MATH 113 PRACTICE FINAL #1–8.

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!

Real thing will be $\cong$ this length.

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

extra notes in green added after the 32 min

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) Use Fermat's Little Theorem to find the remainder of 8^{101} when divided by 13. Show all of your calculations in an organized manner.

FLT: $x^{12} \equiv 1$ if $\gcd(x, 13) = 1$.

$101 = \underbrace{12 \cdot 8}_{96} + 5$

So $8^{101} = 8^{12} \cdot 8^5 = 8^5$.

$8^2 = 64 = 12 = -1 \mod 13$, so

$8^5 \equiv 8^2 \cdot 8^2 \cdot 8 = (-1)(-1)(8) = \boxed{8}$

f) ~~(b)~~ (5 points) The polynomial $\overbrace{x^3 - x^2 - x - 2}^{= f(x)}$ in $\mathbb{Z}_7[x]$ can be factored into linear factors. Find this factorization, using the division algorithm for polynomials if necessary.

x	$f(x)$
0	-2
1	$1-1-1-2 \neq 0$
2	$8-4-2-2=0$

so $x-2$ is a Factor

x	x^2+x+1
2	$4+2+1=7$ $=0$

$$\begin{array}{r|l} & x^2 + x + 1 \\ x-2 & x^3 - x^2 - x - 2 \\ & -x^3 + 2x^2 \\ \hline & x^2 - x - 2 \\ & -x^2 + 2x \\ \hline & x - 2 \end{array}$$

$$\begin{array}{r|l} & x + 3 \\ x-2 & x^2 + x + 1 \\ & -x^2 + 2x \\ \hline & 3x + 1 \\ & -3x + 6 \\ \hline & 7 = 0 \end{array}$$

$\boxed{(x-2)^2(x+3)}$

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

$\gcd(115, 65) = 5$ so 5 solutions.

divide all by 5:

$23x \equiv 15 \mod 13$

$10x \equiv 15 \mod 13$

$-3x \equiv 15 \mod 13$

divide by -3

$x \equiv -5 = 8 \mod 13$

$\boxed{\text{in } \mathbb{Z}_{65}: \; x = 8, 21, 34, 47, 60}$

(d) (5 points) What is the characteristic of the ring $\mathbb{Z}_6 \times \mathbb{Z}_{28} \times \mathbb{Z}_{15}$? (You may write your answer as a product of primes if it is a large integer.)

shift down

$\operatorname{lcm}(6, 28, 15)$

$= \operatorname{lcm}(2 \cdot 3, 2^2 \cdot 7, 3 \cdot 5)$

$= \boxed{2^2 \cdot 3 \cdot 5 \cdot 7}$

(e) (5 points) Find the order of the element $(1,3,7,8,9)(2,3,4,7)(5,6,8)$ in the symmetric group S_9.

in disj. cycle not:

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

$\operatorname{lcm}(7,2) = \boxed{14}$

5)

~~(f)~~ (5 points) Show that $\frac{17}{11} - \frac{3}{7}\sqrt{5}$ is in the field of quotients of the integral subdomain $D = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$ of $\mathbb{R}$ by expressing it as a ratio of two appropriate elements.

$$\frac{7}{7} \cdot \frac{17}{11} - \frac{3}{7}\sqrt{5} \cdot \frac{11}{11}$$

$$= \frac{7 \cdot 17 - 33\sqrt{5}}{77}$$

num $\in D$, denom $\in D$ ✓

(g) (5 points) Suppose $\phi : G \to H$ is a group homomorphism which is NOT one-to-one. If $|G| = 24$ and G has normal subgroups of orders 24, 12, 8, and 1 (and no others), what groups can $im(\phi)$ possibly be isomorphic to?

$|\ker| = 24, 12, 8.$

1st isom thm

$G/\ker \cong im,$

so $|im| = \frac{24}{24}, \frac{24}{12}, \frac{24}{8}$

$= 1, 2,$ or $3.$

so $im(\phi) \cong \{e\}, \mathbb{Z}_2$ or $\mathbb{Z}_3.$

(h) (5 points) Give addition and multiplication tables for two nonisomorphic rings R and S, each of order 2.

R:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

$\cong \mathbb{Z}_2$

S:

+	0	x
0	0	x
x	x	0

·	0	x
0	0	0
x	0	0

no unity

can get by

$2\mathbb{Z}/4\mathbb{Z}.$

any names ok here, except one should prob be 0.

2. (10 points) Construct a field with 25 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.

In $\mathbb{Z}_5$, perfect sq are : $0, 1^2, 2^2, 3^2, 4^2$

$0, 1, -1, -1, 1$

So x^2+2 is irred. in $\mathbb{Z}_5[x]$.

Then $\mathbb{Z}_5[x]/\langle x^2+2\rangle$ is a field of 25 elts, since by book

thm: x^2+2 irred $\Rightarrow$ $\langle x^2+2\rangle$ maximal,

and by a thm: ring/(max'l ideal) $\cong$ field.

Elements are cosets of the form

$ax+b+\langle x^2+2\rangle$,

w/ $a, b \in \mathbb{Z}_5$. (the $ax+b$ are all poss. remainders)

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) The group $\mathbb{R}/\mathbb{Z}$ under addition has at least one element of order 7.

TRUE *FALSE*

eg $\frac{1}{7} + \mathbb{Z}$.

(b) A finite abelian group has prime order if and only if it has no proper nontrivial subgroups.

TRUE *FALSE*

(c) If G is a cyclic group, then every factor group of G is cyclic.

TRUE *FALSE*

(d) If $A \subset B \subset C$ are groups such that $A \lhd B$ and $B \lhd C$, then $A \lhd C$.

TRUE *FALSE*

try $C = D_4$ for examples

(e) The group S_9 has at least one element of order 16.

TRUE *FALSE*

Can't get lcm = 16 for disjoint cycles w/ 9 elts.

(f) Every abelian group whose order is divisible by 8 contains a cyclic subgroup of order 8.

TRUE *FALSE*

eg $\mathbb{Z}_4 \times \mathbb{Z}_2$

(g) The groups $\mathbb{Z}_{12} \times \mathbb{Z}_{14}$ and $\mathbb{Z}_6 \times \mathbb{Z}_{28}$ are isomorphic.

TRUE *FALSE*

$(\mathbb{Z}_3 \times \mathbb{Z}_4) \times (\mathbb{Z}_2 \times \mathbb{Z}_7)$ vs $(\mathbb{Z}_2 \times \mathbb{Z}_3) \times (\mathbb{Z}_4 \times \mathbb{Z}_7)$

(h) If g is an element of a finite nonabelian group G, then $|g|$ divides $|G|$.

TRUE *FALSE*

Lagrange (cor)

(i) In the dihedral group D_n (symmetries of an n-gon), there exists an element of order k for each positive integer k which divides n.

TRUE *FALSE*

$r^{\frac{n}{k}}$ w/ $r=$ smallest rotation.

(j) The union of two subrings of a ring R must also be a subring of R.

TRUE *FALSE*

Eg: in $\mathbb{Z}_6$

$\langle 2 \rangle \cup \langle 3 \rangle = \{0, 2, 3, 4\}$

not gp.

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 $D_4 \times S_7$ which has order 16.

$D_4 \times \langle (1,2) \rangle$

order 8 order 2

(b) An abelian group with at least 34 elements of order 17.

$\mathbb{Z}_{17} \times \mathbb{Z}_{17}$

16 choices 16 choices $16 \times 16 > 34$

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

S_5 (lots of 5-cycles)

≥ 6

any (a,b,c,d,e)

a,b,c,d,e. all diff

(d) A subgroup of $GL(2, \mathbb{R})$ which has exactly 8 elements.

$$\left\{ \begin{bmatrix} i^a & 0 \\ 0 & (-1)^b \end{bmatrix} : \begin{array}{l} a \in \{0,1,2,3\} \\ b \in \{0,1\} \end{array} \right\}$$

(e) A pair of zero divisors in the ring $\mathbb{Z}_5 \times M_2(\mathbb{Z})$.

$$\left(0, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) \cdot \left(1, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\right)$$

$$= \left(0, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\right)$$

(f) A polynomial ring R which is an integral domain and an ideal I such that R/I is a field.

$$R = Q[x], \quad I = \langle x \rangle$$

$$R/I \cong Q$$

(g) A nontrivial ring homomorphism $\varphi: \mathbb{Z}[x] \to \mathbb{Z} \times \mathbb{Z}$.

$$f(x) \longmapsto (f(0), f(1))$$

$$\forall f(x) \in \mathbb{Z}[x].$$

one eval hom in each coord.

(h) A polynomial in $\mathbb{Z}[x]$ which has 4 terms and is irreducible using Eisenstein's Criterion with $p = 3$.

$$x^8 - 3x^3 + 18x^2 - 6$$

$3 \nmid 1$ $\quad 3 \mid -3$ $\quad 3 \mid 18$ $\quad 3 \mid -6$

$9 \nmid -6$

(i) A basis for the field extension $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$, viewed as a vector space over $\mathbb{Q}$.

$$\{1, \sqrt{2}\} \times \{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$$

$$= \{1, \sqrt{2}, \sqrt[3]{5}, \sqrt{2}\cdot\sqrt[3]{5}, (\sqrt[3]{5})^2, \sqrt{2}\cdot(\sqrt[3]{5})^2\}$$

(j) An extension field of $\mathbb{Q}$ which is algebraic of degree 4.

$x^4 - 7$ irred Eis $p = 7$

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

(k) A field which has the same algebraic closure $\overline{\mathbb{Q}}$ as $\mathbb{Q}$ but is not equal to $\mathbb{Q}$ or $\overline{\mathbb{Q}}$.

$$\mathbb{Q}(\sqrt{2})$$

any alg extn between

$\mathbb{Q}$ & $\overline{\mathbb{Q}}$

5. All parts of this problem deal with $\mathbb{Z}_9 \times \mathbb{Z}_3$.

(a) (5 points) Viewing $G = \mathbb{Z}_9 \times \mathbb{Z}_3$ as an additive group, find a subgroup K which is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$. You may describe your group by writing out the complete list of elements or by a set of generators. ~~In 1-2 sentences, explain why~~ your answer ~~is correct.~~

Briefly justify

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

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

K has 9 elements, all w/ order ≤ 3, so by FTFGAG, K must be $\cong \mathbb{Z}_3 \times \mathbb{Z}_3$

(b) (5 points) Viewing $G = \mathbb{Z}_9 \times \mathbb{Z}_3$ as an additive group, find a subgroup H such that G/H is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$. ~~Justify~~ your answer ~~in 1-2 sentences~~.

Briefly justify

$$H = \langle (3,0) \rangle.$$

Cosets $(a,b) + H$ all have order ≤ 3, since $(3a, 3b) \in H$ $\forall a, b$,

and G/H has $27/3 = 9$ elts.

By FTFGAG, $G/H \cong \mathbb{Z}_3 \times \mathbb{Z}_3$

(c) (5 points) Viewing $R = \mathbb{Z}_9 \times \mathbb{Z}_3$ as a ring, find a subring S of R which is not an ideal. Briefly justify your answer.

$S = \langle (1,1) \rangle$

$= \{ (0,0), (1,1), (2,2), (3,0), (4,1), (5,2), (6,0), (7,1), (8,2) \}$. subring, (closed under mult)

but $(1,2) \cdot (1,1) = (1,2) \notin S$.

(d) (5 points) Viewing $R = \mathbb{Z}_9 \times \mathbb{Z}_3$ as a ring, find an ideal I of R which is not a prime ideal. Briefly justify your answer.

$I = \{0\} \times \mathbb{Z}_3$.

$(3,0)(3,0) = (0,0) \in I$,

but $(3,0) \notin I$.

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 an extension field of F. If $\alpha \in E$ is algebraic over F and $\beta \in F(\alpha)$, prove that $deg(\beta, F)$ divides $deg(\alpha, F)$.

   (b) Suppose E is a finite extension of a field F. Let $p(x) \in F[x]$ be a polynomial which is irreducible over F. If the degree of $p(x)$ does not divide $[E : F]$, prove that E does not contain any zeroes of $p(x)$.

Pf: Since $\beta \in F(\alpha)$, $F(\beta) \subseteq F(\alpha)$,

So we have

$$\begin{array}{c} F(\alpha) \\ | \\ F(\beta) \\ | \\ F \end{array}$$

Using "chain rule" for field extns,

$$deg(\alpha, F) = deg(\beta, F) \cdot deg(\alpha, F(\beta)),$$

So $deg(\beta, F)$ divides $deg(\alpha, F)$.

$$\begin{tikzcd}[column sep=small]
E \arrow[dd, dash] \arrow[dr, dash] & \\
& F(\alpha) \\
F \arrow[ur, dash] &
\end{tikzcd}$$

$p(x)$ irred $/_F$

Let $d = \deg p(x)$ over F,

$n = [E : F]$, so

$d \nmid n$.

Pf by cont. Suppose E contains a zero α of $p(x)$.

Since $p(\alpha) = 0$ and $p(x)$ is irred. over F, we know

$\text{irr}(\alpha, F) = p(x)$.

Then $F \leq F(\alpha) \leq E$, so by "chain rule" for field extns,

$d = [F(\alpha) : F]$ divides

$n = [E : F]$, which is imposs, so E contains no zeros of $p(x)$.

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

   (a) State the definition of a *unit* in a ring and the definition of a *zero divisor* in a ring. Prove that in the ring $\mathbb{Z}[x]$, the element x is neither a unit nor a zero divisor.

   (b) State the definition of a *unit* in a ring and the definition of a *zero divisor* in a ring. Prove that if D is an integral domain, then $D[x]$ is also an integral domain.

A unit is an element $r \in R$ s.t. $\exists s \in R$ w/ $rs = 1$.

A zero div. is an element $r \in R$ st $\exists s \in R$ w/ $rs = 0$.

Consider $x \cdot f(x)$ w/ $f(x) \in \mathbb{Z}[x]$.

If $f(x) \neq 0$, then $\deg x\, f(x) = \deg f(x) + 1$, since $\mathbb{Z}$ is an integral domain.

Thus, it is impossible for $x \cdot f(x)$ to be 1, and it can only be 0 if $f(x) = 0$, so x is neither a unit nor a zero div.

See defs on prev page.

Pf. Suppose D = int dom. Then clearly $D[x]$ is comm, and $1 \in D$ is also unity in $D[x]$, viewed as a constant poly.

Now we need to show $D[x]$ has no zero divisors.

Suppose $f(x), g(x) \in D[x]$ w/ $f(x)g(x) = 0$. If ax^n and bx^m are the highest degree terms of f & g, then $(ax^n)(bx^m) = abx^{m+n}$ is the highest deg term of $f(x)g(x)$. This can only be the 0 poly if $ab = 0$, and since D = int dom, this means $a = 0$ and $f(x) = 0$ or $b = 0$ and $g(x) = 0$, so $D[x]$ is an int dom.

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

   (a) Let $\phi : G \to G'$ be a group homomorphism. Prove that if N is a ~~normal~~ subgroup of G, then $\phi[N]$ is a ~~normal~~ subgroup of G'.

   (b) Let $\phi : G \to G'$ be a group homomorphism. Prove that if N' is a ~~normal~~ subgroup of G', then $N = \phi^{-1}[N']$ is a ~~normal~~ subgroup of G.

Pf: Use sub gp criterion:

- nonempty
- $a', b' \in \varphi(N) \Rightarrow a'b'^{-1} \in \varphi(N)$.

Lemma: Since φ is a gp hom

$$e \longmapsto e'$$

$$g^{-1} \longmapsto \varphi(g)^{-1} \quad \forall g \in G.$$

Since $e' \in \varphi[N]$, $\varphi[N]$ is nonempty.

Suppose $a', b' \in \varphi[N]$, i.e..

$a' = \varphi(a)$, $b' = \varphi(b)$ f.s. $a, b \in G$.

then
$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1})$$
$$= \varphi(a)\varphi(b)^{-1}$$
$$= a'(b')^{-1},$$
so $a'(b')^{-1} \in \varphi[N]$

and $\varphi[N] \leq G'$.

<u>Pf</u>: Use subgp criterion.

- $e = \varphi^{-1}(e')$, so $\varphi^{-1}[N']$ is nonempty
- Suppose $a, b \in \varphi^{-1}[N']$, i.e. $\varphi(a), \varphi(b) \in N'$.

then $\varphi(ab^{-1}) = \varphi(a)\,\varphi(b)^{-1}$

$\in N'$, since $\varphi(a), \varphi(b) \in N'$

So $ab^{-1} \in \varphi^{-1}[N']$, and

$\varphi^{-1}[N'] \leq G$.

9. *(Note, this exact question *will* be on the real final.)*

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

Don't want to influence your answers :)

   (b) (5 points) What is your favorite 113 theorem not addressed in the proofs on this exam (i.e. problems 6-8)? Briefly describe (3-5 sentences) something that you like about the proof or about an application of the theorem you choose.