MATH 581 — FINAL EXAM

June 7, 2006

NAME: SOLUTIONS

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

A field is a commutative ring in which all nonzero elements are units. An example is $\mathbb{Q}$.

(b) group

A group is a nonempty set G with an operation $\cdot$ so that
(1) If $a, b, c \in G$, then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
(2) There is an identity element $e_G \in G$ so that $e_G \cdot a = a = a \cdot e_G$ for all $a \in G$.
(3) If $a \in G$, there is an element $a^{-1} \in G$ so that $a \cdot a^{-1} = e_G = a^{-1} \cdot a$.
An example of a group is $\mathbb{Z}$ under the operation of addition.

(c) ideal

An ideal I is a nonempty subset of a commutative ring R so that
(1) If $a, b \in I$, then $a + b \in I$
(2) If $a \in I$ and $r \in R$, then $ra \in I$.
An example of an ideal is the set $3\mathbb{Z} = \langle 3 \rangle = \{3n : n \in \mathbb{Z}\}$. This is an ideal in the ring $\mathbb{Z}$.

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

(a) an integral domain that is not a field

The ring $\mathbb{Z}$ is an integral domain but not a field.

(b) a non-abelian group

The group S_3 is a non-abelian group.

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

The field $\mathbb{Q}[\sqrt[3]{2}]$ 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.

Proof: First observe that since H and N are subgroups, necessarily e_G is in each of them, and hence, $e_G \in H \cap N$. Thus, $H \cap N$ is nonempty. Let $a, b \in H \cap N$, i.e., $a, b \in H$ and $a, b \in N$. Using that H is a subgroup we get that $a + b \in H$ and $a^{-1} \in H$. Similarly, we get that $a + b \in N$ and $a^{-1} \in N$. Thus, $a + b \in H \cap N$ and $a^{-1} \in H \cap N$. Hence, $H \cap N$ 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.

Proof: We know from part (a) that $H \cap N$ is a subgroup of G so we only need to show it is a normal subgroup. Let $h \in H \cap N$ and $g \in G$. To see this $H \cap N$ is normal, we need only show that $ghg^{-1} \in H \cap N$. Using that $h \in H$ and H is a normal subgroup of G, we have that $ghg^{-1} \in H$. Similarly, $ghg^{-1} \in N$. Thus, $ghg^{-1} \in H \cap N$ and hence it is a normal subgroup of G. ■

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

Proof: Lagrange's theorem shows that $|H \cap N|$ must divide 49 and 100. However, the only common divisor of 49 and 100 is 1, so $|H \cap N| = 1$. Since it is a subgroup, it must contain e_G and hence $H \cap N = \{e_G\}$. ■

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 $N = \langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \rangle$.

Proof: Observe that $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$. Thus, we see the two sets are equal. ■

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

We have that $[G : N] = 6/3 = 2$.

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

Proof: Since N is an index 2 subgroup you proved in the last homework set that N is necessarily normal. See the solutions from the homework for the proof. ■

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

There are only 2 distinct cosets, we can choose representatives for them so they are given by $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} N$ and $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} N$. This is a group with only two elements, so it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. If you prefer to stay with multiplicative notation, it is isomorphic to $\{\pm 1\}$.

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 $\mathbb{Q}[x]/\langle x^{13} - 13\rangle \cong \mathbb{Q}[\sqrt[13]{13}]$.

Proof: Observe that $f(x) = x^{13} - 13$ is irreducible by Eisenstein's criterion with $p = 13$. Define $\varphi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt[13]{13}]$ by $\varphi(f(x)) = f(\sqrt[13]{13})$. This is an evaluation map, so it is a homomorphism. It is onto because $a \mapsto a$ for $a \in \mathbb{Q}$ and $x \mapsto \sqrt[13]{13}$ and this element generates the extension. Since $f(x) = x^{13} - 13$ is irreducible and is clearly in the kernel of φ, we have that $\ker \varphi = \langle x^{13} - 13\rangle$. The first isomorphism theorem then gives the result. ■

(ii) What is $[\mathbb{Q}[\sqrt[13]{13}] : \mathbb{Q}]$?

$[\mathbb{Q}[\sqrt[13]{13}] : \mathbb{Q}] = \deg f(x) = 13$.

(b) (i) Prove that $(\mathbb{Z}/5\mathbb{Z})[x]/\langle x^3 + 3x + 3\rangle$ is a field.

Proof: To see this is a field, we need only show that $f(x) = x^3+3x+3$ is irreducible in $(\mathbb{Z}/5\mathbb{Z})[x]$. Since $f(x)$ has degree 3, it is enough to check that it has no roots in $\mathbb{Z}/5\mathbb{Z}$. It is then easy to plug in $\overline{0}, \ldots, \overline{4}$ and see that none are zeros of $f(x)$. ■

(ii) How many elements are in this field?

Since $f(x)$ has degree 3, there are $5^3 = 125$ elements 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.

Proof: Let $\star$ be the group operation on G and $*$ the group operation on H. Define a group operation $\cdot$ on $G \times H$ by $(a,b) \cdot (c,d) = (a \star c, b * d)$. Note that $G \times H$ is clearly closed under this operation since G and H are groups and hence closed. It also follows we have associativity because we have it for $\star$ and $*$. Observe that (e_G, e_H) is the identity element of $G \times H$ under the operation $\cdot$. Let $(a,b) \in G \times H$. It is then easy to see that (a^{-1}, b^{-1}) is the inverse of (a,b). Thus, $G \times H$ is a group. ■

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

Proof: Observe that A is nonempty as $(e_G, e_H) \in A$. Let (a, e_H) and (b, e_H) be in A. Then we have $(a, e_H) \cdot (b, e_H) = (a \star b, e_H) \in A$. Similarly, $(a, e_H)^{-1} = (a^{-1}, e_H) \in A$. Thus, A is a subgroup. Let $(g,h) \in G \times H$. To see A is normal we calculate:

$$\begin{aligned} (g,h) \cdot (a, e_H) \cdot (g,h)^{-1} &= (g,h) \cdot (a, e_H) \cdot (g^{-1}, h^{-1}) \\ &= (g \star a \star g^{-1}, h * e_H * h^{-1}) \\ &= (g \star a \star g^{-1}, e_H) \in A. \end{aligned}$$

Thus, A is a normal subgroup. ■

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

Proof: Define $\varphi : G \to A$ by $\varphi(g) = (g, e_H)$. Let $a, b \in G$. We have that $\varphi(a \star b) = (a \star b, e_H) = (a, e_H) \cdot (b, e_H) = \varphi(a) \cdot \varphi(b)$. Thus, φ is a homomorphism. Let $(a, e_H) \in A$. Clearly we have $\varphi(a) = (a, e_H)$, so φ is surjective. Let $a \in \ker \varphi$, i.e., $(a, e_H) = (e_G, e_H)$. Thus, $a = e_G$ and so φ is injective. Hence we have that φ is an isomorphism. ■

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

Proof: Define $\varphi : G \times H \to H$ by $\varphi((g,h)) = h$. It is easy to check that this map is onto and is a homomorphism. Let $(g,h) \in \ker \varphi$, i.e., $h = e_H$. It is then clear that $\ker \varphi = A$ and so the first isomorphism theorem gives the result. ■

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.

The map φ is a group homomorphism if $\varphi(a \star b) = \varphi(a) * \varphi(b)$ for all $a, b \in G$ where $\star$ is the operation on G and $*$ is the operation on H.

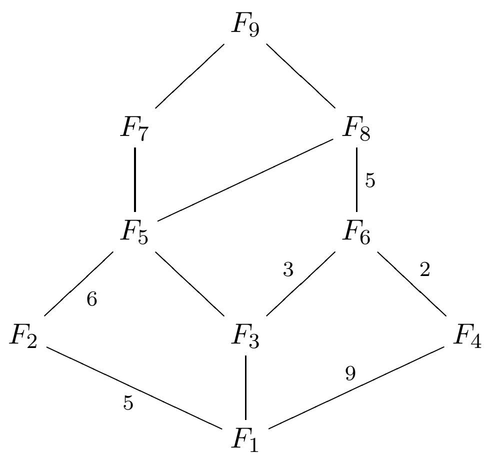
(b) Prove that if $\varphi : G \to H$ and $\psi : H \to N$ are group isomorphisms, then $\psi \circ \varphi : G \to N$ is a group isomorphism.

Proof: Let $\cdot$ be the operation on N. Let $a, b \in G$. We have

$$\begin{aligned} \psi \circ \varphi(a \star b) &= \psi(\varphi(a \star b) \\ &= \psi(\varphi(a) * \varphi(b)) \\ &= \psi(\varphi(a)) \cdot \psi(\varphi(b)) \end{aligned}$$

where we have used that ψ and φ are homomorphisms. Thus, $\psi \circ \varphi$ is a homomorphism. Let $g \in \ker \psi \circ \varphi$. In particular, we have $\psi(\varphi(g)) = e_N$. However, ψ is an isomorphism and hence injective, so $\varphi(g) = e_H$. Similarly, φ is injective so $g = e_G$. Thus, $\ker \psi \circ \varphi = \{e_G\}$ and so $\psi \circ \varphi$ is injective. Let $n \in N$. The fact that φ is surjective implies that there exists $h \in H$ so that $\varphi(h) = n$. Similarly, ψ is surjective so there exists $g \in G$ so that $\psi(g) = h$. Thus, $\psi \circ \varphi(g) = n$ and hence $\psi \circ \varphi$ is surjective. Hence we have shown that $\psi \circ \varphi$ is an 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?

No, F_4 is not even a subset of F_5.

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

$[F_8 : F_4] = [F_8 : F_6][F_6 : F_4] = 5 \cdot 2 = 10$

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

Observe that $[F_8 : F_1] = [F_8 : F_5][F_5 : F_2][F_2 : F_1] = 30[F_8 : F_5]$ on the one hand, and on the other it is given by $[F_8 : F_1] = [F_8 : F_6][F_6 : F_4][F_4 : F_1] = 5 \cdot 2 \cdot 9 = 90$. Thus, it must be that $[F_8 : F_5] = 3$.

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

Note that $[F_6 : F_1] = [F_6 : F_3][F_3 : F_1] = 3[F_3 : F_1]$ and we also have $[F_6 : F_1] = [F_6 : F_4][F_4 : F_1] = 18$. Thus, $[F_3 : F_1] = 6$.

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

Observe that $[F_5 : F_1] = [F_5 : F_3][F_3 : F_1] = 6[F_5 : F_3]$ and we also have $[F_5 : F_1] = [F_5 : F_2][F_2 : F_1] = 30$. Thus, $[F_5 : F_3] = 5$.

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

It is not possible. We have calculated that $[F_8 : F_1] = 90$. We also know that $[F_9 : F_1] = [F_9 : F_8][F_8 : F_1]$. So if it were 120, we would have $90|120$.

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

Proof: Suppose m is a unit in $\mathbb{Z}/n\mathbb{Z}$. Then there exists $a \in \mathbb{Z}/n\mathbb{Z}$ so that $ma = 1$ in $\mathbb{Z}/n\mathbb{Z}$, i.e., $n|(am-1)$. Thus, we have that there exists $b \in \mathbb{Z}$ so that $nb = am - 1$, i.e., $1 = ma + nb$. Note that since $\gcd(m,n)|m$ and $\gcd(m,n)|n$, we have that it divides $ma + nb$, i.e., $\gcd(m,n)|1$ and hence must be 1.
Now suppose that $\gcd(m,n) = 1$. Then there exists $a, b \in \mathbb{Z}$ so that $ma + nb = 1$. Reducing this modulo n we have the equation $ma = 1$ in $\mathbb{Z}/n\mathbb{Z}$, i.e., m is a unit in $\mathbb{Z}/n\mathbb{Z}$. ■

(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?

The elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ are the units in $\mathbb{Z}/p\mathbb{Z}$. From part (a) we see these are the elements that are relatively prime to p, i.e., the elements $\{1, 2, \ldots, p-1\}$. Thus there are $p-1$ elements in the group $(\mathbb{Z}/p\mathbb{Z})^\times$.

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

Proof: Let a be an integer so that $\gcd(a,p) = 1$. Using parts (a) and (b) this implies that $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. The order of this group is $p-1$, so $a^{p-1} = 1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, i.e., $a^{p-1} \equiv 1 \pmod{p}$. ■