Instructor: Leo Goldmakher

NAME: _____

Williams College
Department of Mathematics and Statistics

MATH 394 : GALOIS THEORY

Problem Set 3 – due Thursday, February 22nd

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**
3.1	
3.2	
3.3	
3.4	
3.5	
3.6	
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 3

3.1 (The Return of Abstract Algebra: This Time, it's Ring Theory!) This problem is a review of the basic concepts from ring theory – for the definitions, please see the supplementary notes (posted on the website).

(a) Give an example of a noncommutative ring.

(b) Suppose S is a subring of the ring R. Prove that $S^\times \leq R^\times$. [*In applications of ring theory (e.g. to algebraic number theory) this is a very desirable property.*]

(c) Find a subset $S \subseteq \mathbb{Z}_6$ such that S isn't a subring of $\mathbb{Z}_6$, but is a ring under the same addition and multiplication as $\mathbb{Z}_6$. What is $S^\times$? What is $\mathbb{Z}_6^\times$? [*Note that this breaks the nice property from **3.1**b.*]

(d) Find all $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_6$ which preserve addition and multiplication.

(e) Prove that the only ring homomorphism from $\mathbb{Z}_6$ to itself is the identity map.

(f) Suppose $\varphi : R \to S$ is a ring homomorphism. Prove that φ is a *group* homomorphism from $R^\times \to S^\times$. Would this result still hold if we removed the requirement that $\varphi(1) = 1$ from the definition of ring homomorphism?

(g) Suppose $\varphi : R \to S$ is a ring homomorphism, and that $\ker \varphi$ is a subring of R. What can you conclude about the ring S?

(h) Is $\mathbb{Z}$ an ideal of $\mathbb{R}$ (viewed as a ring)? Is $\mathbb{Z}$ an ideal of $\mathbb{Q}$ (viewed as a ring)?

(i) Consider the set $I := \{f \in \mathbb{Z}[t] : f(0) \text{ is even}\}$. Prove that I is an ideal of the ring $\mathbb{Z}[t]$, but not a principal ideal. Find a minimal set of generators of I.

3.2 Given $f, g \in \mathbb{Z}[t]$ with g a monic polynomial, prove that there exist unique $q, r \in \mathbb{Z}[t]$ such that $f = gq + r$ and $\deg r < \deg g$. [*In your write-up you may assume any of the properties we listed in class, but please make sure you know how to prove all those properties from first principles.*]

3.3 The goal of this exercise is to review and develop some nice properties of symmetric groups.

(a) Prove that the collection of adjacent transpositions

$$\{(k\ k+1) : 1 \leq k < n\}$$

generates all of S_n.

(b) Prove that the transposition (1 2) and the n-cycle $(1\ 2\ \cdots\ n)$ generate all of S_n. [*Hint: use part (a).*]

(c) Prove that given a prime p, any transposition and any p-cycle generate all of S_p. [*Hint: relabel elements to put yourself in a position to use part (b).*]

(d) Show by example that primality is a necessary condition in part (c). In other words, find an integer n, as well as a transposition and an n-cycle in S_n, which do *not* generate S_n.

(e) Suppose $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct complex numbers, and $\sigma \in S_n$. What is the relationship between

$$\prod_{i<j}(\alpha_i - \alpha_j) \qquad \text{and} \qquad \prod_{i<j}(\alpha_{\sigma(i)} - \alpha_{\sigma(j)})$$

in terms of σ? Be as precise as possible.

(f) Suppose $\varphi : S_n \to \{\pm 1\}$ is a nontrivial homomorphism. Prove that φ is the sign function on S_n. [*Hint: start by proving that $\varphi(\sigma) = \varphi\big((1\ 2)\big)$ for any transposition $\sigma \in S_n$.*]

3.4 The goal of this exercise is to calculate the Galois group of $f(x) := x^4 - 2$. Denote the roots of f as follows:

$$\alpha_1 := \sqrt[4]{2} \quad \alpha_2 := i\sqrt[4]{2} \quad \alpha_3 := -\sqrt[4]{2} \quad \alpha_4 := -i\sqrt[4]{2}$$

(a) Write down as many independent rational relations among the α_i's as you can. (By *independent* I mean that you can't derive any of the relations from any combination of other relations in your list.)

(b) Explain why (1 2) isn't an element of $\mathrm{Gal}(f)$.

(c) List all elements of $\mathrm{Gal}(f)$.

(d) $\mathrm{Gal}(f)$ is isomorphic to a familiar group. Which one?

(e) Denote $G_0 := \mathrm{Gal}(f)$, and set $G_i := [G_{i-1}, G_{i-1}]$ for all i. Does this sequence terminate? Does the Galois theoretic prediction agree with what you know about the shape of the roots?

3.5 The goal of this exercise is to give a beautiful proof (due to McKay) of Cauchy's theorem:

Cauchy's Theorem. *Let G be a group of order n. If $p \mid n$, then G has an element of order p.*

Let e denote the identity of G, and set

$$A := \{(g_1, g_2, \ldots, g_p) \in G^p : g_1 g_2 \cdots g_p = e\}.$$

In words, A is the set of all *ordered* p-tuples of elements of G whose product is the identity. (Note that G might be nonabelian.) Now set

$$\sigma := (1 \;\; 2 \;\; \cdots \;\; p) \in S_p$$

and let A^σ denote the set of all fixed points of σ, i.e.

$$A^\sigma := \{x \in A : \sigma(x) = x\}.$$

Observe that A^σ is nonempty, since it contains the trivial fixed point $(e, e, \ldots, e)$.

(a) Prove that **if** there exists a nontrivial fixed point of σ, then G contains an element of order p.

(b) Define a relation $\sim$ on A as follows: given $x, y \in A$, we say $x \sim y$ if and only if $\sigma^k(x) = y$ for some integer k. Prove that $\sim$ is an equivalence relation on A.

(c) Show that

$$A \setminus A^\sigma = \bigcup_{x \in A \setminus A^\sigma} [x],$$

where $[x] = \{y \in A : x \sim y\}$ (i.e. $[x]$ is the equivalence class of x under $\sim$).

(d) Prove that $|A \setminus A^\sigma|$ is a multiple of p.

(e) Conclude the proof of the theorem. [*Hint: What can you say about $|A|$?*]

(f) Show by example that primality of p in Cauchy's theorem is necessary. In other words, find a group G and a divisor d of $|G|$ such that G has no elements of order d.

3.6 The goal of this exercise is to prove

Cayley's Theorem. *Every finite group can be embedded in a symmetric group.*

Suppose G is a finite group. For each $g \in G$, define the function

$$\begin{aligned} \phi_g : G &\longrightarrow G \\ a &\longmapsto ga \end{aligned}$$

(a) Prove that $\phi_g \in S_G$ for every $g \in G$. Here S_G denotes the symmetric group of G.

(b) Let $\phi : G \to S_G$ be the function defined by $\phi(g) = \phi_g$. Prove that ϕ is an injective homomorphism.

(c) Prove that if G has order n, then it is isomorphic to a subgroup of S_n.