Logistics: Final Exam will be Thursday May 2 from 1:00-3:00 for in-person students. No notes, books or other aids.

Reminders:

1. Know the **formal definition**. Intuitive definitions are important for understanding but proofs require the use of the formal definition. If you are unsure of the formal definition, ask; don't guess.
2. All proofs should be formal and adhere to the same expectations as your written homework including the use of complete sentences, a clear beginning and conclusion, and appropriate use of symbols.
3. Unless explicitly stated otherwise, all answers require a rigorous explanation.
4. The final is cumulative and may include questions on any of the material from Chapters 1-6, 9-11, 13, 16, 17.

Suggestions:

1. Read over your commented-on homework. If a problem has a circle around the number, you would not have gotten full-credit for that problem. Do you understand why something is marked as incorrect or missing? How can you not make that mistake again?
2. Read over my solutions to the homework. What details in my solutions are absent from yours? Did you and I prove things the same way? If mine was different, does it have any advantages? What are the things from my solutions you want to make sure to include in the future?
3. Make a list of all the examples of groups we have discussed thus far. Which are cyclic or not? Abelian or not? Finite or infinite? Which ones are isomorphic to each other?
4. Look at old Midterms.
5. Look at other problems from the text.

Definitions: equivalence relations, equivalence classes, set operations (intersections, unions, difference, Cartesian product, relations, functions, domain, range, image, one-to-one/injective, onto/surjective, bijective

Chapter 2

Definitions: greatest common divisor, least common multiple, relatively prime, Euclidean algorithm, prime number, composite number

Notation: $gcd(m,n)$

Results:

- Proof by mathematical induction.
- There exist integers r and s such that $ra+sb=gcd(a,b)$

- (Thm 2.9 The Division Algorithm) For every $a, b \in \mathbb{Z}$ such that $b > 0$ there exist unique $q, r \in \mathbb{Z}$, such that $a = qb + r$ where $0 \leq r < b$.
- (Lemma 2.13) Suppose $a, b \in \mathbb{Z}$ and p is a prime. If $p \mid ab$ then $p \mid a$ ore $p \mid b$.
- (Thm 2.15) The prime factorization of an integer is unique up to the order of the primes.

Chapter 3

Definitions: binary operation, associativity, identity, inverse, commutativity, **group**, order of a group, group of symmetries of an object, addition and multiplication modulo n, group of units, general linear group, **subgroup**, proper subgroup, trivial subgroup

Notation: $(\mathbb{Z}, +)$ and with $\mathbb{R}, \mathbb{Q}$, $(\mathbb{Z}_n, +)$, $(U(n), \cdot)$, $GL_n(\mathbb{R})$, $|G|$, $SL_2(\mathbb{R})$

Results:

- If G is a group, then
  - (Prop 3.17) the identity is unique.
  - (Prop 3.18) $\forall a \in G$, a^{-1} is unique.
  - (Props 3.19 and 3.20) $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$ and $(a^{-1})^{-1} = a$.
  - (Prop 3.21) $\forall a, b \in G$, equation $ax = b$ and $xa = b$ have unique solutions.
  - (Prop 3.22) $\forall a, b \in G$, both equations $ab = ac$ and $ba = ca$ imply $b = c$.
- (Thm 3.23) We can use the usual laws of exponents when manipulating repeated group operations on a single element. Specifically, if $g, h \in G$ a group and $m, n \in \mathbb{Z}$, then
  - $g^m g^n = g^{m+n}$
  - $(g^m)^n = g^{mn}$
  - $(gh)^n = ((gh)^{-1})^{-n} = (h^{-1}g^{-1})^{-n}$
- **H is a subgroup of G if and only if**
  - **(Prop 3.30) (i) $e \in H$, (ii) $h_1 h_2 \in H$ for every $h_1, h_2 \in H$, and (iii) $h^{-1} \in H$ for every $h \in H$.**
  - **(Prop 3.31) (i) $H \neq \emptyset$ and (ii)$gh^{-1} \in H$ for every $g, h \in H$.**

Chapter 4

Definitions: Cyclic group, cyclic subgroup, generator of a group, cyclic subgroup generated by a, order of an element of a group, abelian group

Notation: $\langle a \rangle$, $|b|$, $n\mathbb{Z}$

Results:

- (Thm 4.9) Cyclic groups are abelian.
- (Thm 4.10) Every subgroup of a cyclic group is cyclic.

- (Prop 4.12) If $G = \langle a \rangle$ of order n, then $a^k = e$ if and only of $n \,|\, k$.
- (Thm 4.13) If $G = \langle a \rangle$ of order n and $b = a^\ell \in G$, then $|b| = \frac{n}{d}$ where $d = gcd(n, \ell)$.
- (Cor 4.11 of Prop 4.12) The subgroups of $(\mathbb{Z}, +)$ are $\langle 1 \rangle = \mathbb{Z}$, $\langle 2 \rangle = 2\mathbb{Z}$, $\langle 3 \rangle = 3\mathbb{Z}, \cdots$.
- (Cor 4.14 of Thm 4.13) Suppose $1 \leq r < n$. Then, $\mathbb{Z}_n = \langle r \rangle$ if and only if $gcd(n, r) = 1$.

Chapter 5 Section 1

Definitions permutation, the symmetric group on n letters, a permutation group, disjoint cycles, transposition, even/odd permutation, length of a permutation.

Notation: S_X, S_n, permutation notation including disjoint cycle notation and transposition representation,

Results

- (Thm 5.1)The set of all permutations of the set X under function composition is a group.
- (Prop 5.8) Disjoint cycles permute.
- (Thm 5.9) Every permutation can be written as a product of disjoint cycles.
- (Prop 5.12) Any permutation of a finite set can be written as a product of transpositions, provided the set has at least two elements.
- (Thm 5.15) For every permutation σ, the parity (even or odd) of the number of transpositions in any transposition representation of σ is fixed. (i.e. always even or always odd).

More Chapter 5

Definitions: the alternating group, the dihedral group

Notation: A_n, D_n

Results:

- (Thm 5.16, Prop 5.17) $A_n \leq S_n$ and $|A_n| = \frac{1}{2}|S_n|$
- (Thm 5.20, 5.21) $D_n \leq S_n$, $|D_n| = 2n$ and D_n can be generated by a rotation by $360/n$ and a single reflection.

Chapter 6

Definitions: left coset, right coset, coset representative,the **index** of H in G, **Lagrange's Theorem**

Notation: gH and Hg, $[G : H]$,

Results:

- (Lemma 6.3) $H \leq G$ and $g_1, g_2 \in G$. TFAE

- $g_1H = g_2H$
- $Hg_1^{-1} = Hg_2^{-1}$
- $g_1H \subseteq g_2H$
- $g_2 \in g_1H$
- $g_1^{-1}g_2 \in H$

- (Thm 6.4) Left (right) cosets of H in G partition G.
- (Thm 6.8) The number of left cosets of H in G is the same as the number of right cosets of H in G. Consequently the notion of the **index** of H is G is well-defined.
- (Prop 6.9) For $H \leq G$ and $g \in G$, the map $\phi : G \to G$ defined as $\phi(x) = gx$ is a bijection (or, equivalently, ϕ defines a permutation of G). Consequently, for every $H \leq G$ and $g \in G$, $|H| = |gH|$.
- (Thm 6.10, Lagrange's Theorem) $H \leq G$, a finite group. Then
  - $\frac{|G|}{|H|} = [G : H]$, and
  - $|H| \Big| |G|$.
- (Cor 6.11, 6.12, 6.13 Consequences of LT)
  - $\forall g \in G$ finite, $|g| \Big| |G|$.
  - $\forall G$ such that $|G| = p$, a prime, G is cyclic.
  - If $K \leq H \leq G$ finite, then $[G : K] = [G : H][H : K]$.
- (Prop 6.15 that the converse of LT is false) While $6 \Big| A_4$, there does not exist a subgroup of A_4 of order 6.

Chapter 9

Definitions: group G is isomorphic to group H, external direct product, internal direct product

Notation: $G \times H$, $G = HK$

Results:

- (Thm 9.6) $\phi : G \to H$ group isomorphism. TFAE
  - $\phi^{-1} : H \to G$ group isomorphism
  - $|G| = |H|$
  - If one is abelian, the other is abelian
  - If one is cyclic, the other is cyclic
  - If one has a subgroup of order n, then the other has a subgroup of order n.
- (Thm 9.7, 9.7) All infinite cyclic groups are isomorphic to $\mathbb{Z}$ and all cyclic groups of order n are isomorphic to $\mathbb{Z}_n$.

- (Cor 9.9) Every group of prime order p is isomorphic to $\mathbb{Z}_p$.
- (Thm 9.12 Cayley's Theorem) Every group is isomorphic to a group of permutations.
- (Thm 9.17) Let $g \in G$ and $h \in H$ such that $|g| = r$ and $|h| = s$, then the element (g,h) in the group $G \times H$ has order $lcm(r,s)$.
- (Thm 9.27) If G is the internal direct product of H and K, then G is isomorphic to $H \times K$.

Chapter 10

Definitions: **normal subgroup**, factor group or quotient group, simple group

Notation: $N \lhd G$, G/N

Results:

- (Thm 10.3) $N \leq G$. TFAE
  - $N \lhd G$
  - $\forall g \in G$, $gNg^{-1} \subseteq N$
  - $\forall g \in G$, $gNg^{-1} = N$
- (Thm 10.4) If $N \lhd G$, then the set of cosets of N in G form a group of order $[G : N]$ with group operation $(aN)(bN) = abN$.
- (Thm 10.11) A_n is simple for $n \geq 5$.

Chapter 11

Definitions: **group homomorphism**, **group isomorphism**, **kernel**, the canonical homomorphism, automorphism, the group of automorphisms of a group G

Notation: $\ker\phi$

Results:

1. (Proposition 11.4) If ϕ is a group homomorphism, then the identity in the domain is mapped to the identity in the range, $\phi(g^{-1}) = (\phi(g))^{-1}$, the image of a subgroup is a subgroup and the inverse image of a subgroup is a subgroup. Moreover, inverse images also preserve normality.
2. (Theorem 11.5) The kernel of a homomorphism is a normal subgroup of the domain group.
3. (Theorem 11.10, The First Isomorphism Theorem) If $\psi : G \to H$ is a group homomorphism with kernel K and ϕ is the canonical homomorphism, then there exists a unique isomorphism $\eta : G/K \to \phi(G)$ such that $\psi = \eta \circ \phi$.

Chapter 13

Results: Theorem 13.4 The Fundamental Theorem of Finite Abelian Groups

Chapter 16

Definitions: **ring**, **a ring with unity**, a **commutative ring**, **integral domain**, division ring, **unit**, **field**, **subring**, Gaussian integers, **ideal**, **ring homomorphism**, **kernel** of a ring homomorphism, **ring isomorphism**, trivial ideal, **principal ideal**, factor ring, **maximal ideal**, **prime ideal**

Notation: R/I

Results:

1. (Prop 16.8) R is a ring with $a,b \in R$, then (1) $a0 = 0a = a$, (2) $a(-b) = (-a)b = -(ab)$, and (3) $(-a)(-b) = ab$.
2. (Prop 16.10) R a ring and $S \subseteq R$. We can show that S is a subring of R by demonstrating three things: (1) $S \neq \emptyset$, (2) $\forall a,b \in S,\ ab \in S$, and (3) $\forall a,b \in S,\ a-b \in S$.
3. (Prop 16.15 Cancellation Law) If R is a commutative ring with unity, the being an integral domain is equivalent to the existence of a cancellation law. (ie $a\ \emptyset$ and $ab = ac$ implies $b = c$)
4. (Thm 16.16) Every finite integral domain is a field.
5. (Prop 16.22) Given a ring homomorphism f, then (1) f preserves commutativity, (2) $f(0) = 0$, (3) $f(1) = 1$ provided f is onto, and f preserves being a field provided f is not the trivial homomorphism.
6. (Prop 16.27) The kernel of a ring homomorphism is an ideal.
7. (Thm 16.29) Let I be an ideal of ring R. The factor group R/I is a ring under the multiplicative operation $(a+I)(b+I) = ab+I$.
8. (Thm 16.30) I an ideal of ring R and $f : R \to R/I$ is defined as $f(r) = r+I$. Then f is a ring homomorphism from R onto R/I with kernel I.
9. (Thm 16.31) The First (Ring) Isomorphism Theorem. If $\psi : R \to S$ is a group homomorphism with kernel I and ϕ is the canonical homomorphism, then there exists a unique isomorphism $\eta : R/I \to \phi(R)$ such that $\psi = \eta \circ \phi$.
10. (Thm 16.35) R is commutative with unity and M is an ideal. Then, M is maximal if and only if R/M is a field.
11. (Prop 16.38) Suppose R is commutative with unity where $1 \neq 0$. Then P is prime if and only if R/P is an integral domain.

New Topics
Chapter 17

Definitions: polynomial over the ring R, coefficient, leading coefficient, monic, degree, **irreducible**

Notation: $R[x]$

Results:

1. (Thm 17.3) If R is commutative with unity, then $R[x]$ is commutative with unity.
2. (Thm 17.4) If R is an integral domain, then $R[x]$ is an integral domain and $\forall f(x), g(x) \in R[x]$, $deg(fg) = deg(f) + deg(g)$.
3. (Thm 17.6) The Division Algorithm
4. (Cor 17.8) Let F be a field, $\alpha \in F$, and $p(x) \in F[x]$.

$$p(\alpha) = 0 \Leftrightarrow (x - \alpha) \text{is a factor of } p(x)$$

5. (Cor 17.9) F field, $p(x) \in F[x]$ of degree n, and $p(x) \neq 0$. Then $p(x)$ has at most n zeros in F.
6. (Thm 17.20) If F is a field, then every ideal in $F[x]$ is a principle ideal.
7. (Thm 17.22) Let F be a field and $p(x) \in F[x]$.
   $\langle p(x) \rangle$ is maximal $\Leftrightarrow$ $p(x)$ is irreducible.