Besides the topics in the review for the Midterm, see Hw 6, the following topics may appear in the Final Exam

I. Homomorphisms and Quotient Groups. Define normal subgroups.

1. Show that $H \leq G$ is always normal in $N_G(H)$. In particular $N \leq G$ if and only if $N_G(N) = G$.

2. Let $H \leq G$. Consider the relation $u \sim v$ if and only if $v^{-1}u \in H$. Show that it is an equivalence relation and the equivalence classes (i.e. left cosets) are sets of the form $uH = \{uh \mid h \in H\}$, $u \in G$.

3. State and prove Lagrange’s Theorem.

4. If $G$ is a finite group then $|x|$ divides $|G|$ for any $x \in G$. Moreover if $|G|$ is prime then $G$ is cyclic.

5. Show that if $H \leq G$ and $|G : H| = 2$ then $H \leq G$.

6. Give an example for which $H \leq K \leq G$ but $H$ is not a normal subgroup of $G$.

7. Let $H, K \leq G$ be finite subgroups and $HK = \{hk \mid h \in H, k \in K\}$. Show that $|HK| = |H||K|/|H \cap K|$. Moreover there are exactly $|H \cap K|$ number of distinct ways $y \in HK$ can be written as $y = hk$, $h \in H, k \in K$.

8. If $H, K \leq G$, then $HK \leq G$ if and only if $HK = KH$. In particular if one of the subgroups is normal in $G$ then their product is a subgroup.

9. If $N \leq G$ show that $xN \cdot yN = xyN$ is a well defined operation on left cosets of $N$ if and only if $N \trianglelefteq G$. In the latter case show that the left cosets form a group with respect to the above operation called the quotient group.

10. Define homomorphisms and isomorphisms between groups. Define the group of automorphisms of a group.
11. Given a homomorphism $\phi : G_1 \rightarrow G_2$ where $G_{1,2}$ are groups, show that:
   (a) $\phi(H) \leq G_2 \forall H \leq G_1$;
   (b) $\phi^{-1}(K) \leq G_1 \forall K \leq G_2$;
   (c) $\ker \phi \trianglelefteq G_1$;
   (d) If $N \trianglelefteq G_1$ then $\phi(N) \trianglelefteq \phi(G_1)$; give an example when $\phi(N)$ is not normal in $G_2$;
   (e) If $K \trianglelefteq G_2$ then $\phi^{-1}(K) \trianglelefteq G_1$.

12. Define the Alternating Subgroup of a group of permutations. Show that $A_n \trianglelefteq S_n$, $n \in \mathbb{N}$.

13. State and prove the four Isomorphism Theorems for groups.


15. Define simple groups and composition series.

16. Prove the existence and uniqueness (modulo a permutation) of composition series for finite groups (Jordan - Hölder Theorem).

II. Group Actions Define transitive actions.

1. Show that the orbit of an element under a group action has the same cardinality as the index of the stabilizer of the element.

2. Define the left multiplication action of a group on itself and on left cosets of one of its subgroups.

3. Show that the above actions are transitive and find their kernels.

4. State and prove Cayley’s Theorem.

5. Show that if $p$ is the smallest prime dividing $|G|$ and $N \leq G$, $|G : N| = p$ then $N \trianglelefteq G$.

6. Define the conjugation action of a group on itself and on its subsets and find the stabilizers and kernels.

7. State and prove the Class Equation.

8. Show that if $|G| = p^\alpha$, $p$ prime then $Z(G) \neq 1$. Moreover if $\alpha = 2$ then $G$ is abelian and $G \cong Z_{p^2}$ or $G \cong Z_p \times Z_p$.

9. Consider $H \trianglelefteq G$, show that $G$ acts by conjugation on $H$ and it induces a homomorphism from $G$ to $Aut(G)$. Find the kernel of this action. What happens when $H = G$?
10. Define $\text{Inn}(G)$ and show that $G/Z(G) \cong \text{Inn}(G)$.

11. Define characteristic subgroups and show that
   (a) characteristic subgroups are normal;
   (b) if $H$ is the unique subgroup of $G$ of given order then $H \text{ char } G$;
   (c) if $H \text{ char } H \leq G$ then $H \leq G$.

12. Let $p$ be a prime and $G$ a finite group with $p | |G|$. Define $p-$subgroups and $p-$Sylow subgroups.


14. Show that any simple group of order 60 must be isomorphic with $A_5$, in particular show that $A_5$ is simple.


16. Show that $A_n$, $n \geq 5$ is simple.

III. Rings Define rings, rings with identity, commutative rings, zero divisors, units, integral domains, fields and subrings.

1. Show that in a ring $R$:
   (a) $0a = a0 = 0$, $\forall a \in R$;
   (b) $(-a)b = a(-b) = -(ab)$, $\forall a, b \in R$;
   (c) $(-a)(-b) = ab$, $\forall a, b \in R$;
   (d) if $a$ is not a zero divisor then $ab = ac$ implies $b = c$ and $ba = ca$ implies $b = c$ for all $b, c \in R$;
   (e) if $R$ has identity 1, then the identity is unique, units have a unique inverse, and $-a = (-1)a$.

2. Show that any finite integral domain is a field.

3. Define the polynomial ring over a commutative ring $R$. Show that if $R$ is an integral domain then so is $R[x]$, and the units of $R[x]$ are the units of $R$.

4. Define homomorphisms of rings. State and prove similar properties to I.11.

5. Let $I$ be a subring of $R$. Show that multiplication of left cosets of $I$ is well defined if and only if $I$ is an ideal. In the latter case show that $R/I$ is a ring called the quotient ring.
6. State and prove the four Isomorphism Theorems for rings.

7. Show that \( \mathbb{Z}[x]/n\mathbb{Z}[x] \cong (\mathbb{Z}/n\mathbb{Z})[x] \).


9. Let \( R \) be a ring with identity, \( A \subseteq R \). Show that the set:

\[
RAR = \{ r_1a_1l_1 + r_2a_2l_2 + \ldots + r_na_nl_n \mid n \in \mathbb{N}, a_i \in A, r_i, l_i \in R, \forall i = 1, 2, \ldots n \}
\]

is the smallest ideal containing the set \( A \), called the ideal generated by \( A \). How does the above formula simplifies when \( R \) is commutative?

10. Show that in a ring with identity an ideal which contains a unit must be the entire ring. Deduce that a field can only have trivial ideals.

11. Define maximal ideals and show that in a commutative ring an ideal is maximal if and only if its quotient ring is a field.

12. Define prime ideals in a commutative ring and show that an ideal is prime if and only if its quotient is an integral domain.

13. Show that any maximal ideal in a commutative ring is a prime ideal.

14. Show that \((x)\) is a prime ideal in \( \mathbb{Z}[x] \), but not maximal, while \((x)\) is a maximal ideal hence also prime in \( \mathbb{Q}[x] \).

15. Let \( R \) be a commutative ring and \( D \subset R \) be a nonempty subset, closed under multiplication which has does not contain zero or any zero divisor. Define the ring of fractions of \( D \) with respect to \( R \), and show its existence and uniqueness. If \( R \) is an integral domain define and show the existence and uniqueness of its field of fractions.

16. Show that \( \mathbb{Q} \) is the field of fractions of both \( \mathbb{Z} \) and \( 2\mathbb{Z} \).

17. Show that the field of fractions for \( \mathbb{Z}[x] \) is isomorphic with the field of fractions for \( \mathbb{Q}[x] \). Note that this field is called the field of rational functions.


20. Show that $\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{a_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_n^{a_n}\mathbb{Z})$, where $n = p_1^{a_1}p_2^{a_2} \cdots p_n^{a_n}$. Deduce that the Euler function satisfies $\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \cdots \phi(p_n^{a_n}) = p_1^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1) \cdots p_n^{a_n-1}(p_n-1)$.


22. Define divisors and the greatest common divisor in a commutative ring. Show that in a commutative ring with identity $d|a$ if and only if $a \in (d)$ and $d = g.c.d(a,b)$ if and only if $(a,b) \subseteq (d)$ and $(a,b) \subseteq (d')$ implies $(d) \subseteq (d')$. Moreover in an integral domain two greatest common divisors can only differ by (multiplication by) a unit.

23. Define Euclidian domains. Show that in an Euclidian domain any ideal is principal.

24. Show that every two elements in an Euclidian domain have a greatest common divisor which is is the last nonzero reminder in the Euclidian Algorithm.

25. Show that $\mathbb{Q}[x]$ is an Euclidian domain. What is the greatest common divisor of $x^3$ and $x^2 + 1$?

26. Show that $(2,x)$ is not a principal ideal in $\mathbb{Z}[x]$. What is the greatest common divisor of 2 and $x$? Deduce that $\mathbb{Z}[x]$ is not an Euclidian domain.

27. Textbook pages 278 - 279 Exercises: 4, 5, 6, 11, 12.