The actual test will consist of a subset of these problems. You will have two hours to complete the test.

Instructions:

- This test will be closed note and closed book.
- In order to receive full credit, you must **show your work.**
- Raise your hand if you have a question.
- Unless told explicitly otherwise, **in each ring there is a multiplicative identity** $1 \neq 0$**.**

On this sample exam, there are many problems which serve as a model for a problem, but where the details may change for the actual comprehensive exam (e.g., polynomials or integers that appear in problem statements may change).

Part 1: Short Answer

Complete each of the exercises in this section. (On the actual comprehensive exam, you'll have approximately five problems to complete.)

1 Consider the cylic group $C_{4900} = \langle x \rangle$ of order $4900 = 2^2 \cdot 5^2 \cdot 7^2$.

(a) Give the number of generators of C_{4900}.

(b) List explicitly the elements x^a, with $0 \leq a \leq 4899$, of order 10.

Answer: $|x^a| = 10$ if $a =$ ____.

(If it helps, you can simply give the prime factorizations of a. I am not interested in your ability to multiply integers.)

2 Consider the cyclic groups $\mathbb{Z}/30\mathbb{Z}$ and $C_{18} = \langle x \rangle$ of orders 30 and 18 respectively, and suppose that

$$\begin{aligned} \varphi_a : \mathbb{Z}/30\mathbb{Z} &\to C_{18} \\ 1 &\mapsto x^a \end{aligned}$$

extends to a well-defined group homomorphism from $\mathbb{Z}/30\mathbb{Z}$ to C_{18}.

(a) List the values of a with $0 \leq a \leq 17$ for which this is true. (I.e. The map defines a well-defined group homomorphism.)

(b) Give a brief explanation why such a well-defined group homomorphism can not be surjective.

3 Consider the symmetric group $G = S_7$ and let $\sigma = (1\ 2\ 3\ 6\ 5\ 4\ 7)$ be a 7-cycle.

(a) Express σ as the product of (not necessarily disjoint) transpositions.

(b) Compute the number of conjugates of σ in S_7.

(c) Let τ be the 7-cycle $(3\ 7\ 1\ 4\ 5\ 6\ 2)$. Give an element α that conjugates σ to τ, i.e. give α such that $\alpha\sigma\alpha^{-1} = \tau$.

(d) Noting that S_7 acts on itself by conjugation, explicitly use the Orbit-Stabilizer theorem to find the size of the stabilizer of σ under this action and the elements of the Stabilizer subgroup of S_7.

The stabilizer of σ in this context is better known as ______________. (Using appropriate notation in place of words here is fine.)

(e) Noting that $\sigma \in A_7$, what is the size of the conjugacy class of σ in A_7? Stated otherwise, how many conjugates in A_7 does σ have? Briefly, state a result that justifies your answer.

Answer: The number of conjugates of σ in A_7 is __________

because ....

4 Suppose that A is an Abelian group of order $200 = 2^3 \cdot 5^2$. Give the isomorphism classes for A in a table below. In the left hand column, give the elementary divisor decomposition and in the right hand column, give the invariant factor decomposition. **Groups on the same row should be isomorphic.** You do not need to show your work.

5 Give the number of non-isomorphic Abelian groups of order $400 = 2^4 \cdot 5^2$.

6 Prove that there are no simple groups of order 56.

7 Give the definition of a nilpotent element in a ring R. Then prove that the set of nilpotent elements in $M_2(\mathbb{Q})$ is **not** an ideal.

8 Suppose G is a non-cyclic group of order $205 = 5 \cdot 41$. Give, with proof, the number of elements of order 5 in G.

9 Find **ALL** solutions x in the integers to the simultaneous congruences.

$$x \equiv 7 \mod 11$$
$$x \equiv 2 \mod 5$$

10 Draw the lattice diagram of prime ideals for the polynomial ring $\mathbb{Q}[x]$. *Note:* There are infinitely many prime ideals so you will need a way to indicate them all.

11 Suppose H a subgroup of G of index 2. Show that $H \triangleleft G$.

12 Suppose $\mathbb{F}$ is a field. Prove that $\mathbb{F}[x]$ is a principal ideal domain.

13 List all abelian groups (up to isomorphism) of order 72.

14 Let G be a group.

(a) Let G be a group, $Z(G)$ the center of G. Prove that if $G/Z(G)$ is cyclic, then G is abelian.

(b) Suppose G is a group of order p^2, where p is a prime. Prove that G is abelian.

(c) Prove that if G is an abelian group of order pq, where p and q are distinct primes, then G is cyclic.

15 Let R be a commutative ring with $1 \neq 0$ whose only ideals are 0 and R. Show that R is a field.

16 List all group homomorphisms from $\mathbb{Z}/40\mathbb{Z}$ to $\mathbb{Z}/60\mathbb{Z}$. Your answer must give a complete list, and indicate your notation clearly. You do not need to justify your answer.

17 Determine the greatest common divisor of 1761 and 1567.

18 Decide which of the following are ring homomorphisms from $M_2(\mathbb{Z})$ to $\mathbb{Z}$:

(a) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a$

(b) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a + d$

(c) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc$

19 Decide which of the following are ideals of the ring $\mathbb{Z} \times \mathbb{Z}$:

(a) $\{(a, a) \mid a \in \mathbb{Z}\}$

(b) $\{(2a, 2b) \mid a, b \in \mathbb{Z}\}$

(c) $\{(2a, 0) \mid a \in \mathbb{Z}\}$

(d) $\{(a, -a) \mid a \in \mathbb{Z}\}$

20 List all group homomorphisms from $\mathbb{Z}/40\mathbb{Z}$ to $\mathbb{Z}/60\mathbb{Z}$. Your answer must give a complete list, and indicate your notation clearly. You do not need to justify your answer.

21 Let A and B be groups. Prove that $A \times B \cong B \times A$.

22 Solve the simultaneous system of congruences

$$x \equiv 3 \mod 16 \qquad x \equiv 9 \mod 25 \qquad y \equiv 42 \mod 49$$

23 Prove:

(a) Any group of order 35 is cyclic.

(b) Any group of order 147 is not simple.

24 Determine the greatest common divisor of 1761 and 1567.

25 Define $\phi : \mathbb{C}^\times \to \mathbb{R}^\times$ by $\phi(a+bi) = a^2+b^2$. Prove that ϕ is a homomorphism and find the image of ϕ. Describe the kernel and fibers of ϕ geometrically (as subsets of the plane).

Recall $S^\times$ is the set $S \setminus \{0\}$ under the usual multiplication operation.

26 Give examples of each of the following or briefly explain why they can't exist:

(a) An integral domain that is not a field.
(b) A non-abelian simple group.
(c) An abelian simple group that is not cyclic.
(d) A non-abelian group with non-trivial center.
(e) A finitely generated abelian group that is not cyclic.
(f) An integral domain that is not a unique factorization domain.
(g) A principal ideal domain that is not a Euclidean domain.
(h) An infinite non-abelian group.
(i) A finite integral domain.
(j) A ring that is not an integral domain, but that is commutative.

27 Prove that if A and B are subsets of G with $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.

28 Let r and s be the usual generators for the dihedral group of order 8. List the elements of D_8 as $1, r, r^2, r^3, s, sr, sr^2, sr^3$ and label these with the integers 1, 2, …, 8 respectively. Exhibit the image of D_8 under the left regular representation of D_8 into S_8.

29 Prove that if G is an abelian group of order pq, where p and q are distinct primes, then G is cyclic.

30 Show that $f(x) = 10x^4 + 6x^3 + 18x^2 + 6x + 21$ and $g(x) = x^3 - 5x + 3$ are irreducible in $\mathbb{Q}[x]$, and that $h(x) = x^3 - 5x + 2$ is reducible.

PART 2: GROUP THEORY

Complete 2 of the following problems. *On the actual comprehensive exam, there will be four problems for you to choose from.*

31 Suppose G is a group with H, K subgroups of G. Prove that if $H \leq N_G(K)$, then $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G.

32 Suppose that a finite group G is of order 105, $|G| = 3 \cdot 5 \cdot 7$, and that G has normal subgroups of order 3, 5 and 7. Prove or disprove: G is cyclic.

33 Let P be a p-group, $|P| = p^a > 1$ for p a prime, and let A be a nonempty finite set. Suppose that P acts on A and define *the set of fixed points* of this action:

$$A_0 = \{a \in A \mid g \cdot a = a \text{ for every } g \in P\}.$$

Prove that

$$|A| \equiv |A_0| \pmod{p}.$$

34 Let $\varphi(n)$ denote the Euler φ-function. Prove that if p is a prime and $n \in \mathbb{Z}^+$, then

$$n \,\Big|\, \varphi(p^n - 1).$$

(Hint: Compute the order of $\bar{p}$ in the appropriate group first.)

35 Prove that if G is a group of order p^2 for p a prime, then G is Abelian.

36 Suppose G is a finite group of order $|G| = 14,553 = 3^3 \cdot 7^2 \cdot 11$ and that N is a normal subgroup of G of order $|N| = 11$. Prove that $N \leq Z(G)$.

37 Suppose G is a group, $H \leq G$, and $\mathrm{Aut}(H)$ the group of automorphisms of H.

(a) Using the First Isomorphism theorem, give a **full** proof of the following statement.
The quotient group $N_G(H)/C_G(H) \cong A \leq \mathrm{Aut}(H)$.

(b) Suppose now that P is a Sylow p-subgroup of S_p for a prime p. Prove that

$$N_{S_p}(P)/C_{S_p}(P) \cong \mathrm{Aut}(P).$$

38 Let G be a finite group of order 22. Prove that G is cyclic or isomorphic to the dihedral group D_{22}.

39 Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

40

(a) Prove that if $\sigma : G \to G$ is the map $\sigma(x) = x^{-1}$ is a homomorphism, then G is an abelian group.

(b) Let G be a finite group which possesses an automorphism σ such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, prove that G is abelian.
Hint: Show that every element of G can be written in the form $x^{-1}\sigma(x)$ and apply σ to such an expression.

41 Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups of A:

(a) $H = \{a^n \mid a \in A\}$

(b) $K = \{a \in A \mid a^n = 1\}$

42 Prove that the subgroup generated by any two distinct elements of order 2 in S_3 is all of S_3.

43 A group H is *finitely generated* if there is a finite set A such that $H = \langle A \rangle$.

(a) Prove that every finite group is finitely generated.

(b) Prove that $\mathbb{Z}$ is finitely generated.

(c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic. [If H is a finitely generated subgroup of $\mathbb{Q}$, show that $H \leq \langle \frac{1}{k} \rangle$, where k is the product of all of the denominators which appear in a set of generators of H.]

(d) Prove that $\mathbb{Q}$ is not finitely generated.

44 Classify groups of order 4 by proving that if $|G| = 4$ then $G \cong Z_4$ or $G \cong V_4$.

45 Let $\phi : G \to H$ be a homomorphism of groups with kernel K and let $a, b \in \phi(G)$. Let $X \in G/K$ be the fiber above a and let Y be the fiber above b, i.e., $X = \phi^{-1}(a), Y = \phi^{-1}(b)$. Fix an element u of X (so $\phi(u) = a$). Prove that if $XY = Z$ in the quotient group G/K and w is any member of Z, then there is some $v \in Y$ such that $uv = w$. [Show $u^{-1}w \in Y$.]

46 Prove that in the quotient group G/N, $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$.

47 Let $\phi : \mathbb{R}^\times \to \mathbb{R}^\times$ be the map sending x to the absolute value of x. Prove that ϕ is a homomorphism and find the image of ϕ. Describe the kernel and fibers of ϕ.

48 Let N be a finite subgroup of G and suppose $G = \langle T \rangle$ and $N = \langle S \rangle$ for some subsets T and S of G. Prove that N is normal in G iff $tSt^{-1} \subseteq N$ for all $t \in T$.

49 The *join* of a non-empty collection of subgroups is the smallest subgroup that contains them all. Prove that the join of any non-empty collection of normal subgroups of a group is a normal subgroup. *Hint: It may be helpful to show that* $g\langle \cup_{i\in I} A_i \rangle g^{-1} = \langle \cup_{i\in I} gA_ig^{-1} \rangle$.

50 Let G be a finite group, let H be a subgroup of G and $N \trianglelefteq G$. Prove that if $|H|$ and $|G : N|$ are relatively prime then $H \leq N$.

51 Let M and N be normal subgroups of G such that $G = MN$. Prove that $G/(M \cap N) \cong (G/M) \times (G/N)$.

52 Prove that if $H \trianglelefteq G$ of prime index p, then for all $K \leq G$ either (i) $K \leq H$ or (ii) $G = HK$ and $|K : K \cap H| = p$.

53 If G is a group of odd order, prove for any nonidentity $x \in G$ that x and x^{-1} are not conjugate in G.

54 Let G be a group of order 203. Prove that if H is a normal subgroup of order 7 in G then $H \leq Z(G)$. Deduce that G is abelian in this case.

55 Let P be a Sylow p-subgroup of H and let H be a subgroup of K. If $P \trianglelefteq H$ and $H \trianglelefteq K$, prove that P is normal in K.

56 If A and B are normal subgroups of G such that G/A and G/B are both abelian, prove that $G/(A \cap B)$ is abelian.

57 Prove that if K is a normal subgroup of G, then $K' = \langle [x, y] \mid x, y \in K \rangle \trianglelefteq G$.

58 A group G is a torsion group if every element has finite order. Prove: If $H \triangleleft G$ and both H and G/H are torsion then G is torsion.

59 Show that a group of order 150 has a normal subgroup of order 5 or 25.

PART 2: RING AND FIELD THEORY

Complete 2 of the following problems. *On the actual comprehensive exam, there will be four problems for you to choose from.*

60 Prove that in a PID every nonzero element is a prime if, and only if, it is irreducible.

61 Suppose R is a commutative ring with 1 and for each $x \in R$, there is a positive integer $n > 1$ so that $x^n = x$. Prove that every nonzero prime ideal is maximal.

62 Let $\mathbb{F}_7$ denote the finite field with 7 elements.

(a) Explicitly construct a finite field with $343 = 7^3$ elements. Explain your work.

(b) The field you constructed in part (a) is a simple extension of $\mathbb{F}_7$ so let α be an element in some extension of $\mathbb{F}_7$ such that $|\mathbb{F}_7(\alpha)| = 343$. Find the inverse of the element $1+\alpha \in \mathbb{F}_7(\alpha)$.

63 Find, with brief justification, all ring homomorphisms from $\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$.

64 Consider the ring of Gaussian integers $\mathbb{Z}[i]$.

(a) Prove that if $\alpha = a + bi$ for $a, b \in \mathbb{Z}$ is a Gaussian integer with $N(\alpha) = p$ for p a prime of $\mathbb{Z}$, then α is irreducible.

(b) List all the units of $\mathbb{Z}[i]$.

(c) Give an example of a prime number $p \in \mathbb{Z}$ such that p is irreducible in $\mathbb{Z}[i]$. Justify your answer by stating an appropriate result.

65 Let F be a field and define the ring $F((x))$ of *formal Laurent series* with coefficients from F by

$$F((x)) = \left\{ \sum_{n \geq N}^{\infty} a_n x^n \mid a_n \in F \text{ and } N \in \mathbb{Z} \right\}.$$

Prove that $F((x))$ is a field.

66 Let R be a ring, U, V ideals of R such that R/U and R/V are commutative with $U \cap V = \{0\}$. Prove that R is commutative.

67 Let R be the ring of all continuous real valued functions on the closed interval $[0, 1]$. Prove that the map $\phi : R \to \mathbb{R}$ defined by $\phi(f) = \int_0^1 f(t)dt$ is a homomorphism of additive groups but not a ring homomorphism.

68 Let R and S be nonzero rings with identity and denote their respective identities by 1_R and 1_S. Let $\phi : R \to S$ be a nonzero homomorphism of rings.

(a) Prove that if $\phi(1_R) \neq 1_S$ then $\phi(1_R)$ is a zero divisor in S. Deduce that if S is an integral domain then every ring homomorphism from R to S sends the identity of R to the identity of S.

(b) Prove that if $\phi(1_R) = 1_S$ then $\phi(u)$ is a unit in S and that $\phi(u^{-1}) = \phi(u)^{-1}$ for each unit u of R.

69 Let I and J be ideals of R.

(a) Prove that $I + J$ is the smallest ideal of R containing both I and J.

(b) Prove that IJ is an ideal contained in $I \cap J$.

(c) Give an example where $IJ \neq I \cap J$.

(d) Prove that if R is commutative and if $I + J = R$ then $IJ = I \cap J$.

70 Assume R is commutative ring with identity $1 \neq 0$ and for each $a \in R$ there is an integer $n > 1$ (depending on a) such that $a^n = a$. Prove that every prime ideal of R is a maximal ideal.

71 Let R be a Euclidean domain. Let m be the minimum integer in the set of norms of nonzero elements of R. Prove that every nonzero element of R of norm m is a unit. Deduce that a nonzero element of norm zero (it such an element exists) is a unit.

72 Let R be a principal ideal domain.

(a) Prove that if P is a prime ideal in R, the P is maximal.

(b) Prove that if M is a maximal ideal of R, then R/M is a field.

(c) Prove that a quotient of a PID by a prime ideal is again a PID.

73 Let $I = (a)$ be a principal ideal in a commutative ring R with 1. Suppose P is a prime ideal such that $P \subsetneq I$. Prove that $P \subset \cap_{n \geq 1} I^n$.

74 Prove that (x, y) and $(2, x, y)$ are prime ideals in $\mathbb{Z}(x, y)$, but only the latter ideal is a maximal ideal.

75 Let F be a finite field. Prove that $F[x]$ contains infinitely many primes.

76 Let $R = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$ be the set of polynomials in x with rational coefficients whose constant term is an integer.

(a) Prove that R is an integral domain and its units are ± 1.

(b) Show that the irreducibles in R are $\pm p$ where p is a prime in $\mathbb{Z}$ and the polynomials $f(x)$ that are irreducible in $\mathbb{Q}[x]$ and have a constant term ± 1. prove that these irreducibles are prime in R.

(c) Show that x cannot be written as the product of irreducibles in R (in particular, that x is not irreducible) and conclude that R is not a UFD.

(d) Show that x is not a prime in R and describe the quotient ring $R/(x)$.

77 Show that the polynomial $(x - 1)(x - 2) \cdots (x - n) - 1$ is irreducible over $\mathbb{Z}$ for all $n \geq 1$. (Hint: If the polynomial factors consider the values of the factors at $x = 1, 2, \ldots, n$.)

78 Prove that $K_1 = \mathbb{F}_{11}[x]/(x^2 + 1)$ and $K_2 = \mathbb{F}_{11}[y]/(y^2 + 2y + 2)$ are both fields with 121 elements. Prove that the map which sends the element $p(\overline{x})$ of K_1 to the element $p(\overline{y} + 1)$ of K_2 (where p any polynomial with coefficients in $\mathbb{F}_{11}$) is well defined and gives a ring (hence field) isomorphism from K_1 to K_2.

79 Let F be a field and let $f(x)$ be a polynomial of degree n in $F[x]$. The polynomial $g(x) = x^n f(1/n)$ is called the *reverse* of $f(x)$. Describe the coefficients of g in terms of the coefficients of f. If $f(0) \neq 0$ prove that f is irreducible iff g is irreducible.

80 Prove that $x^3 + 12x^2 + 18x + 6$ is irreducible over $\mathbb{Z}[i]$.