Exam 3 will be on Monday, November 19, 2018. The syllabus for this exam is Chapter 11, Section 13.1, and Chapter 16 in Judson.

You should be sure to know precise definition of the terms we have used, and you should know precise statements (including all relevant hypotheses) for the main theorems proved. Know the following terms or phrases, including definitions, and results. Some are repeated for convenience from earlier sections.

- A function $f : G \to H$ between groups G and H is a homomorphism if $f(ab) = f(a)f(b)$ for all a, $b \in G$. Some properties of homomorphisms are: $f(1) = 1$, $f(a^{-1}) = (f(a))^{-1}$, $f(a^k) = (f(a))^k$ for all $k \in \mathbb{Z}$.
- A bijective homomorphism $f : G \to H$ is an isomorphism.
- Kernel of a group homomorphism
- Normal subgroup
- Right and left cosets of a subgroup H of a group G.
- The index $[G : H]$ of a subgroup H in a group G.
- Let H be a subgroup of a group G and let a, $b \in G$. Then the following are properties of the cosets of H:
    1. $Ha = H$ if and only if $a \in H$.
    2. $Ha = Hb$ if and only if $ab^{-1} \in H$.
    3. If $a \in Hb$, then $Ha = Hb$.
    4. Either $Ha = Hb$ or $Ha \cap Hb = \emptyset$.
    5. The distinct right (left) cosets of H are a partition of G, and if the order of G is finite, then the number of right (left) cosets is $|G|/|H|$.
- If G is a group and H is a subgroup, then H is a normal subgroup if $gH = Hg$ for all $g \in G$.
- A subgroup H of G is normal if and only if $gHg^{-1} \subseteq H$ for all $g \in G$.
- If G is a group, then then subgroups $\{1\}$, G and $Z(G) =$ the center of G, are always normal subgroups of G.
- If G is abelian, then every subgroup of G is normal in G.
- If H is a subgroup of index 2 in G, then H is normal in G.
- If K is a normal subgroup of G, then $Ka \cdot Kb = Kab$ is a well defined multiplication of right (=left) cosets. In this case the set $G/K = \{Ka : a \in G\}$ of right (=left) cosets of K forms a group under this multiplication. Some of the properties of this group G/K are:

1. The group operation is $(Ka)(Kb) = Kab$.
2. The identity of G/K is the coset K.
3. The inverse of Ka is Ka^{-1}, i.e., $(Ka)^{-1} = Ka^{-1}$.
4. The exponent rule in G/K is $(Ka)^n = Ka^n$.
5. The order of Ka is the smallest positive power n such that $a^n \in K$.
6. The mapping $\varphi : G \to G/K$ defined by $\varphi(a) = Ka$ is a surjective group homomorphism.
7. If G is abelian, then G/K is abelian.
8. If $G = \langle a \rangle$ is cyclic, then G/K is also cyclic; in fact $G/K = \langle Ka \rangle$
9. If G is finite, then $|G/K| = |G|/|K| = [G : K]$.

- If $\alpha : G \to H$ is a group homomorphism, the (1) $\alpha(G)$ is a subgroup of H, and (2) $\mathrm{Ker}(\alpha)$ is a *normal* subgroup of G.
- ***Isomorphism Theorem for Groups.*** If $\alpha : G \to H$ is a group homomorphism, then $\alpha(G) \cong G/\operatorname{Ker}(\alpha)$.
- Know the criterion for an abelian group G to be the internal direct product of subgroups H and K. Specifically, G is the internal direct sum of H and K provided $HK = \{hk : h \in H,\, k \in K\}$ and $H \cap K = \{1\}$. In this case G is isomorphic to the external direct product $H \times K$ via the isomorphism $\phi : H \times K \to G$ given by $\phi(h, k) = hk$.
- ***Fundamental Theorem of Finite Abelian Groups.*** Every finite abelian group G is isomorphic to a direct product of cyclic groups of prime power order.
- Ring, commutative ring.
- Subring
- ***Subring Test.*** A subset S of a ring R is a subring if and only if
  1. $0 \in S$.
  2. If $s \in S$ and $t \in S$, then $s + t$, st, and $-s$ are all in S.
- Units in a ring
- Characteristic of a ring.
- Division Ring
- Field
- A ring R is an *integral domain* if R is commutative with identity, $1 \neq 0$, and $ab = 0 \implies a = 0$ or $b = 0$.
- A subring of a field is an integral domain.

- The characteristic of any domain is either 0 or a prime.
- Every finite integral domain is a field.
- An *ideal* of a ring R is an additive subgroup A such that $Ra \subseteq A$ and $aR \subseteq A$ for all $a \in A$. Thus, to check that a nonempty $A \subset R$ is an ideal, it is necessary to check:
  1. If a, $b \in A$ then $a \pm b \in A$.
  2. If $a \in A$ and $r \in R$, then $ra \in A$ and $ar \in A$.
- Let A be an ideal of the ring R. Then the additive factor group R/A becomes a ring with the multiplication $(r + A)(s + A) = rs + A$. The unity of R/A is $1 + A$, and R/A is commutative if R is commutative (but R/A can be commutative without R being commutative).
- Let A is an ideal of a ring R, then the ideals of R/A are all of the form B/A where B is an ideal of R containing A. (Theorem 4, page 183).
- If R is commutative and $a \in R$, then $Ra = \{ra | r \in R\}$ is an ideal of R called the *principal ideal generated by a.*
- An ideal P of a commutative ring R is a *prime ideal* if $P \neq R$ and P has the property:

$$\text{If } rs \in P, \text{ then } r \in P \text{ or } s \in P.$$

- An ideal M of a ring R is *maximal* if $M \neq R$ and the only ideals A such that $M \subseteq A \subseteq R$ are $A = M$ and $A = R$.
- The only ideals of a division ring R are $|set0$ and R.
- If R is a commutative ring, an ideal $P \neq R$ is a prime ideal if and only if R/P is an integral domain.
- If R is a commutative ring, an ideal A of R is maximal if and only if R/A is a field.
- If R is a commutative ring, then every maximal ideal is a prime ideal.
- If R is a ring, then the ideals of the matrix ring $M_n(R)$ are all of the form $M_n(A)$ where A is an ideal of R.
- If R and S are rings, a map $\theta : R \to S$ is a *ring homomorphism* if for all r and $r_1 \in R$:
  1. $\theta(r + r_1) = \theta(r) + \theta(r_1)$.
  2. $\theta(rr_1) = \theta(r)\theta(r_1)$.
- If $\theta : R \to S$ is a ring homomorphism, then
  1. $\theta(R)$ is a subring of S.
  2. $\mathrm{Ker}(\theta)$ is an ideal of R.

- ***Isomorphism Theorem for Rings.*** If $\theta : R \to A$ is a ring homomorphism, then $\theta(R) \cong R/\operatorname{Ker}(\theta)$, via the ring isomorphism $\overline{\theta} : R/\operatorname{Ker}(\theta) \to \theta(R)$ given by $\overline{\theta}(r + \operatorname{Ker}(\theta)) = \theta(r)$.
- ***Chinese Remainder Theorem.*** Let A and B be ideals of a ring R.
  1. If $A + B = R$ then $R/(A \cap B) \cong R/A \times R/B$.
  2. If $A + B = R$ and $A \cap B = 0$ then $\cong R/A \times R/B$.
- If m and n are relatively prime, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Here the isomorphism is an isomorphism of rings.

Review Exercises

1. Let N be a normal subgroup of prime index p in a group G. Explain why the quotient group G/N is cyclic.
2. List the cosets of $\langle 7 \rangle$ in $\mathbb{Z}_{16}^*$. Is the quotient group $\mathbb{Z}_{16}^*/\langle 7 \rangle$ cyclic?
3. Let $\mathbb{R}$ be the additive group of the real numbers, $\mathbb{Z}$ its cyclic subgroup
$$\langle 1 \rangle = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$
and let W be the quotient group $\mathbb{R}/\mathbb{Z}$.
   (a) What is the order of the coset $(-2/5) + \mathbb{Z}$ in the group W?
   (b) Use the fact that $\sqrt{3}$ is irrational to show that the coset $\sqrt{3} + \mathbb{Z}$ does not have finite order in the group W.
4. If $G = \mathbb{Z}_6 \times \mathbb{Z}_4$ let $H = \{(0,0), (0,2)\}$ and $K = \{(0,0), (3,0)\}$.
   (a) Check that H and K are subgroups of G.
   (b) List all of the cosets of H. List all of the cosets of K.
   (c) What is the isomorphism class of G/H?
   (d) What is the isomorphism class of G/K?
5. Give a complete list of the distinct isomorphism classes of abelian groups of order 600.
6. Are the groups $\mathbb{Z}_5 \times \mathbb{Z}_{10} \times \mathbb{Z}_{25} \times \mathbb{Z}_{36} \times \mathbb{Z}_{54}$ and $\mathbb{Z}_{50} \times \mathbb{Z}_{108} \times \mathbb{Z}_{450}$ isomorphic?
7. What is the isomorphism type of the group $U(20)$ (the group of units of the ring $\mathbb{Z}_{20}$).
8. Two of the following groups of order 864 are isomorphic. Which are the two?
   (a) $\mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_{36}$
   (b) $\mathbb{Z}_3 \times \mathbb{Z}_{12} \times \mathbb{Z}_{24}$
   (c) $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_9$

9. Which of the following are subrings of the field $\mathbb{R}$ of real numbers.
   (a) $A = \left\{m + n\sqrt{2} | m,\ n \in \mathbb{Z} \text{ and } n \text{ is even}\right\}$
   (b) $B = \left\{m + n\sqrt{2} | m,\ n \in Z \text{ and } m \text{ is odd}\right\}$
10. Consider the following conditions on the set of all 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with rational entries. Which conditions below define a commutative ring? If the set is a ring, find all units.
    (a) All matrices with $d = a$, $c = b$.
    (b) All matrices with $a = 0$ and $d = 0$.
11. An element a of a commutative ring R is called **nilpotent** if $a^n = 0$ for some positive integer n. Prove that if u is a unit and a is nilpotent, then $u - a$ is a unit in R.
12. Define $\phi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ by $\phi(m + n\sqrt{2}) = m - n\sqrt{2}$, for all $m,\ n \in \mathbb{Z}$. Show that ϕ is an isomorphism of $\mathbb{Z}[\sqrt{2}]$ with itself.
13. What is the characteristic of the ring $\mathbb{Z}_m \oplus \mathbb{Z}_n$?
14. In the ring $\mathbb{Z}[i]$ of Gaussian integers let $\langle p \rangle$ be the ideal generated by a prime number. Show that $\mathbb{Z}[i]/\langle p \rangle$ has p^2 elements, and has characteristic p.
15. In the ring of Gaussian integers show that the ideal $\langle 5 - i \rangle$ is not a prime ideal.

    Hint: Show that $\mathbb{Z}[i]/\langle 5 - i \rangle \cong \mathbb{Z}_{26}$ by defining an onto ring homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}[pi]/\langle 5 - i \rangle$ by $\phi(n) = n + \langle 5 - i \rangle$.