $x^q - x$. But $D(x^q - x) = -1$, and so this polynomial has no repeated roots.

8. (15pts) (i) *Let L/K be a finite field extension. Carefully state a criterion for L/K be separable which involves $[L : K]$.*

L/K is separable if and only if the number of ring homorphisms of L/K into a normal closure N is at least $[L : K]$.

(ii) *Is every finite separable extension of a finite separable extension, separable?*

Yes. Let M/K and L/M be two finite separable extensions. Let N/L be a normal closure. Then the number of ring homorphisms $\pi\colon M \longrightarrow N$ is equal to $[M : K]$ as M/K is separable and for each such map π, the number of ring homorphisms $\psi\colon L \longrightarrow N$ extending π is equal to $[L : M]$, as L/M is separable. But then there at least

$$[L : K] = [L : M][M : K]$$

ring homorphisms $\pi\colon L \longrightarrow N$ over K.

(iii) *Is every finite normal extension of a finite normal extension, normal?*

No. Consider $K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt{2})$ and $L = \mathbb{Q}(\sqrt[4]{2})$. Then L/M and M/K are normal as they are quadratic. But $x^4 - 2$ is irreducible over $\mathbb{Q}$, by Eisenstein, has a root in L but does not split in L.

9. (25pts) *Find the indicated Galois groups. Carefully justify your answers.*
(i) $(x^2-2)(x^2-3)$ *over* $\mathbb{Q}$.

Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let $M = \mathbb{Q}(\sqrt{2})$. Now $x^2 - 2$ is irreducible by Eisenstein, applied with $p = 2$, so that $[M : K] = 2$. Similarly $[L : M] = 1$ or 2, depending on whether $x^2 - 3$ is reducible over M. But if it is reducible, then $L = M$ and $\sqrt{3} \in M$, which it is easy to check does not happen. Thus $[L : K] = 4$. It follows that the Galois group has order 4.
On the other hand, an element of the Galois group must send a root of $x^2 - 2$ to another root, and so it must send $\sqrt{2}$ to $\pm\sqrt{2}$. Similarly for $\sqrt{3}$. As there are at most 4 such maps, and the action of an element of the Galois group is determined by its action on the $\sqrt{2}$, $\sqrt{3}$, the result follows.

(ii) $x^{15} - 1$ *over* $\mathbb{Q}$.

Φ_{15} is irreducible over $\mathbb{Q}$ and so the Galois group is isomorphic to U_{15}. But $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. By inspection every element has order at most 4 and there is an element of order 4 (for example 2). So this group is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$.

(iii) $x^7 - 5$ *over the splitting field of* $x^7 - 1$ *over* $\mathbb{Q}$.

As 7 is prime, either $x^7 - 5$ is irreducible over K or it splits in K. Now $x^7 - 5$ is irreducible over $\mathbb{Q}$ by Eisenstein, and so the only way it could split in K, is if we adjoin a root, in which case $[K : \mathbb{Q}]$ would be divisible by 7. As it is not $x^7 - 5$ is irreducible over K. As $x^7 - 1$ splits in K, it follows that the Galois group is cyclic, of order 7.

(iv) $x^4 - 3$ *over* $\mathbb{F}_5$.

$\mathbb{Z}_4$.
As we are over a finite field, the Galois must be cyclic. We only need to check that $x^4 + 2$ is irreducible. If it had a linear factor, then we would have a root. But $a^4 = 1$, if $a \neq 0$, and so there are no roots.
Otherwise it factors as

$$x^4 + 2 = (x^2 + ax + b)(x^2 + cx + d).$$

Looking at the cubic term we have $a + c = 0$. Thus

$$x^4 + 2 = (x^2 + ax + b)(x^2 - ax + d).$$

Looking at the quadratic terms, we have $b + d = a^2$. Looking at the linear term we have $ab = ad$. If $a \neq 0$, then $b = d$, so that $b^2 = 2$. But 2 is not a square mod 5, impossible. Thus $a = 0$. But then $d = -b$ and $b^2 = 3$, again impossible.
Thus $x^4 + 2$ is irreducible. Let $\alpha \in L$ be a root. Then $K(\alpha)/K$ is normal, as it is an extension of finite fields and so $x^4 + 2$ splits in $K(\alpha)$. Thus $L = K(\alpha)$ and so L/K has degree four.

(v) $x^4 - 3$ over $\mathbb{Q}$.

D_4.
A splitting field is given by $L = \mathbb{Q}(\alpha, i)$ is a splitting field, where α is a root of $x^4 - 3$ and i is a square root of -1. Now $\mathbb{Q}(\alpha)/\mathbb{Q}$ has degree four, as $x^4 - 3$ is irreducible by Eisenstein. On the other hand i is not an element of $\mathbb{Q}(\alpha)$ as i is not real. Thus the degree of $L/\mathbb{Q}$ is eight.
Let $M = \mathbb{Q}(i)$. Then L/M has degree four. Thus $x^4 - 3$ is irreducible, and as $x^4 - 1$ splits in M, this is a cyclic extension of degree four (that is the Galois group is cyclic).
Let σ be the corresponding generator. Let τ be the automorphism, given as complex conjugation. Then $\sigma^4 = \tau^2 = 1$. It suffices to compute $\tau\sigma\tau$, which it is easy to see is σ^3 (compare their actions on α and i). But this is precisely a presentation for D_4.

10. (10pts) *State and prove the Fundamental Theorem of Algebra, stating carefully what you use to prove this result.*

Let $f(x) \in \mathbb{C}[x]$. Then $f(x)$ splits over $\mathbb{C}$.
It suffices to prove that there are no non-trivial finite extensions of $\mathbb{C}$. Let $L/\mathbb{C}$ a finite extension. Passing to a normal closure over $\mathbb{R}$, we may assume that $L/\mathbb{R}$ is Galois. Let G be the Galois group and let H by a Sylow 2-subgroup. Let M be the corresponding fixed field. Then $M/\mathbb{R}$ has odd degree. Let $\alpha \in M$. Then the minimum polynomial of α has odd degree. As every odd degree real polynomial has a root, it follows that $\alpha \in \mathbb{R}$, so that $M = \mathbb{R}$.
Thus we may assume that G has degree a power of two. Replacing G by a subgroup, we may assume that G is the Galois group of $L/\mathbb{C}$. Suppose that G is not trivia. As G is a 2-group, it has a subgroup of index two, call it H. Let M be the corresponding field. Then $M/\mathbb{C}$ has degree two. As every quadratic polynomial has a root (the quadratic formula), $M = \mathbb{C}$, a contradiction.

11. (10pts) *Find $\Phi_4(x)$, $\Phi_6(x)$ and $\Phi_{12}(x)$ in characteristic zero.*

$$x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x) = (x^2 - 1)(x^2 + 1).$$

Thus $\Phi_4(x) = x^2 + 1$.

$$x^6 - 1 = \Phi_1\Phi_2\Phi_3\Phi_6 = (x^3 - 1)(x^3 + 1) = (x^3 - 1)(x + 1)(x^2 - x + 1)$$

Thus $\Phi_6(x) = x^2 - x + 1$.

$$x^{12} - 1 = \Phi_1\Phi_2\Phi_3\Phi_4\Phi_6\Phi_{12} = (x^6 - 1)(x^6 + 1).$$

So

$$x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1) = \Phi_2\Phi_{12}.$$

Thus

$$\Phi_{12} = x^4 - x^2 + 1.$$

Bonus Challenge Problems

12. (10pts) *If R is Noetherian then prove that the power series ring $R[\![x]\!]$ is Noetherian. (You may assume that every finitely generated module over a Noetherian ring is Noetherian).*

13. (10pts) *Show that any set of characters is linearly independent.*

14. (10pts) Let G be a collection of automorphisms acting on a field L and let $K = L^G$ be the fixed field. Show that $[L : K] \geq |G|$.

15. (10pts) *Prove that* $\Phi_n(x)$ *is irreducible over* $\mathbb{Q}$.