MATH 581 — FINAL EXAM

June 7, 2006

NAME: ______________________________________

1. Do not open this exam until you are told to begin.
2. This exam has 9 pages including this cover. There are 9 problems.
3. Your final consists of this exam (90 points) and the out of class cryptography assignment (10 points).
4. Do not separate the pages of the exam.
5. Your proofs should be neat and legible. You may and should use the back of pages for scrap work.
6. If you are unsure whether you can quote a result from class or the book, please ask.
7. Please turn **off** all cell phones.

PROBLEM	POINTS	SCORE
1	9	
2	9	
3	9	
4	11	
5	8	
6	12	
7	8	
8	12	
9	12	
TOTAL	90	

1. (3 points each) Define AND give an example of each of the following. You do not need to prove your example is an example.

(a) field

(b) group

(c) ideal

2. (3 points each) Give examples of the following.

(a) an integral domain that is not a field

(b) a non-abelian group

(c) a field K that is a degree 3 extension of $\mathbb{Q}$

3. (3 points each) Let H and N be subgroups of a group G.

(a) Prove that $H \cap N$ is a subgroup of G.

(b) Prove that if H and N are both normal subgroups of G, then $H \cap N$ is a normal subgroup of G.

(c) Suppose $|H| = 49$ and $|N| = 100$. Prove that $H \cap N = \{e_G\}$.

4. (3+2+3+3 points) Let $G = S_3$, the symmetric group on 3 elements. Set

$$N = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

(a) Show that $N = \langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \rangle$.

(b) What is $[G : N]$?

(c) Show that N is a normal subgroup of G.

(d) List the elements of the group G/N. What familiar group is G/N isomorphic to?

5. (4 points each) Do either part (a) or part (b). Please indicate clearly which one you'd like me to grade.

(a) **(i)** Prove that $\mathbb{Q}[x]/\langle x^{13} - 13\rangle \cong \mathbb{Q}[\sqrt[13]{13}]$.
(ii) What is $[\mathbb{Q}[\sqrt[13]{13}] : \mathbb{Q}]$?

(b) **(i)** Prove that $(\mathbb{Z}/5\mathbb{Z})\,[x]/\langle x^3 + 3x + 3\rangle$ is a field.
(ii) How many elements are in this field?

6. (3 points each) Let G and H be groups.

(a) Prove that $G \times H = \{(g, h) : g \in G, h \in H\}$ is a group.

(b) Set $A = \{(g, e_H) : g \in G\}$. Prove that A is a normal subgroup of $G \times H$.

(c) Prove that $G \cong A$.

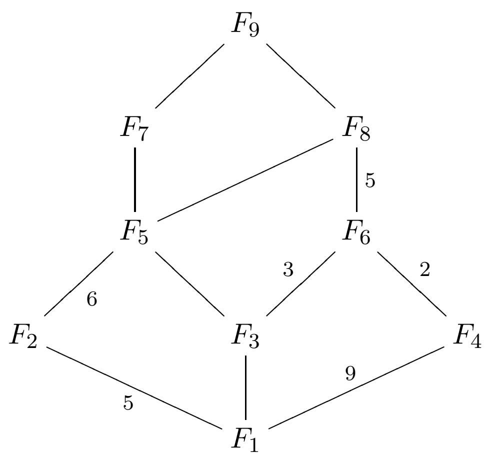
(d) Prove that $(G \times H)/A \cong H$.

7. (3+5 points) Let G, H and N be groups.

(a) Define what it means for a map $\varphi : G \to H$ to be a group homomorphism.

(b) Prove that if $\varphi : G \to H$ and $\psi : H \to N$ are group isomorphisms, then $\psi \circ \varphi : G \to N$ is a group isomorphism.

8. (2 points each) Use the following tower of fields to answer the questions below. Recall that lines indicate containment between fields.



(a) Is it possible for $F_5 \cap F_6 = F_4$? If not, why not?

(b) What is $[F_8 : F_4]$?

(c) What is $[F_8 : F_5]$?

(d) What is $[F_3 : F_1]$?

(e) What is $[F_5 : F_3]$?

(f) Is it possible that $[F_9 : F_1] = 120$? If not, why not?

9. (4 points each) **(a)** Prove that m is a unit in $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(m, n) = 1$.

(b) Recall that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the group of units in $\mathbb{Z}/n\mathbb{Z}$. What are the elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ for p a prime? What is the order of this group?

(c) Prove that $a^{p-1} \equiv 1 \pmod{p}$ for all a such that $\gcd(a, p) = 1$.