MATH 113 FINAL EXAM
December 14, 2012

This exam has 9 problems on 18 pages, including this cover sheet. The only thing you may have out during the exam is one or more writing utensils. You have 180 minutes to complete the exam.

DIRECTIONS

- Be sure to carefully read the directions for each problem.
- All work must be done on this exam. If you need more space for any problem, feel free to continue your work on the back of the page. Draw an arrow or write a note indicating this, so I know where to look for the rest of your work.
- For the proofs, you may use more shorthand than is accepted in homework, but make sure your arguments are as clear as possible. If you want to use theorems from the homework or reading, you must state the precise result you are using. Exception: for the "big-name" theorems, you may just use the name of the result.
- Good luck – do the best you can!

Problem	Max	Score
1	40	
2	10	
3	20	
4	55	
5	20	
6	15	
7	15	
8	15	
9	10	
Total	200	

1. The parts of this problem are not related to each other. Your justifications should be very brief, and you don't need to use complete sentences.

   (a) (5 points) Find $\varphi(15)$, where φ denotes Euler's function. Then use Euler's Theorem to find the remainder of 7^{103} when divided by 15. Show all of your calculations in an organized manner.

$\textcircled{1}\ \textcircled{2}\ \cancel{3}\ \textcircled{4}\ \cancel{5}\ \cancel{6}\ \textcircled{7}\ \textcircled{8}\ \cancel{9}\ \cancel{10}\ \textcircled{11}\ \cancel{12}\ \textcircled{13}\ \textcircled{14}\ \cancel{15}$

$\varphi(15) = 8$, so by Euler $7^8 \equiv 1 \mod 15$

$$7^{103} = 7^{80+\overset{16+7}{\cancel{23}}} = 7^7 = 7^2 \cdot 7^2 \cdot 7^2 \cdot 7$$

$$= \cancel{4 \cdot 4} \cdot 4 \cdot 7$$

$$= 28 = \boxed{13}$$

$7^2 = 49$

$= 4$

$4^2 = 16 = 1$

   (b) (5 points) Find the kernel of the ring homomorphism $\phi : \mathbb{Z}[x, y] \to \mathbb{Z}[x]$ given by $\phi(f(x, y)) = f(x, 0)$.

φ kills of all terms w/ y's, so the kernel is all poly multiples of y, i.e.

$\langle y \rangle = \ker \varphi$.

(c) (5 points) Consider the congruence $65x \equiv 115 \pmod{75}$. Find all solutions in $\mathbb{Z}_{75}$, showing your work.

$\gcd(65, 75) = 5$, so $\exists$ 5 solutions.

divide by 5:

$$13x \equiv 23 \mod 15$$

$$-2x \equiv 23 \quad ''$$

$$-2x \equiv 8 \quad ''$$

$$x \equiv -4 = 11 \text{ in } \mathbb{Z}_{15}$$

$$\boxed{\text{in } \mathbb{Z}_{75}: \ x = 11, 26, 41, 56, \text{ or } 71}$$

+15 +15 . . . .

(d) (5 points) Prove that the quotient group $\mathbb{Z}_6 \times \mathbb{Z}_2 / \langle (2,0) \rangle$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ by finding an appropriate group homomorphism and applying the first isomorphism theorem.

$$\varphi: \mathbb{Z}_6 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$(a, b) \longmapsto (a \bmod 2, b)$$

(i.e. $a \mapsto 0$ if even, 1 if odd)

is clearly surjective, and its kernel is $\langle (2,0) \rangle$,

so by 1st isom Thm:

$$\mathbb{Z}_6 \times \mathbb{Z}_2 / \langle (2,0) \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

(e) (5 points) How many elements of order 2 are there in the group D_7?

In D_7, all reflections have order 2 (there are 7 of them) and no rotation has order 2, so $\boxed{7}$.

(f) (5 points) The polynomial $x^3 + x^2 - \overset{-4x}{\cancel{1}1x} + 3$ in $\mathbb{Z}_7[x]$ can be factored into linear factors. Find this factorization, using the division algorithm for polynomials.

x	$f(x)$
0	0
1	$1+1-4+3=1$
2	$8+4-8+3=7=0$

$$
\begin{array}{r|l}
 & x^2 + 3x + 2 \\ \hline
x-2 & x^3 + x^2 - 4x + 3 \\
 & \underline{-x^3 + 2x^2} \\
 & 3x^2 \\
 & \underline{-3x^2 + 6x} \\
 & 2x + 3 \\
 & \underline{-2x + 4} \\
 & 7 = 0.
\end{array}
$$

$$(x-2)\underbrace{(x^2+3x+2)}_{\text{easy to factor}}$$

$$\boxed{(x-2)(x+1)(x+2)}$$

(g) (5 points) Suppose $\phi : G \to H$ is a group homomorphism. If $|ker(\phi)| = 6$ and $|H| = 15$, what are the possible sizes of G?

By 1st isom thm, $\frac{|G|}{|ker|} = |im|$.

im φ is a subgroup of H, so

$|im \varphi| = 1, 3, 5,$ or 15.

Then $|G| = \underset{\{1,3,5,15\}}{|im|} \cdot \underset{6}{|ker|}$,

i.e. $\boxed{6, 18, 30, 90}$

(h) (5 points) Find a subring R of $\mathbb{Z}_{24}$ and an ideal I of R such that the quotient ring R/I has two elements but is not isomorphic to $\mathbb{Z}_2$. Fill in the addition and multiplication tables for your cosets below.

R/I :

+	$0+I$	$2+I$
$0+I$	$0+I$	$2+I$
$2+I$	$2+I$	$0+I$

$\cdot$	$0+I$	$2+I$
$0+I$	$0+I$	$0+I$
$2+I$	$0+I$	$0+I$

$R = \langle 2 \rangle = \{0, 2, 4, \dots, 22\}$.

no unity in

$|R| = 12$.

$I = \langle 4 \rangle = \{0, 4, \dots, 20\}$. $|I| = 6$

2. (10 points) Construct a field with 8 elements, by taking an appropriate quotient of a polynomial ring. Be sure to describe the elements of your field and justify your work, quoting any relevant theorems you need.

We know x^3+x^2+1 is irred over $\mathbb{Z}_2$, since its deg is ≤ 3 and neither 0 nor 1 is a root.

Thus by a thm, $I=\langle x^3+x^2+1\rangle$ is a maximal ideal of $\mathbb{Z}_2[x]$.

We know (by another thm), a ring/maxl ideal is a field, so

$$\mathbb{Z}_2[x]/\langle x^3+x^2+1\rangle$$ is a field.

Coset reps can be given by all poss remainders after dividing by x^3+x^2+1, i.e. each coset is of the form $(ax^2+bx+c)+I$ w/ $a,b,c\in\mathbb{Z}_2$. There are 8 of these, so our field has 8 elts.

3. (2 points each) No justification is required, but you may use the space to do (ungraded) scratch work if you want. Circle the correct answer, and make sure there is no ambiguity if you change your mind.

(a) In the group $\mathbb{Q}/\mathbb{Z}$ under addition, every element has finite order.

[✓ *TRUE*] *FALSE*

$\frac{a}{b} + \mathbb{Z}$ has order b if reduced.

(b) Let D be the integral subdomain $D = \{a + bi : a, b \in \mathbb{Z}\}$ of $\mathbb{C}$. Then the field of quotients of D is $\{c + di : c, d \in \cancel{\mathbb{R}}\}$.

$\mathbb{Q}$

TRUE [✓ *FALSE*]

(c) If g_1 and g_2 are elements of a group G such that $|g_1| = 2$ and $|g_2| = 3$, then $|g_1 g_2| = 6$.

TRUE [✓ *FALSE*]

Eg. $g_1 = (1, 2)$, $g_2 = (1, 2, 3)$ $\in S_3$.

(d) Every nonabelian group has at least one proper nonabelian subgroup.

TRUE [✓ *FALSE*]

S_3, D_4 have proper subs of size ≤ 4 only, so all abelian.

(e) The set of 3×3 invertible upper triangular matrices with real entries forms a subgroup of $GL(3, \mathbb{R})$.

[✓ *TRUE*] *FALSE*

(f) If G is a group and H and K are two subgroups of G, then $H \cap K$ is a subgroup of G.

[✓ *TRUE*] *FALSE*

Proved in HW

(g) The groups $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{14}$ and $\mathbb{Z}_{36} \times \mathbb{Z}_{28}$ are isomorphic.

By FTFGAG: *TRUE* [✓ *FALSE*]

$\cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_2 \times \mathbb{Z}_7$

$\cong \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_4 \times \mathbb{Z}_7$

(h) The ring $\mathbb{Z}[x]$ has infinitely many ideals.

[✓ *TRUE*] *FALSE*

Eg: $\langle x \rangle, \langle x^2 \rangle, \langle x^3 \rangle, \ldots$

(i) If G is an infinite group and $H \leq G$, then the index $[G : H]$ is also infinite.

TRUE [✓ *FALSE*]

Eg. $G = \mathbb{Z}$, $H = 2\mathbb{Z}$. index 2.

(j) If E and F are fields, then $E \times F$ is also a field.

TRUE [✓ *FALSE*]

Not even an integral domain, e.g. $(0,1)(1,0) = (0,0)$, so we have zero divisors.

4. (5 points each) For each of the items listed below, give a *specific* example with the stated property. All of these are possible, and no justification is required.

(a) A subgroup of $D_4 \times GL(2, \mathbb{C})$ which has order 32.

size 8

$$D_4 \times \left\langle \begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix} \right\rangle$$

8 elts × 4 elts. = 32.

(b) A cyclic subgroup H of $G = \mathbb{Z}_{12} \times \mathbb{Z}_{10}$ such that there are 8 cosets of H in G.

$$|H| = \frac{12 \cdot 10}{8} = \frac{60}{4} = 15,$$ so

$$\boxed{\langle (4, 2) \rangle}$$ works

order 3 order 5

$\mathrm{lcm}(3, 5) = 15$

(c) A nonabelian group with at least eight elements of order 5.

$$S_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

or S_5

or $D_5 \times D_5$ etc.

(d) A subgroup of S_9 which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$.

$$\langle (1,2),\ (3,4,5),\ (6,7,8,9) \rangle$$

(e) Three rings R, S, and T with different characteristics, such that the direct product ring $R \times S \times T$ has characteristic 44.

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{11}$$

char $\quad 2 \quad 4 \quad 11$

$$\mathrm{lcm}(2, 4, 11) = 44$$

(f) A polynomial ring R which is *not* an integral domain and an ideal I such that R/I is a field.

$R = \mathbb{Z}_6[x]$, $\quad I = \langle 2, x \rangle$

$$R/I \cong \mathbb{Z}_2$$

(g) A nontrivial ring homomorphism $\mathbb{Z}[x,y] \to M_2(\mathbb{Z})$.

$$f(x,y) \longmapsto \begin{bmatrix} f(1,1) & 0 \\ 0 & f(0,1) \end{bmatrix}$$

hom since it's essentially 2 eval homomorphisms.

(h) A polynomial in $\mathbb{Z}[x]$ which has 4 terms and is irreducible using Eisenstein's Criterion with $p = 7$.

$$x^{17} - 77x^{11} + 49x - 21$$

(i) A basis for the field extension $\mathbb{Q}(\sqrt{5}, i)$, viewed as a vector space over $\mathbb{Q}$.

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{5}, i) \arrow[d, dash, "x^2+1"] \\
\mathbb{Q}(\sqrt{5}) \arrow[d, dash, "x^2-5"] \\
\mathbb{Q}
\end{tikzcd}$$

$$\{1, \sqrt{5}\} \times \{1, i\}$$

basis:

$$\{1, \sqrt{5}, i, i\sqrt{5}\}.$$

(j) An irreducible polynomial in $\mathbb{Q}(\pi^3)[x]$ such that the corresponding extension field of $\mathbb{Q}(\pi^3)$ contains π.

$$\boxed{X^3 - \pi^3}$$

(irred since factoring requires using π, π^2, ie $(x-\pi)(x^2+\pi x+\pi^2)$)

π is a root.

(k) A field F which contains $\mathbb{Q}$ as a proper subfield and is a proper subfield of $\mathbb{Q}(\sqrt[4]{7})$, i.e. $\mathbb{Q} \lneq F \lneq \mathbb{Q}(\sqrt[4]{(7)})$.

$$\boxed{F = \mathbb{Q}(\sqrt{7})}$$

$$\begin{tikzcd}
\mathbb{Q}(\sqrt[4]{7}) \arrow[d, dash] \arrow[dd, dash, bend right, "\deg 4"'] \\
\mathbb{Q}(\sqrt{7}) \arrow[d, dash, "\deg 2"] \\
\mathbb{Q}
\end{tikzcd}$$

$\sqrt{7} \in \mathbb{Q}(\sqrt[4]{7})$.

5. All parts of this problem deal with $\mathbb{Z}_4 \times \mathbb{Z}_2$.

(a) (5 points) Viewing $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ as an additive group, find two different subgroups K and L, each of which is isomorphic to $\mathbb{Z}_4$. Briefly justify your answer.

$K = \langle (1,0) \rangle = \langle (3,0) \rangle.$

$L = \langle (1,1) \rangle = \langle (3,1) \rangle.$

these are both $\cong \mathbb{Z}_4$ since they are gen by a single order 4 element.

(b) (5 points) Viewing $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ as an additive group, find a subgroup H which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Briefly justify your answer.

$H = \{(0,0), (0,1), (2,0), (2,1)\}.$

this is a subgroup of order 4, and each elt has order ≤ 2, so by FTFGAG, it is $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(c) (5 points) Viewing $R = \mathbb{Z}_4 \times \mathbb{Z}_2$ as a ring, find a subring S of R which is not an ideal. Briefly justify your answer.

$S = \{(0,0), (1,1), (2,0), (3,1)\}$.

Clearly an additive sub, & it's closed under mult.

But

$$\underset{\in R}{(2,1)} \cdot \underset{\in S}{(1,1)} = \underset{\notin S}{(2,1)}, \text{ so } S \neq \text{ideal}.$$

(d) (5 points) Viewing $R = \mathbb{Z}_4 \times \mathbb{Z}_2$ as a ring, find an ideal I of R which is not a prime ideal. Briefly justify your answer.

$I = \langle (0,1) \rangle = \{0\} \times \mathbb{Z}_2$ is a principal ideal, but

$$\underset{\notin I}{(2,0)} \underset{\notin I}{(2,1)} = \underset{\in I}{(0,0)}, \text{ so}$$

I is not prime.

6. (10 points) Prove **ONE** of the following. If you try both, clearly indicate which one you want to be graded.

   (a) Suppose E is a finite extension of a field F and $[E : F]$ is a prime number. Prove that E is a simple extension of F.

   (b) Suppose p is an odd prime. Prove that no field of order p^2 is algebraically closed.

a)

$$\begin{tikzcd} E \arrow[d, dash, "\deg p"] \\ F \end{tikzcd}$$

Pf: Let $[E:F] = p$, p prime. Take any $\alpha \in E$ but not F.

then $F < F(\alpha) \subseteq E$.

By "chain rule" for field extn indexes,

$p = [E:F] = [E:F(\alpha)] \cdot [F(\alpha):F]$.

Since $\alpha \notin F$, $[F(\alpha):F] \neq 1$, so it must be p, since p is prime. But then $[E:F(\alpha)] = 1$, which means $E = F(\alpha)$.

b) Pf: Suppose F is a field of order p^2, then it must have characteristic p.

(p odd).

Claim: Some $x^2 - k$ is irreducible over F. Consider the perfect squares in F. Since $1 \neq -1$, but $1^2 = (-1)^2 = 1$, there are at most $p^2 - 1$ different perfect squares in F. Thus there is some k that is not a perfect square, making $x^2 - k$ irred over F. Since $F[x]$ contains a deg 2 poly w/ no roots in F, F is not algebraically closed.

7. (10 points) Prove **ONE** of the following. If you try both, clearly indicate which one you want to be graded.

   (a) Suppose A and B are ideals of a ring R. Prove that $A + B$ is also an ideal of R.

   (b) Let $\phi : R \to S$ be a surjective ring homomorphism, and let I be an ideal of R. Prove that $\varphi(I)$ is an ideal of S.

a) $A+B = \{a+b : a \in A, b \in B\}$.

Pf: We will use the ideal criterion.

- Since $0 \in A$, $0 \in B$, we have $0+0 = 0 \in A+B$.

- Suppose $a_1 + b_1 \in A+B$ and $a_2 + b_2 \in A+B$. (i.e. $a_i \in A$, $b_i \in B$)

Then $(a_1+b_1) - (a_2+b_2)$
$= (a_1 - a_2) + (b_1 - b_2)$ using assoc/dist,

$a_1 - a_2 \in A$ since A is an ideal

$b_1 - b_2 \in B$ " B " "

So $(a_1+b_1) - (a_2+b_2) \in A+B$.

- Suppose $r \in R$, $a+b \in A+B$.

Then $r(a+b)$ and $(a+b)r \in A+B$

since $ra, ar \in A$ and $rb, br \in B$ since A, B = ideals.

b) $\varphi : R \longrightarrow S$ surj., $I =$ ideal of R.

Show $\varphi(I) =$ ideal of S.

Thm: use ideal criterion:

- For a ring hom, $0_R \mapsto 0_S$, so

  $0_S \in \varphi(I)$ since $0_R \in I$.

- Suppose $a', b' \in \varphi(I)$, i.e,

  $\exists\ a, b \in I$ st $a' = \varphi(a)$, $b' = \varphi(b)$.

  Then by hom prop, $\varphi(a-b)$

  $= \varphi(a) - \varphi(b) = a' - b'$, so

  $a' - b' \in \varphi(I)$.

- Suppose $r' \in S$, $a' \in \varphi(I)$.

  Then $a' = \varphi(a)$ for some $a \in I$,

  and since φ surj, $r' = \varphi(r)$

  f.s. $r \in R$. Then $\varphi(ar) = \varphi(a)\varphi(r)$

  $= a'r'$

  so $a'r' \in \varphi(I)$. Similarly, $r'a' \in \varphi(I)$.

So $\varphi(I)$ is an ideal.

8. (10 points) Prove **ONE** of the following. If you try both, clearly indicate which one you want to be graded.

   (a) Suppose that G is a cyclic group and H is a subgroup of G. Prove that G/H is cyclic.

   (b) Let H be a normal subgroup of G of index m. Prove that $g^m \in H$ for all $g \in G$. (Hint: use what you know about G/H.)

See practice midterm.

9. (a) (5 points) What is your favorite group? Why?

?

(b) (5 points) What is your favorite 113 theorem? Briefly describe (3-5 sentences) something that you like about the proof or about an application of the theorem you choose.