MATH 220C: FINAL EXAMINATION
JUNE 4, 2018
DANIEL HALMRAST

Problem 1

Let K/k be a finite extension of fields, with k infinite.

Part a. Define what it means for K/k to be separable.

Definition. *Let L be an algebraic closure of K. We say that K/k is separable if the number of k-embeddings of K into L is equal to the degree $[K : k]$ of the extension.*

Part b. Suppose K/k is separable. Prove that K/k is simple, i.e. that there exists $\alpha \in K$ such that $K = k(\alpha)$.

Proof. Since K/k is a finite separable extension, it is built up from simple extensions. That is, there is a tower

$$F_0 = k \subset F_1 \subset \cdots \subset F_n = K$$

with $F_{i+1} = F_i(\alpha_i)$ where the extension $F_i(\alpha_i)$ is separable. We will prove that a separable extension of the form $k(\alpha_1, \alpha_2)/k$ is simple, and use induction to show that K/k is simple.

So, let $k(\alpha_1, \alpha_2)/k$ be a separable extension, with L an algebraic closure of k. In particular, we know that there are $n = [k(\alpha_1, \alpha_2) : k]$ distinct k-embeddings of $k(\alpha_1, \alpha_2)$ into L. Denote these embeddings as σ_i for $1 \leq i \leq n$.

Now, define a polynomial f as

$$f(x) = \prod_{i \neq j} ((\sigma_i(\alpha_1) - \sigma_j(\alpha_1)) + (\sigma_i(\alpha_2) - \sigma_j(\alpha_2))x)$$

Since each σ_i is a distinct k-embedding of $k(\alpha_1, \alpha_2)$, it follows that at least one of

$$\sigma_i(\alpha_1) - \sigma_j(\alpha_1)$$
$$\sigma_i(\alpha_2) - \sigma_j(\alpha_2)$$

is nonzero for each $i \neq j$. Thus, f is not the zero polynomial. So, let a be such that $f(a) \neq 0$. Then, it follows that each linear term of $f(a)$ is nonzero as well. That is, for every $i \neq j$,

$$((\sigma_i(\alpha_1) - \sigma_j(\alpha_1)) + (\sigma_i(\alpha_2) - \sigma_j(\alpha_2))a) \neq 0$$

or

$$\sigma_i(\alpha_1) + \sigma_i(\alpha_2)a \neq \sigma_j(\alpha_1) + \sigma_j(\alpha_2)a$$

which implies (by linearity of σ) that

$$\sigma_i(\alpha_1 + a\alpha_2) \neq \sigma_j(\alpha_1 + a\alpha_2)$$

for all $i \neq j$. Thus, each σ_i sends $\alpha_1 + a\alpha_2$ to a different element of $k(\alpha_1, \alpha_2)$, and so the separability degree of $k(\alpha_1 + a\alpha_2)$ (the number of distinct k-embeddings of $k(\alpha_1 + a\alpha_2)$ into an algebraic closure L) is

$$[k(\alpha_1 + a\alpha_2) : k]_s \geq n$$

and since $\alpha_1 + a\alpha_2 \in k(\alpha_1, \alpha_2)$, the extension $k(\alpha_1 + a\alpha_2)$ is separable. Thus the separability degree equals the degree of the extension. However, since $k(\alpha_1 + a\alpha_2) \subset k(\alpha_1, \alpha_2)$, we know that

$$[k(\alpha_1 + a\alpha_2) : k] \leq [k(\alpha_1, \alpha_2) : k] = n$$

and thus $[k(\alpha_1 + a\alpha_2) : k] = n$. Therefore, the extension

$$[k(\alpha_1, \alpha_2) : k(\alpha_1 + a\alpha_2)] = 1$$

and so $k(\alpha_1, \alpha_2) = k(\alpha_1 + a\alpha_2)$ and $k(\alpha_1, \alpha_2)$ is indeed simple.

Finally, we argue by induction that every finite separable extension is simple. Let F_i be as defined earlier in the proof. We will induct on the length of the tower $i + 1$. The base case for $i = 1$ implies that $K = k(\alpha)$ which is already a simple extension.

So, suppose K has a separable simple tower F_i of length $j + 1$, and assume that every separable extension with a separable simple tower F_i of length j is simple. Now,

$$K = F_j(\alpha_j)$$

By the inductive hypothesis, F_j is simple. Thus, $F_j = k(\beta)$ for some β. Then, $K = k(\alpha_j, \beta)$ where $k(\alpha_j, \beta)$ is a separable extension. By the earlier result of this proof, $k(\alpha_j, \beta)$ is in fact a simple extension, and so $K = k(\alpha_j, \beta)$ is a simple extension as well, as desired. $\square$

Part c. Define what it means for K/k to be normal.

Definition. *A finite extension K/k is called normal if K is the splitting field for some polynomial in $k[X]$.*

Part d. Suppose K/k is normal, and let L/K be a finite normal extension. Is the extension L/k necessarily normal?

Proof. We illustrate with a counterexample that L/k is not necessarily normal. Consider the tower $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. Now, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal, since $\mathbb{Q}(\sqrt{2})$ is the splitting field for $f(X) = X^2 - 2$. Furthermore, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ is normal, as it is the splitting field for $g(X) = X^2 - \sqrt{2}$.

However, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal. This is clear, since the minimal polynomial for $\sqrt[4]{2}$ over $\mathbb{Q}$ is $h(X) = X^4 - 2$, which has complex roots. Thus, $\mathbb{Q}(\sqrt[4]{2})$ is not the splitting field for any polynomial over $\mathbb{Q}$, and is not normal over $\mathbb{Q}$ as desired. $\square$

Problem 2

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots in $\mathbb{C}$ of the polynomial

$$f(x) = x^4 + 4x + 2$$

and let $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$.

Part a. Determine the number of real and non-real roots of $f(x)$.

Proof. Consider the derivative

$$f'(x) = 4x^3 + 4$$

which is zero precisely when $x^3+1 = 0$. This has one root at -1, and dividing out the factor $(x+1)$ splits $f'(x)$ into

$$f'(x) = 4(x+1)(x^2 - x + 1)$$

and so the other two roots of $f'(x)$ are

$$\alpha_{\pm} = \frac{1 \pm \sqrt{1-4}}{2}$$

which are both complex. Thus, there is only one real root of $f'(x)$ at $x = -1$. We calculate the second derivative

$$f''(x) = 12x^2$$

which is always non-negative, and positive for $x \neq 0$. Thus, $f(x)$ is always concave up. Finally, we note that

$$f(-1) = 1 - 4 + 2 = -1$$

is less than zero, but since f is everywhere concave up, f is increasing after $x = -1$ and decreasing before $x = -1$, and so there are exactly two real roots of f, one before $x = -1$ and one after $x = -1$. The other two roots of f must then be complex. $\square$

Part b. Explain why the number $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$ is the root of a cubic polynomial $g(x)$ over $\mathbb{Q}$. Determine the number of real and non-real roots of g.

Proof. We define all three roots of a cubic polynomial as

$$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$$
$$\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$$
$$\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$$

Now, we will establish that the monic polynomial with these three roots is in fact a polynomial over $\mathbb{Q}$. We calculate

$$\begin{aligned} g(x) &= \prod_{i=1}^{3}(x - \beta_i) \\ &= x^3 - \beta_1 x^2 - \beta_2 x^2 - \beta_3 x^2 + \beta_1\beta_2 x + \beta_1\beta_3 x + \beta_2\beta_3 x - \beta_1\beta_2\beta_3 \\ &= x^3 - (\beta_1 + \beta_2 + \beta_3)x^2 + (\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3)x - \beta_1\beta_2\beta_3 \end{aligned}$$

So, all we have to show is that

$$a_2 = -(\beta_1 + \beta_2 + \beta_3)$$
$$a_3 = \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3$$
$$a_4 = -\beta_1\beta_2\beta_3$$

are in $\mathbb{Q}$. We will do this by showing that a_2, a_3, a_4 are all fixed by the action of the Galois group $G(K/\mathbb{Q})$.

Now, observe that any permutation of the roots α_i will also permute the set $\{\beta_i\}$. This follows from the fact that $\beta_1, \beta_2, \beta_3$ represent the three ways to partition the roots into two disjoint sets. Thus, any permutation of the roots α_i will send one partition β_i to another partition β_j. For σ a permutation of the roots, we will denote $\beta_{\sigma(i)}$ to be $\sigma(\beta_i)$ the result of permuting the roots by σ. That is,

$$\beta_{\sigma(1)} = \sigma(\alpha_1)\sigma(\alpha_2) + \sigma(\alpha_3)\sigma(\alpha_4)$$

and so on.

Observe that

$$\sigma(a_2) = -(\beta_{\sigma(1)} + \beta_{\sigma(2)} + \beta_{\sigma(3)})$$

which, by rearranging, is just

$$\sigma(a_2) = -(\beta_1 + \beta_2 + \beta_3) = a_2$$

and so a_2 is fixed by each $\sigma \in G(K/\mathbb{Q})$.

We observe similarly that a_3 and a_4 are fixed under permutations of $\{\beta_i\}$, and are thus also fixed for each $\sigma \in G(K/\mathbb{Q})$. Therefore, each coefficient is in the fixed field of $G(K/\mathbb{Q})$, and thus are all in $\mathbb{Q}$ as desired.

So, $g(x)$ is a polynomial over $\mathbb{Q}$ with β_1 as a root.

Finally, we show that $g(x)$ has one real root and two complex roots. To see this, recall that $g(x)$ has β_i as its roots. Now, without loss of generality, let $\alpha_2 = \overline{\alpha_1}$ be the two complex roots of f. Then, we observe that

$$\begin{aligned}\beta_1 &= \alpha_1\overline{\alpha_1} + \alpha_3\alpha_4 \\ &= \|\alpha_1\|^2 + \alpha_3\alpha_4\end{aligned}$$

is the sum of real numbers, and is therefore real. However, writing α_1 as $a + bi$, we see that

$$\begin{aligned}\beta_2 &= \alpha_1\alpha_3 + \overline{\alpha_1}\alpha_4 \\ &= \alpha_3 a + \alpha_3 bi + \alpha_4 a - \alpha_4 bi \\ &= (\alpha_3 + \alpha_4)a + (\alpha_3 - \alpha_4)bi\end{aligned}$$

and since $\alpha_3 \neq \alpha_4$, this number is non-real. Finally, this implies that $\overline{\beta_2} = \beta_3$ is the other complex root, and so g has one real root, and two complex roots, as desired. $\square$

Part c. Show that K contains a splitting field L for $g(x)$ over $\mathbb{Q}$.

Proof. Recall from the previous part that the roots of $g(x)$ are

$$\begin{aligned}\beta_1 &= \alpha_1\alpha_2 + \alpha_3\alpha_4 \\ \beta_2 &= \alpha_1\alpha_3 + \alpha_2\alpha_4 \\ \beta_3 &= \alpha_1\alpha_4 + \alpha_2\alpha_3\end{aligned}$$

which are all in K. Thus, $\mathbb{Q}(\beta_1, \beta_2, \beta_3) \subset K$, and since $L = \mathbb{Q}(\beta_1, \beta_2, \beta_3)$ is the splitting field for $g(x)$ over $\mathbb{Q}$, $L \subset K$ as desired. $\square$

Part d. Show that the Galois group of K over L is a subgroup of the Klein four group.

Proof. The Galois group of K over L must fix L, so in particular it must fix β_1. We also know it is a subgroup of the Galois group of K over $\mathbb{Q}$, and thus must be a permutation of the roots α_i. However, the only permutations that fix β_1 are (in cycle notation) $\{e, (12), (34), (12)(34)\}$ which is the Klein four group. Thus, the Galois group of K over L must be a subgroup of the Klein four group as desired. $\square$

Problem 3

Suppose G is a finite group, and K is an algebraically closed field of characteristic zero.

Part a. State Schur's lemma concerning irreducible KG-modules.

Lemma. *Suppose U, W are irreducible KG-modules, and $f : U \to W$ is a KG-module homomorphism. Then, f is either an isomorphism or the zero map. Furthermore, if $g : U \to U$ is a KG-module homomorphism, then g is a multiple of the identity.*

Part b. Suppose that G is abelian. Show that each irreducible KG-module has dimension 1 as a K-vector space.

Proof. Since G is abelian, each element is its own conjugacy class. Thus, there are exactly $|G|$ conjugacy classes in G. This implies that there are exactly $|G|$ irreducible representations of G. Now, the first column of the character table for G shows the dimensions of the irreducible representations, and the normality condition on the first column of the character table says that the sum of the squares of the dimensions of the irreducible representations have to equal the order of the group. Now, since there are exactly $|G|$ irreducible representations, each with dimension ≥ 1, they must all have dimension 1 to square-sum to $|G|$. Thus, the dimension of each irreducible representation is 1, as desired. □

Part c. Suppose G is abelian, and let χ be any irreducible K-valued character of G. Evaluate $\sum_{g \in G} \chi(g)$.

Proof. Suppose first that χ is the trivial character. Then, $\chi(g) = 1$ for all $g \in G$, and

$$\sum_{g \in G} \chi(g) = |G|$$

So, assume χ is not the trivial character. We know from the orthogonality relation on the rows of the character table of G that

$$|G|\langle \chi, \chi^{(1)} \rangle = 0$$

we evaluate the left hand side to

$$\begin{aligned} |G|\langle \chi, \chi^{(1)} \rangle &= \sum_{g \in G} \chi(g)\overline{\chi^{(1)}(g)} \\ &= \sum_{g \in G} \chi(g)(1) \\ &= \sum_{g \in G} \chi(g) \end{aligned}$$

and so $\sum_{g \in G} \chi(g) = 0$. $\square$

Problem 4

Let G denote the permutation group S_4 on four letters.

Part a. Calculate the size of each conjugacy class of G, and write down a representative of each conjugacy class.

Proof. We do so by brute-force calculation. The results are tabulated below. Observe that

$$\begin{aligned}S_4 = \{&(1), (12), (13), (14), (23), (24), (34),\\ &(123), (132), (124), (142), (134), (143), (234), (243),\\ &(12)(34), (13)(24), (14)(23),\\ &(1234), (1432), (1243), (1342), (1324), (1423)\}\end{aligned}$$

and so we compute the conjugacy classes:

Conjugacy Class	**Size**
$\{(1)\}$	1
$\{(12), (13), (14), (23), (24), (34)\}$	6
$\{(123), (132), (124), (142), (134), (143), (234), (243)\}$	8
$\{(12)(34), (13)(24), (14)(23)\}$	3
$\{(1234), (1432), (1243), (1342), (1324), (1423)\}$	6

We obtained this table by observing that conjugation in S_4 amounts to a relabeling of the symbols, and thus cannot change the cycle type. Furthermore, S_4 acts 4-transitively on the set of four letters, and so for any two elements with the same cycle type, there is a relabeling which takes one to the other. That is, suppose $(abcd)$ and $(efgh)$ are of the same cycle type. Then, there is an element σ of S_4 which takes (a, b, c, d) to

$(e, f, g, h) = (\sigma(a), \sigma(b), \sigma(c), \sigma(d))$. Thus,

$$\sigma(abcd)\sigma^{-1} = (\sigma(a)\sigma(b)\sigma(c)\sigma(d)) = (efgh)$$

and similarly for other cycle types.

From here on out, the conjugacy classes will be represented by

Conjugacy Class	**Size**
(1)	1
(12)	6
(123)	8
(12)(34)	3
(1234)	6

$\square$

Part b. Let V be a $\mathbb{C}$-vector space with basis $\{e_1, e_2, e_3, e_4\}$. Suppose that G acts on V by permuting the elements of this basis in the obvious way, and let χ_V be the corresponding character of V. Calculate the value of χ_V on each conjugacy class of V, and determine whether or not χ_V is irreducible.

Proof. Note that the matrix representation of an element $g \in G$ acting on V in the basis $\{e_i\}$ is a permutation matrix, whose trace is just the number of basis vectors fixed by g. This follows from the fact that a permutation matrix has columns of all zeros except one 1, and if column j has a 1 in the jth row (on the diagonal), then the matrix sends the jth basis vector to itself. Thus, the trace (the sum of the diagonal elements) is just the number of basis vectors fixed by g.

We calculate the value of χ_V on each conjugacy class directly

S_4	(1)	(12)	(123)	(12)(34)	(1234)
$\lvert c_i \rvert$	1	6	8	3	6
χ_V	4	2	1	0	0

Now, if χ_V were irreducible, we must have that

$$\langle \chi_V, \chi_V \rangle = 1$$

so, we calculate

$$\begin{aligned}
|G|\langle \chi_V, \chi_V \rangle &= \sum_{g \in G} \chi_V(g)\overline{\chi_v(g)} \\
&= \sum_{i=1}^{5} |c_i|\chi_V(g_i)\overline{\chi_V(g_i)} && g_i \in c_i \\
&= 1(4)(4) + 6(2)(2) + 8(1)(1) + 3(0)(0) + 6(0)(0) \\
&= 16 + 24 + 8 = 48
\end{aligned}$$

since $|G| = 4! = 24$, it follows that χ_V is not irreducible. □

Part c. Let $\chi^{(1)}$ denote the trivial character. By considering $\chi_V - \chi^{(1)}$, show that G has an irreducible character ψ of degree three.

Proof. Let $\psi = \chi_V - \chi^{(1)}$. First, we calculate the values of ψ on the conjugacy classes.

S_4	(1)	(12)	(123)	(12)(34)	(1234)
$\lvert c_i \rvert$	1	6	8	3	6
$\chi^{(1)}$	1	1	1	1	1
χ_V	4	2	1	0	0
ψ	3	1	0	-1	-1

Now, ψ is irreducible if and only if $\langle \psi, \psi \rangle = 1$. So, we calculate

$$\begin{aligned}
|G|\langle \psi, \psi \rangle &= \sum_{i=1}^{5} |c_i| \psi(g_i)\overline{\psi(g_i)} \\
&= 1(3)(3) + 6(1)(1) + 8(0)(0) + 3(-1)(-1) + 6(-1)(-1) \\
&= 9 + 6 + 3 + 6 = 24 = |G|
\end{aligned}$$

and so $\langle \psi, \psi \rangle = 1$ and ψ is irreducible.

Furthermore, since $\psi(1) = 3$, ψ has degree three, as desired. □

Part d. Determine the degrees of all the irreducible characters of G.

Proof. By the normality condition on the first column of the character table for G, the sum of the squares of the degrees of the irreducible characters of G must be equal to $|G|$. Furthermore, since there are 5 conjugacy classes in G, there are 5 irreducible characters on G. Let n_i for $1 \leq i \leq 5$ be the degrees of the characters.

We know two characters already. The trivial character $\chi^{(1)}$ has degree 1, so $n_1 = 1$. The character ψ found in the last part (which we will call the second character) has degree 3, so $n_2 = 3$. Thus,

$$|G| = 24 = n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 1 + 3^2 + n_3^2 + n_4^2 + n_5^2$$

and so

$$n_3^2 + n_4^2 + n_5^2 = 24 - 9 - 1 = 14$$

The only integer solution to this is (up to relabeling)

$$n_3 = 3$$

$$n_4 = 2$$

$$n_5 = 1$$

and so the degrees of all the irreducible characters of G are

$$n_1 = 1$$

$$n_2 = 3$$

$$n_3 = 3$$

$$n_4 = 2$$

$$n_5 = 1$$

$\square$