Name:

MATH 113 PRACTICE FINAL # | - 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

≓ this length.

	2.6	G
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 offer 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 8¹⁰¹ when divided by 13. Show all of your calculations in an organized manner.

FLT:
$$x^{n} \equiv 1$$
 if $g cd(x, (3) = 1$.
 $|D| = (2 \cdot 8 + 5)$
 g_{0}
So $g^{101} = g^{12} \cdot 8^{5} = 8^{5}$.
 $g^{2} = 64 = (2 = -1 \text{ m} \cdot d^{-13})$, so
 $g^{5} \equiv g^{2} \cdot 8^{2} \cdot 8 = (-1)(-1)(8) = [8]$
F) (5 points) The polynomial $x^{3} - x^{2} - x - 2$ in $\mathbb{Z}_{7}[x]$ can be factored into linear
factors. Find this factorization, using the division algorithm for polynomials if
necessary.
 $x + 4x + 1$
 $\frac{x}{2} + x + 1}{2} + \frac{x^{2} + x + 1}{4 + 2x1 = 7}$
 $x - 2 \int x^{3} - x^{2} - x - 2$
 $-x^{3} + 1x^{2}$
 $x - 2 \int x^{3} - x^{2} - x - 2$
 $-x^{3} + 1x^{2}$
 $x - 2 \int x^{3} - x^{2} - x - 2$
 $-x^{3} + 1x^{2}$
 $x - 2 \int x^{3} - x^{2} - x - 2$
 $-x^{3} + 1x^{2}$
 $x - 2 \int x^{3} - x^{2} - x - 2$
 $-x^{3} + 1x^{2}$
 $x - 2 \int x^{3} - x^{2} - x - 2$
 $-x^{3} + 1x^{2}$
 $x - 2 \int x^{3} + x + 1$
 $-x^{3} + 2x^{2}$
 $x - 2 \int x^{3} + x + 1$
 $-x^{3} + 2x^{2}$
 $x - 2 \int x^{3} + x + 1$
 $-3x + 1$
 $(x - 2)^{2}(x + 3)^{7} = 0$

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

$$g cd(115, 15) = 5$$

$$g cd$$

$$= 2^2 \cdot 3 \cdot 5 \cdot 7$$

(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:

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

 $lcm(7, 2) = [14]$

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

$$\frac{4}{7} \cdot \frac{17}{11} - \frac{3}{7} \sqrt{5} \cdot \frac{11}{11}$$

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

$$= \frac{7 \cdot 17}{77}$$

$$= \frac{77}{77}$$

$$= \frac{77}{77}$$

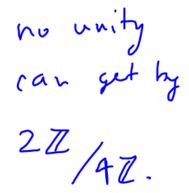
(g) (5 points) Suppose $\phi: G \to H$ is a group homomorphism which is NOT one-toone. If |G| = 24 and G has normal subgroups of orders 24, 12, 8, and 1 (and no others), what groups can $im(\phi)$ possibly be isomorphic to?

$$| \text{ker} | = 24, 12, 8.$$

 $G/\text{ker} \cong \text{im}, \qquad [\text{st isom thm}]$
 $So | \text{im} | = \frac{24}{24}, \frac{24}{12}, \frac{24}{8}$
 $= 1, 2, \text{or } 3.$
 $So | \text{im}(e) \cong \{e\}, Z_2 \text{ or } Z_3.$

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

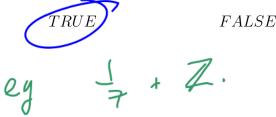
 $\simeq \mathbb{Z}_{2}$



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 Zs, perfect Sq are: 0,1222,32,02 0, 1, -1, -1, 1 So x²+2 is irred, in Zs[x]. is a Then ZsLx Kx2+2> since hybric field of 25 elts; <x2+2) ivred => maximal Jhm; x2+2 ving/maxil and by a thm: ideal) ave of H field. the form Elements $ax+b+\langle x^2+2\rangle,$ v/a, b e Z5. (the axtband all poss.) re mainders

- 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.



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

TRUEFALSE

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

FALSE

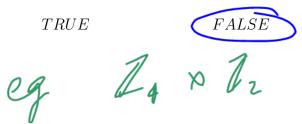
(d) If $A \subset B \subset C$ are groups such that $A \lhd B$ and $B \lhd C$, then $A \lhd C$.

TRUE FALSE try C= D4 for examples

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

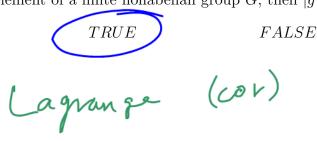
FALSE TRUECan't get lom = 10 for disjoint cycles w/9 elts.

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

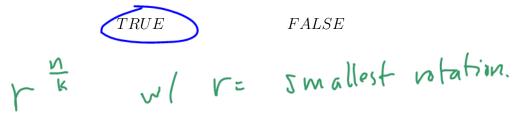


(g) The groups $\mathbb{Z}_{12} \times \mathbb{Z}_{14}$ and $\mathbb{Z}_6 \times \mathbb{Z}_{28}$ are isomorphic.

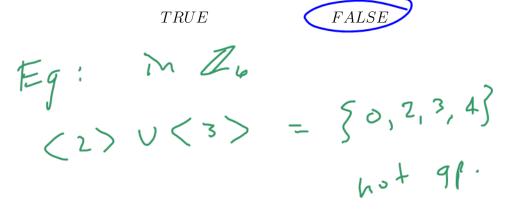
- $(\mathbb{Z}_{3} \times \mathbb{Z}_{4}) \times (\mathbb{Z}_{1} \times \mathbb{Z}_{4}) \quad \text{vs} \quad (\mathbb{Z}_{1} \times \mathbb{Z}_{3}) \times (\mathbb{Z}_{4} \times \mathbb{Z}_{4})$
- (h) If g is an element of a finite nonabelian group G, then |g| divides |G|.



(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.



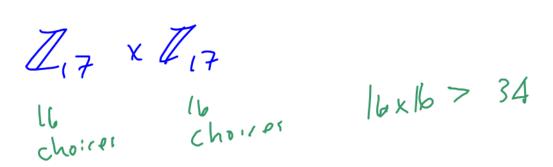
(j) The union of two subrings of a ring R must also be a subring of R.



- 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.

 $P_4 \times \langle (1,2) \rangle$ order 2

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



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

(lots of 5-cycles) 26 ang (a, b, c, de) ang (a, b, c, de) a, b, c, de, au diff

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

$$\begin{cases} \begin{bmatrix} i & 0 \\ 0 & (-i)^{5} \end{bmatrix}, & a \in \{0, 1, 2, 3\} \\ b \in \{0, 1\} \end{bmatrix}$$
(e) A pair of zero divisors in the ring $\mathbb{Z}_{5} \times M_{2}(\mathbb{Z})$.
$$\begin{pmatrix} 0 & 0 & (-i)^{5} \\ 0 & (-i)^{5} \end{pmatrix}, \begin{pmatrix} 1 & 0 & (-i)^{5} \\ 0 & (-i)^{5} \end{pmatrix}, \begin{pmatrix} 0 & 0 & (-i)^{5} \\ 0 & (-i)^{5} \end{pmatrix}, \begin{pmatrix} 0 & (-i)^{5} \\ 0 & (-i)^{5} \end{pmatrix}, \begin{pmatrix} 0 & (-i)^{5} \\ 0 & (-i)^{5} \end{pmatrix}, \begin{pmatrix} 0 & (-i)^{5} \\ 0 & (-i)^{5} \end{pmatrix}, \begin{pmatrix} 0 & (-i)^{5} \\ 0 & (-i)^{5} \end{pmatrix}$$

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

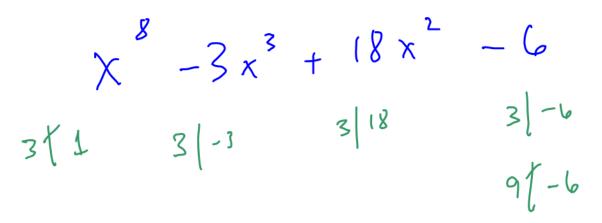
 $\mathcal{I} = \langle x \rangle$ R=Q[x]) $e/z \cong Q$

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

$$F(x) \longrightarrow (f(o), f(1))$$

 $f(x) \in \mathbb{Z}[x].$
one eval him in each coord.

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



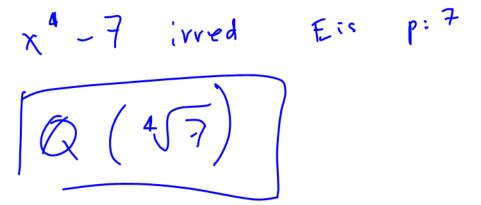
(i) A basis for the field extension $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$, viewed as a vector space over \mathbb{Q} .

 $(1, \sqrt{2}) \times \{1, \sqrt{3}, (\sqrt{3})\}$

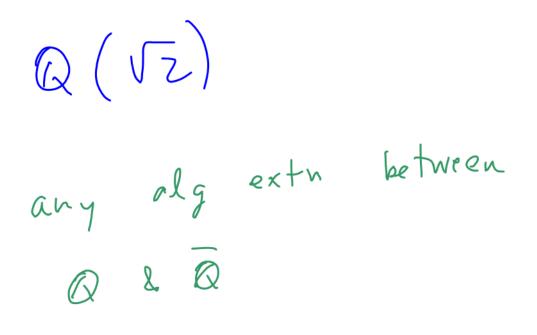
$$= \left\{ 1, \sqrt{2}, \sqrt{35}, \sqrt{2} \cdot \sqrt{5}, (\sqrt{5})^{2} \right\}$$

$$= \left\{ 1, \sqrt{2}, \sqrt{5}, \sqrt{5}, \sqrt{2} \cdot \sqrt{5}, (\sqrt{5})^{2} \right\}$$

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



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



- 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.

 $\langle (3,0), (0,1) \rangle$ J (3a, 6), a, 6: 0, 1, 2]. L'has 9 elements, all w/ order = 3, so by FTFGAG, K must be = Z3 × Z3

(b) (5 points) Viewing G = Z₉ × Z₃ as an additive group, find a subgroup H such that G/H is isomorphic to Z₃ × Z₃. Justify your answer in 1-2 sentences.
Somethy is different for the sentences.

< (3,0)> (a, b) + H all have Cosets (3a, 36)eH order = 3, since Ya, L, and 61/H has 27/3 = 9 elts FTFGAG, S/NS Z3 × Z3

(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.

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

$$= \left\{ (0, \omega), (1, 1), (2, 2), (3, 0), (4, 1), (5, 2), (6, 0), (7, 1), (8, 2) \right\}.$$

$$(8, 2) \left\{ (8, 2) \right\}.$$

$$Subving (closed under (1, 2), (1,$$

(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.

 $\int_{-2}^{2} \{0\} \times \mathbb{Z}_{3}.$ $(3, 0) (3, 0) = (0, 0) \in T,$ $but (3, 0) \notin T.$

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).

 $\beta \in F(\alpha), F(\beta) \in F(\alpha),$ Sin ce Using "chain mle" So we have F(x) for field extus. deg(x, F)= $deg(F, F) \cdot deg(x, F(F))$, deg (β, F) divides deg (α, F) . (2

$$E = p(x) \text{ inred } /_F$$

$$F(x) \quad \text{Let } d = deg \quad p(x) \text{ over } F,$$

$$F = [E:F], so$$

$$d[N.$$

$$Pf \quad hy \quad \text{cont.} \quad \text{Suppose } E \quad \text{contains}$$

$$a \quad \text{zero} \quad d \quad \text{of} \quad p(x).$$

$$Since \quad p(\alpha) = 0 \quad \text{and} \quad p(x)$$

$$is \quad \text{irred.} \quad \text{over} \quad F, \text{ we know}$$

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

$$Then \quad F \in F(\alpha) \leq E, so \quad hy$$

$$"chain \quad rule" \quad for \quad field \quad extns,$$

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

$$n = [E:F], \quad \text{which is imposs},$$

$$So \quad E \quad (avtains \quad no \quad zews \quad if p(x).$$

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 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.

VER St. Frek unit is an element rs = 1. is an element ver st Jser w/ A zen div. w/ rs=0. $w = f(x) \in \mathbb{Z}[x].$ x ~f (x) insider $f(x) \neq 0$, then deg 14 x f(x) = deg f(x) + 1Zis an integral domain. Thus, it is impossible for x.f(x) to ;t can only be o be 1, and so x is neither $i \in f(x) = 0,$ nor a zero div. unit

on pren page. See defs D= int dom. then P.F. Suppose clearly D[x] is comm, and LED is also unity in D[x], viewed as a constant poly. provine need to show D[x] has ho Zero divisors. Suppose F(x), g(x) E D[x] w/ f(x) g(x) = 0. (f ax and bx are the highest degree terms of f 8g, $fhen (ax^n) (bx^m) = ab x^{m+n}$ is the highest deg term of F(x) g(x). This can only be the O poly if ab=0, and since D=nt dom, His weaks a=0 and f(x)=0 or b=0 and f(x)=0, g(x)=0,

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.

$$F: Use rub qp criterion:
non empty
a', b' ettN) = a'b'' \in P(N).$$
Lemma: Since P is = gp hom
 $e \mapsto e'$
 $g^{-1} \mapsto P(g)^{-1} \quad \forall ge G.$
Since $e' \in P[N], \quad P[N] \quad \text{is nonempt}.$
Since $a', b' \in P[N], \quad ig...$
 $a' = P(a), \quad b' = P(b) \quad \text{fsabeG.}$
 $d' = P(a), \quad b' = P(b) \quad \text{fsabeG.}$
Huen $P(a \ b^{-1}) = P(a) P(b^{-1})$
 $= a' (b')^{-1}, \quad \text{so } a'(b)^{-1}$
 $= a' (b')^{-1}, \quad \text{so } a'(b)^{-1}$
 $and \quad P[N] \in G'.$

Pf: Use subgp criterion. 9-1 [N'] e = l'(e'), 50 is nonempty Suppose a, b e e⁻ⁱ[N']. i.e. $\varphi(\alpha), \varphi(b) \in \mathbb{N}'$. $Y(ab^{-1}) = Y(a) Y(b)^{-1}$ then EN', since $\varphi(a), \varphi(b) \in \mathbb{N}'$ $ab' \in \ell'[N'], and$ 50

 $\gamma'[N'] \leq G_1.$

- 9. (Note, this exact question *will* be on the real final.)
 - (a) (5 points) What is your favorite group? Why?

Nant Y \mathcal{N} ence (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. $\backslash |$ answers ADNN