Instructor: Leo Goldmakher

NAME: ______________________________

Williams College
Department of Mathematics and Statistics

MATH 394 : GALOIS THEORY

Problem Set 10 – due Thursday, May 4th

INSTRUCTIONS:
This assignment must be turned in to my mailbox (on the right as you enter Bascom) by **4pm** sharp. Assignments may be submitted later than this by email to Alyssa, but no later than 4pm on Friday; in this case, the grade will be reduced by 5%.
Assignments submitted later than Friday at 4pm will not be graded.

Please print and attach this page as the first page of your submitted problem set.

PROBLEM	GRADE
10.1	
10.2	
10.3	
10.4	
10.5	
Total	

Please read the following statement and sign below:

I understand that I am not allowed to use the internet to assist with this assignment. I also understand that I must write down the final version of my assignment in isolation from any other person. I pledge to abide by the Williams honor code.

SIGNATURE:______________________________

Problem Set 10

10.1 Given sets A, B and functions $f : A \to B$ and $g : B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$.

(a) Suppose B is finite. Prove that A must be finite, and that f and g are both bijections.

(b) Does (a) still hold if A and B are infinite? Prove / disprove.

10.2 Decide (with proof!) whether or not each of the following is separable.

(a) $x^4 + 4x^3 + 3x^2 + x + 2$ over $\mathbb{F}_7$

(b) $x^n - 1$ over a given field F.

10.3 The goal of this problem is to prove
The Fundamental Lemma. Given L/K a finite Galois extension and $\alpha \in L$. Then

$$m_\alpha(x) = \prod_{\beta \in A} (x - \beta),$$

where $m_\alpha \in K[x]$ is the minimal polynomial of α over K and $A := \{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\}$ is the set of all Galois conjugates of α.

(a) Suppose $f, g \in K[x]$, and let F be a splitting field of g over K. Prove that $f \mid g$ over $K[x]$ iff $f \mid g$ over $F[x]$. [*Hint: use problem* ***9.5***.]

(b) Prove the Fundamental Lemma. [*Hint: Set* $f_\alpha(x) := \prod_{\beta \in A} (x - \beta)$*, and prove that* $f_\alpha \mid m_\alpha$ *and* $m_\alpha \mid f_\alpha$*.*]

10.4 Given L/K a finite Galois extension, let F be an intermediate field corresponding to a group H under the Galois correspondence. Suppose F/K is Galois. Prove that the map $\varphi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ defined by $\sigma \mapsto \sigma\big|_F$ is a surjection. (This completes our proof from class that $\mathrm{Gal}(F/K) \simeq G/H$.)

10.5 Given L/K a finite Galois extension.

(a) Prove that α is a primitive element of L/K iff all Galois conjugates of α are distinct.

(b) Is $i + \sqrt[4]{2}$ a primitive element of $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$? Prove or disprove.

(c) Is $\sqrt[4]{2} + i\sqrt[4]{2}$ a primitive element of $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$? Prove or disprove.

10.* Bonus problem: this may be submitted any time by Friday, May 11th; your solution must be in LaTeX. A correct and complete solution will earn you 2 percentage points added to your overall course grade. Feel free to look up group actions in any textbook, but *not online.* Our goal is to prove
Theorem (Sylow, 1872). If G is a group and $p^k \,\Big|\, |G|$, then G has a subgroup of order p^k.

(a) Given a finite group G and a subgroup $H \leq G$, verify that H acts on G/H by left multiplication (i.e. show that this is a well-defined group action.)

(b) Given H acting on G/H by left multiplication as above (with G finite), consider the set of fixed points of this action:

$$\mathcal{F} := \{[x] \in G/H : h \cdot [x] = [x] \text{ for every } h \in H\}.$$

Prove that $\mathcal{F} = N(H)/H$, where $N(H)$ is the *normalizer* of H. (The normalizer of H is the largest subgroup of G in which H is normal: $N(H) = \{g \in G : H = gHg^{-1}\}$.) Deduce that $\mathcal{F}$ is a group.

(c) Let $G, H, \mathcal{F}$ be as above. Prove that if $|H| = p^n$ for some $n \geq 1$, then $|G/H| \equiv |\mathcal{F}| \pmod{p}$.

(d) Suppose G is a group with $p^k \,\Big|\, |G|$, and that $H \leq G$ has order p^{k-1}. Prove the existence of an intermediate subgroup $H \leq K \leq G$ such that $[K : H] = p$. [*Hint: We may assume* $k > 1$ *(why?). Define the set of fixed points* $\mathcal{F}$ *as above, and consider the natural projection map* $\pi : N(H) \twoheadrightarrow \mathcal{F}$*. Show that there exists a subgroup* $H' \leq \mathcal{F}$ *of order* p*. What can you say about the pullback* $\pi^{-1}(H')$*?*]

(e) Prove Sylow's theorem (stated in the introduction to this problem).