Exam 2 will be on Friday, October 19, 2016. The syllabus for this exam is Chapters 4, 5, 6, 9, 10 in Judson, plus the cyclic group supplement.

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. Here are some items for you to focus on:

1. Know the following terms or phrases, including definitions.
   (a) Order of a group
   (b) Order of an element in a group
   (c) Subgroup
   (d) Subgroup generated by the set (denoted $\langle S \rangle$)
   (e) Center of a group $Z(G)$.
   (f) Conjugates of a subgroup H: gHg^{-1}.
   (g) Cyclic group
   (h) Isomorphism of groups
   (i) Homomorphism of groups
   (j) $\mathbb{Z}_n$ is a group under what operation?
   (k) $\mathbb{Z}_n^*$ is a group under what operation?
   (l) S_n is a group under what operation?
   (m) Know the description of the *dihedral group* D_n by means of generators and relations:

$$\begin{aligned} D_n &= \langle a, b | a^n = e, b^2 = e, bab = a^{-1} \rangle \\ &= \left\{ e, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1} \right\}. \end{aligned}$$

   (n) What is $\mathrm{GL}_n(\mathbb{R})$ and what operation makes it into a group?
   (o) Direct product $G_1 \times G_2$ of groups G_1 and G_2.
   (p) Kernel of a group homomorphism $\sigma : G \to H$. $(= \{a \in G : \sigma(a) = e\}$
   (q) Normal subgroup
   (r) Right and left cosets of a subgroup H of a group G.
   (s) The index $[G : H]$ of a subgroup H in a group G.

2. Here are some skills or theorems that you should know. For convenience, some of the facts that you learned earlier, and which are frequently used, are repeated here.
   - Know how to write a permutation in S_n as a product of disjoint cycles and know how to use this factorization to find the order of a permutation.
   - S_n is the group of permutations of the set $\{1, 2, \ldots, n\}$. $|S_n| = n!$
   - A_n is the group of even permutations in S_n. $|A_n| = (n!)/2$

- Every permutation is a product of disjoint cycles.
- A transposition is a cycle of length 2. Every permutation is a product of transpositions. The number of transpositions in such a product for a permutation σ is always even or always odd. σ is even if it is a product of an even number of transpositions; σ is odd if it is a product of an odd number of transpositions.
- An r-cycle $(j_1, j_2, \ldots, j_r)$ is an even permutation if r is odd and it is odd if r is even. This follows from the factorization

$$(j_1\ j_2\ \ldots\ j_r) = (j_1\ j_r)(j_1\ j_{r-1})\cdots(j_1\ j_2).$$

- A group G is cyclic if $G = \langle a \rangle$, i.e., if every element of G is a power of a.
- If $a \in G$, then the order of a, denoted $o(a)$, is the smallest natural number n such that $a^n = e$. Also, $o(a) = |\langle a \rangle|$.
- Lagrange's Theorem: If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.
- If $a \in G$, then $o(a)$ divides $|G|$.
- If $a \in G$, then $a^m = 1$ if and only if $o(a)$ divides m.
- If $a \in G$ has infinite order, then $a^m = a^k$ if and only if $k = m$.
- If $a \in G$ has finite order $o(a) = n$, then $a^m = a^k$ if and only if $k \equiv m \pmod{n}$.
- If $(a, b) \in G_1 \times G_2$, then $o((a, b)) = \text{lcm}[o(a), o(b)]$.
- If $\sigma \in S_n$ is an r-cycle, then $o(\sigma) = r$.
- If $\sigma = \gamma_1\gamma_2\cdots\gamma_k$ is the disjoint cycle factorization of $\sigma \in S_n$, then $o(\sigma) = \text{lcm}(o(\gamma_1), \ldots, o(\gamma_k))$.
- If $|G|$ is prime, then G is cyclic.
- The subgroups of $\mathbb{Z}$ are the subsets $m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$.
- Every subgroup of a cyclic group is cyclic.
- If G is an infinite cyclic group, then G is isomorphic to $\mathbb{Z}$.
- If G is a cyclic group of finite order n, then G is isomorphic to $\mathbb{Z}_n$.
- 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.
- If $\alpha : G \to H$ is a homomorphism and $a \in G$ has finite order, then $o(\alpha(a))$ divides $o(a)$.
- If $\alpha : G \to H$ is an isomorphism and $a \in G$ has finite order, then $o(\alpha(a)) = o(a)$.
- Two groups G and H are isomorphic if there is an isomorphism $f : G \to H$.
- $U(m) = \{r \in \mathbb{Z}_m : (r, m) = 1\}$. $U(m)$ is a group under multiplication modulo m. under multiplication modulo m. If p is prime then $\mathbb{Z}_p^*$ is a group of order $p - 1$.
- In general $|U(m)| = \varphi(m)$, where $\varphi(m)$ denotes Euler's φ-function.

- $\mathbb{Z}_{mn} \equiv \mathbb{Z}_n \times \mathbb{Z}_m$ if m and n are relatively prime.
- Let $G = \langle a \rangle$ be a finite cyclic group of order n.
  (a) If d is a divisor of n the order of a^d is $o(a^d) = n/d$. More generally, $o(a^k) = n/m$ where $m = \gcd(k, n)$.
  (b) a^m generates G if and only if $\gcd(m, n) = 1$. (Hence, the number of generators of a cyclic group G of order n is $\varphi(n)$.
  (c) If H is any subgroup of G then $H = \langle a^k \rangle$ for some divisor k of n.
  (d) If m and k are divisors of n, then $\langle a^m \rangle \subseteq \langle a^k \rangle$ if and only if $k|m$.
- Know Langrange's Theorem
- Know Euler's Theorem (Section 6.3) and how to prove it using Lagrange's Theorem.

Review Exercises

1. List all of the elements of $G = U(15)$. Show that $G = \langle 2, 13 \rangle$, that is, show that G is generated by 2 and 13. Is G a cyclic group?

   ▶ **Solution.** $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$. To see that $G = \langle 2, 13 \rangle$, note that $1 = 2^0$, $2 = 2^1$, $4 = 2^2$, $8 = 2^3$, $13 = 13^1$, $7 = -8 = (-2)^3 = 13^3$, $11 = 2 \cdot 13$, $14 = 8 \cdot 13$. Thus, $G \subseteq \langle 2, 13 \rangle$, and the other inclusion $\langle 2, 13 \rangle \subseteq G$ is clear. Hence, $G = \langle 2, 13 \rangle$. G is not cyclic since $o(2) = 4$, $13 = -2$ which implies that $o(13) = 4$ also. The elements not in $\langle 2 \rangle$ or $\langle 13 \rangle$ are 11 which has order 2 and $14 = -1$ which also has order 2. Thus, $\mathbb{Z}_{15}^*$ has 1 element of order 1, namely 1, 4 elements of order 4: 2, 8, 13, 7; and 3 elements of order 2: 4, 11, and 14. Since $|G| = 8$ and G does not have an element of order 8, it follows that G is not cyclic. ◀

2. Is the group $U(13)$ a cyclic group? *Hint:* What is the order of the element 2 in the group $U(13)$?

   ▶ **Solution.** Since 13 is prime, $|U(13)| = 13 - 1 = 12$. Since $o(2)|12$, the possible orders for 2 are 1, 2, 3, 4, 6, and 12. Since $2^4 = 16 = 3 \neq 1$ and $2^6 = 64 = -1 \neq 1$ it follows that 1, 2, 3, 4, and 6 are excluded as possible orders for 2. Hence $o(2) = 12$ and $U(13)$ is cyclic with generator 2. ◀

3. Prove that $H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in \mathbb{Z} \right\}$ is a cyclic subgroup of $\mathrm{GL}_2(\mathbb{R})$.

   ▶ **Solution.** Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Then, (by a simple induction argument) $A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ for all $n \in \mathbb{Z}$. Hence, $H = \langle A \rangle$, and H is a cyclic group (of infinite order) generated by A. ◀

4. Explain why $\mathbb{Z}_6$ and S_3 are not isomorphic.

▶ **Solution.** A group isomorphism $\varphi : G \to H$ must preserve the abelian property. That is, if G and H are isomorphic and G is abelian, then so is H. Since $\mathbb{Z}_6$ is abelian, but S_3 is not, it follows that they cannot be isomorphic. ◀

5. Let $G = \langle a \rangle$ where $o(a) = 30$ and let $H = \langle a^4 \rangle$. What is $|H|$?

▶ **Solution.** $|H| = o(a^4)$ The order of a^4 is the smallest n such that $(a^4)^n = e$, i.e., the smallest n such that $a^{4n} = 3$. Since $o(a) = 30$, this means that n is the smallest positive integer such that $30|4n$. Thus, $n = 15$ and $|H| = 15$. ◀

6. Let $G = \langle a \rangle$ and let $H = \langle a^{12}, a^{20} \rangle$. Find a generator for H.

▶ **Solution.** $H = \langle a^{12}, a^{20} \rangle = \left\{ (a^{12})^k (a^{20})^l : k,\ l \in \mathbb{Z} \right\} = \left\{ a^{12k+20l} : k,\ l \in \mathbb{Z} \right\}$. Since $I = \{12k + 20l : k,\ l \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$, it is cyclic, generated by the greatest common divisor of 12 and 20. Thus, $I = (12,\ 20)\mathbb{Z} = 5\mathbb{Z}$, and $H = \langle a^5 \rangle$. ◀

7. Let $G = \mathbb{Z}_4 \times \mathbb{Z}_4$ and let H be the cyclic subgroup generated by (3, 2). List all of the elements of H.

▶ **Solution.** $H = \{(0,\ 0),\ (3,\ 2),\ (2,\ 0),\ (1,\ 2)\}$ ◀

8. List all of the subgroups of $\mathbb{Z}_{12}$.

▶ **Solution.** $\mathbb{Z}_{12}$ is cyclic, so the subgroups are cyclic and are in one-to-one correspondence with the divisors of 12. Thus, the subgroups are:

$$\begin{aligned} H_1 &= \langle 0 \rangle = \{0\} \\ H_2 &= \langle 1 \rangle = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11\} \\ H_3 &= \langle 2 \rangle = \{0,\ 2,\ 4,\ 6,\ 8,\ 10\} \\ H_4 &= \langle 3 \rangle = \{0,\ 3,\ 6,\ 9\} \\ H_5 &= \langle 4 \rangle = \{0,\ 4,\ 8\} \\ H_6 &= \langle 6 \rangle = \{0,\ 6\}\,. \end{aligned}$$

◀

9. Either find a generator for the group $G = U(8) \times \mathbb{Z}_5$ or show that it is not cyclic.

▶ **Solution.** Every non-identity element of $U(8)$ has order 2, while every non-identity element of $\mathbb{Z}_5$ has order 5. Hence, the possible orders of elements of G are 1, 2, 5, and 10, but $|G| = 4 \times 5 = 20$, so G is not cyclic. ◀

10. Suppose that $G = \langle a \rangle$ is a cyclic group of order 20. Find all the generators of G. Find all of the subgroups of G.

▶ **Solution.** The generators of G are the elements a^m such that $(m, 20) = 1$. Thus, the generators are a, a^3, a^7, a^9, a^{11}, a^{13}, a^{17}, a^{19}. The subgroups of G are the cyclic subgroups $\langle a^k \rangle$ where k divides 20. That is, $\langle a^k \rangle$ where $k = 1, 2, 4, 5, 10, 20$. ◀

11. List all of the subgroups of $\mathbb{Z}_{225}$, and give the inclusion relations among the subgroups.

▶ **Solution.** The subgroups of $\mathbb{Z}_{225}$ are of the form $m\mathbb{Z}_{225}$ where $m|225$, and $m\mathbb{Z}_{225} \subseteq k\mathbb{Z}_{225}$ if and only if $k|m$. ◀

12. Verify that $f : \mathbb{R} \to \mathrm{GL}(2, \mathbb{R})$ by $f(r) = \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix}$ is a group homomorphism from the additive group $\mathbb{R}$ to the multiplicative group $\mathrm{GL}(2, \mathbb{R})$.

▶ **Solution.** $f(r+s) = \begin{bmatrix} 1 & r+s \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} = f(r)f(s)$ for all $r, s \in \mathbb{R}$. ◀

13. Assume $H = \{u, v, w, x, y, z\}$ is a group with respect to multiplication and $\varphi : S_3 \to H$ is an isomorphism with

$$\begin{array}{lll} \varphi((1)) = u, & \varphi((1,2,3)) = v, & \varphi((1,3,2)) = w, \\ \varphi((1,2)) = x, & \varphi((1,3)) = y, & \varphi((2,3)) = z. \end{array}$$

Replace each of the following products by the appropriate element of H, i.e., either u, v, w, x, y, or z.

(a) Identity of H $\boxed{u}$ (b) xw $\boxed{y}$ (c) w^{-1} $\boxed{v}$ (d) v^5 $\boxed{w}$ (e) $zv^{-1}x$ $\boxed{u}$

14. Let $H = \{1, 7\} \subseteq U(16)$. Verify that H is a subgroup of $U(16)$ and list all of the left cosets of H.

▶ **Solution.** H is a subgroup since $7^2 = 1$ in $U(16)$ so that $H = \langle 7 \rangle$. The left cosets of H are

$$1H = \{1, 7\}, \qquad 3H = \{3, 5\}, \qquad 9H = \{9, 15\}, \qquad 11H = \{11, 13\}.$$

◀

15. Let $H = \{(1), (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\} \subset S_4$. Verify that H is a subgroup. Determine if it is a normal subgroup. If not, identity an element $g \in S_4$ with $gH \neq Hg$.

▶ **Solution.** H is the cyclic subgroup of S_4 generated by $(1\ \ 2\ \ 3)$. H is not normal since

$$\begin{aligned} (1\ \ 4)\,H &= \{(1\ \ 4), (1\ \ 2\ \ 3\ \ 4), (1\ \ 3\ \ 2\ \ 4)\} \\ &\neq H\,(1\ \ 4) = \{(1\ \ 4), (1\ \ 4\ \ 2\ \ 3), (1\ \ 4\ \ 3\ \ 2)\}. \end{aligned}$$

◀