NORTHWESTERN
UNIVERSITY

Name: _____

Id #:

Math 331-3 Final

Spring Quarter 2015

Tuesday, June 9, 2015

Name:

Instructions:
Show *all* your work on these sheets. Feel free to use the opposite side. Make sure that your final answer is clearly indicated. This test has six problems. No calculators, books, notes, etc. are allowed. Good luck!

Prob.	Possible points	Score
1	20	
2	10	
3	15	
4	15	
5	35	
6	10	
TOTAL	105	

Question 1. (20 *points*). *Provide an example of a finite extension F/E with each of the following indicated properties (for this question only, no justification is required):*

1. *A finite extension F/E of fields which is not Galois.*

   Multiple anwers, including:

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

2. *An extension F/E of degree* 100.

   Multiple anwers, including:

   $$\mathbb{Q}(\sqrt[100]{2})/\mathbb{Q}, \quad \mathbf{F}_{p^{100}}/\mathbf{F}_p, \quad \mathbb{Q}(\zeta_{101})/\mathbb{Q}.$$

3. A Galois extension F/E with $\mathrm{Gal}(F/E) = \mathbb{Z}/6\mathbb{Z}$.

Multiple anwers, including:

$$\mathbf{F}_{p^6}/\mathbf{F}_p, \quad \mathbb{Q}(\zeta_7)/\mathbb{Q}.$$

4. A non-separable extension F/E.

Multiple anwers, including:

$$\mathbf{F}_p(t^{1/p})/\mathbf{F}_p(t).$$

Question 2. (10 *points*). *Determine the number of irreducible polynomials over* $\mathbf{F}_7$ *of degree* 3.

The three roots of a degree 3 irreducible polynomial lie in $\mathbf{F}_{7^3}$ and not in $\mathbf{F}_7$. Conversely, any element in $\mathbf{F}_{7^3}$ and not in $\mathbf{F}_7$ is the root of an irreducible degree three polynomial. Thus there is a 3:1 map from elements of $\mathbf{F}_{7^3}$ minus $\mathbf{F}_7$ to irreducible degree three polynomials. Hence the number of such polynomials is

$$\frac{|\mathbf{F}_{7^3}| - |\mathbf{F}_7|}{3} = \frac{343 - 7}{3} = 112.$$

Question 3. (15 *points*). *Suppose that $f(x)$ is an irreducible separable polynomial over a field K of characteristic zero. Let α and β be two distinct roots of $f(x)$. Prove that*

$$\beta \neq \alpha + 1.$$

Argument I: Let K be the splitting field of $f(x)$. Since the Galois group acts transitively on the roots, there must exist an automorphism σ with $\sigma(\alpha) = \beta = \alpha+1$. By induction, we see that $\sigma^n(\alpha) = \alpha + n$, which means that $\alpha + n$ is a root of $f(x)$ for all integers n. Since the characteristic is zero, these roots are all distinct, which implies that $f(x)$ has infinitely many roots, a contradiction.

Argument II: We see that $\alpha = \beta - 1$ is a root of $f(x + 1)$ and of $f(x)$, and hence also of

$$f(x + 1) - f(x).$$

The degree of this polynomial is less than the degree of $f(x)$ and has α as a root. Yet $f(x)$ is the minimal polynomial of $f(x)$. It follows that $f(x + 1) - f(x) = 0$, or that $f(x + 1) = f(x)$. This implies that $f(x + n) = f(x)$ and thus that $\beta - n$ is a root of this polynomial for all integers n. Since the characteristic is zero, these roots are all distinct, which implies that $f(x)$ has infinitely many roots, a contradiction.

Remark: Note that the result is false in finite characteristic, as can be seen from the polynomials $f(x) = x^p - x - 1$ over $\mathbf{F}_p$.

Question 4. (15 *points*). *Let* $f(x) = x^{2015} + 3x^5 + 3 \in \mathbb{Q}[x]$. *Prove that the splitting field* L *of* $f(x)$ *is not* S_{2015}. *Hint: show that* L *contains a Galois subfield* K *which is incompatible with* $\mathrm{Gal}(L/\mathbb{Q}) = S_{2015}$.

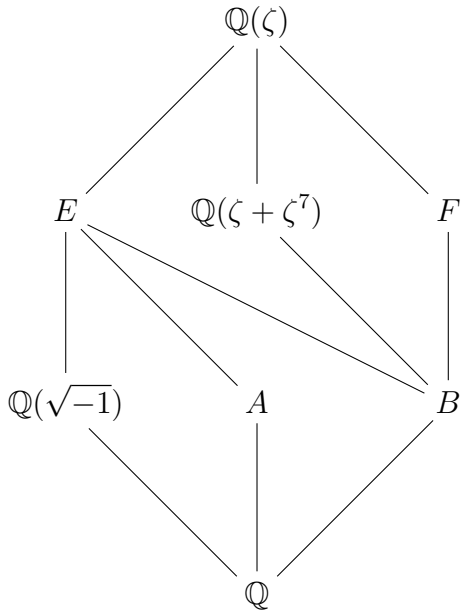
Argument I: If α is a root of $f(x)$, then α^5 is a root of

$$y^{403} + 3y + 3 = 0.$$

This is irreducible, by Eisenstein's criterion. Let K be the splitting field of this polynomial. Clearly $\mathrm{Gal}(K/\mathbb{Q})$ is a subgroup of S_{403} of order divisible by 403. By Galois theory, $\mathrm{Gal}(K/\mathbb{Q})$ is a quotient of $\mathrm{Gal}(L/\mathbb{Q})$. The only proper quotient of S_{2015}, however, is $S_{2015}/A_{2015} = \mathbb{Z}/2\mathbb{Z}$.

Argument II: If α is a root of $f(x)$, then so is $\zeta\alpha$, where $\zeta^5 = 1$ is a primitive 5th root of unity. Hence L contains $K = \mathbb{Q}(\zeta_5)$, and $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$. By Galois theory, $\mathrm{Gal}(K/\mathbb{Q})$ is a quotient of $\mathrm{Gal}(L/\mathbb{Q})$. However, the group $\mathbb{Z}/4\mathbb{Z}$ is not a quotient of S_{2015}.

Question 5. (35 *points*). *Let $\zeta = \zeta_{16}$ be a primitive 16th root of unity. You may assume that $(\mathbb{Z}/16\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, where the isomorphism sends $[a]$ in $(\mathbb{Z}/16\mathbb{Z})^\times$ to the automorphism $\sigma_a : \zeta \to \zeta^a$. You may also assume that the minimal polynomial of ζ is $\zeta^8 + 1 = 0$. Consider the following diagram of subfields, where the given lines indicate an extension of degree 2:*



You may assume that every inclusion of fields of degree two is indicated on this diagram.

1. *Give an explicit isomorphism from $(\mathbb{Z}/16\mathbb{Z})^\times$ to $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.*

$$5 \mapsto (1,0) \in (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}), \qquad 7 \mapsto (0,1) \in (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

2. *Determine* $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta+\zeta^7))$ *as a subgroup of* $(\mathbb{Z}/16\mathbb{Z})^\times$.

   We have $\sigma_7(\zeta+\zeta^7) = \zeta^7+\zeta^{49} = \zeta^7+\zeta$. Hence the Galois group contains σ_7. By assumption, the extension has degree two, and thus the Galois group has order two, and is hence $\langle\sigma_7\rangle$.

3. *Determine* $\mathrm{Gal}(\mathbb{Q}(\zeta+\zeta^7)/\mathbb{Q})$ *as an abstract group, either from the above calculation, or from the diagram.*

   By Galois theory, we need to compute the quotient $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ by the group $\mathrm{Gal}(\mathbb{Q}(\zeta+\zeta^7)/\mathbb{Q})$.

   Argument I : From the previous two questions this quotient is

   $$G/\langle\sigma_7\rangle = (\mathbb{Z}/4\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})/(0,1) = (\mathbb{Z}/4\mathbb{Z}).$$

   Argument II: From the diagram, $\mathrm{Gal}(\mathbb{Q}(\zeta+\zeta^7)/\mathbb{Q})$ has order four, and (by the main theorem of Galois theory) has a unique subgroup of index two. The only such group is $\mathbb{Z}/4\mathbb{Z}$.

4. *Determine* $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta^2))$ *as a subgroup of* $(\mathbb{Z}/16\mathbb{Z})^\times$.

   We have $\sigma_9(\zeta^2) = \zeta^{18} = \zeta^2$. Hence the Galois group contains σ_9. By assumption, the extension has degree two, and thus the Galois group has order two, and is hence $\langle\sigma_9\rangle$.

5. *Determine* $\mathrm{Gal}(\mathbb{Q}(\zeta^2)/\mathbb{Q})$ *as an abstract group, either from the above calculation, or from the diagram.*

   By Galois theory, we need to compute the quotient $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ by the group $\mathrm{Gal}(\mathbb{Q}(\zeta^2)/\mathbb{Q})$. Note that $\sigma_5^2 = \sigma_{25} = \sigma_9$

   Argument I : From the previous two questions this quotient is

   $$G/\langle\sigma_9\rangle = (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})/(2,0) = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}).$$

   Argument II: From the diagram, $\mathrm{Gal}(\mathbb{Q}(\zeta^2)/\mathbb{Q})$ has order four, and (by the main theorem of Galois theory) has three subgroups of index two. The only such group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

6. *Prove that* $E = \mathbb{Q}(\zeta^2)$ *and* $F = \mathbb{Q}(\zeta + \zeta^{-1})$.

Note that $\mathbb{Q}(\zeta^2)$ contains ζ^4 which is a root of $x^2 + 1 = 0$, and thus contains $\mathbb{Q}(\sqrt{-1})$. From the diagram, we deduce that $\mathbb{Q}(\zeta^2) = E$. The field F is fixed by σ_{-1}, and $\mathbb{Q}(\zeta)/F$ has degree at most two, so it gives the third index two field.

7. *Prove that* $B = \mathbb{Q}(\sqrt{2})$ *and deduce that* $A = \mathbb{Q}(\sqrt{-2})$. *Hint: what is* $\zeta^2 + \zeta^{-2}$*?*

If $\alpha = \zeta^2 + \zeta^{-2}$, then $\alpha^2 = \zeta^4 + \zeta^{-4} + 2$. Yet $\zeta^4 = \pm\sqrt{-1}$, so $\zeta^4 + \zeta^{-4} = 0$, and $\alpha^2 = 2$. Thus F contains $\mathbb{Q}(\sqrt{2})$, and so $B = \mathbb{Q}(\sqrt{2})$. It follows that E contains $\mathbb{Q}(\sqrt{-1}, \sqrt{2})$, and so must equal this field. The other quadratic subfield B of the biquadratic field E is hence $\mathbb{Q}(\sqrt{-2})$.

Question 6. *(10 points) Let $f(x)$ be an irreducible polynomial of degree n over $\mathbb{Q}$. Suppose that $f(x)$ remains irreducible over any extension $K/\mathbb{Q}$ of odd degree. Prove that n is a power of 2.*

Let L be the splitting field of $f(x)$, and let $G = \mathrm{Gal}(L/\mathbb{Q})$. Let P be a 2-Sylow subgroup of G, and let $K = L^P$. By the main theorem of Galois theory, $[L : K] = |P|$, and thus $K/\mathbb{Q}$ has odd degree. Hence $f(x)$ is irreducible over K with splitting field L. Let α be a root of $f(x)$. The irreducibility assumption of $f(x)$ over K implies that $[K(\alpha) : K] = n$. Yet certainly $K(\alpha) \subset L$. Hence

$$|P| = [L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K(\alpha)] \cdot n.$$

It follows that n divides the order of P, which is a power of two. Thus n is a power of 2.