Midterm study guide

Here is an outline of things we've learned so far.

Groups: Foundations

- Definition of a group
- Basic properties that follow from the definition (e.g. identity and inverses are unique, $ab = ac \Rightarrow b = c$, etc.)
- order of a group, order of an element.

Dihedral groups

- Definition of D_{2n}
- properties of D_{2n}:
  - What are the elements and their orders?
  - set of generators?
  - which elements commute w/ each other
  - relations? i.e. $sr^i = r^{-i}s$

Symmetric groups

- A a set, definition of S_A (elements are bijections)
- Definition of S_n

- cycle decompositions in S_n, and how to multiply elts given their cycle decomps. (e.g. What is $(1\,2\,3)(2\,4\,3\,1)$?)

Homomorphisms

- Definition of homomorphism, isomorphism.

- How to check that a homomorphism is an iso?

  Show it's bijective or if G and H are both finite, show $\varphi: G \to H$ is either surjective or injective

  (trivial kernel!)

- How to show two groups G, H are not isomorphic? Show that there's some property that one has but not the other.

  e.g.:
  - $|G| \neq |H|$
  - the elements have different orders
  - one's abelian, one's not
  - the centers have different orders
  - the conjugacy classes have different orders
  - etc. (can you come up w/ more ways?)

- If $\varphi: G \to H$ is a homomorphism, then if we know where φ sends the generators of G, we know where it sends every element of G

- Defs of $\ker\varphi$, $\operatorname{im}\varphi$; they're both subgroups

  (exercise: if $X \subseteq G$ is a generating set for G, then

$\varphi(X) = \{\varphi(x) \mid x \in X\}$ generates im φ.)

- Definition of automorphism. If G is a group, $\mathrm{Aut}(G)$ is a group

Subgroups

- subgroup criterion, checking that $H \subseteq G$ is a subgroup
- cyclic subgroups: $\langle x \rangle$. Order of $\langle x \rangle = |x|$.
- subgroup generated by a subset. i.e. if $X \subseteq G$, definition of $\langle X \rangle \leq G$
- special subgroups: $Z(G)$, $C_G(S)$, $N_G(S)$ (for $S \subseteq G$)

Cyclic groups

- Definition and properties
- finite vs. infinite cyclic group

  finite: iso to $\mathbb{Z}/n\mathbb{Z}$; infinite: iso to $\mathbb{Z}$
- subgroups of cyclic groups are cyclic, and in $\mathbb{Z}_n$, there's exactly one subgroup for each divisor of n.

Quotient groups + Normal subgroups

- Def of a quotient group in terms of a homomorphism $\varphi: G \to H$. (Fibers are the elements)
- equivalent definitions of normality: $N \trianglelefteq G \iff xNx^{-1} = N \ \forall x \in G$

$\Leftrightarrow xN = Nx \ \forall x \in G \Leftrightarrow N_G(N) = G \Leftrightarrow$ coset multiplication is well-defined $\Leftrightarrow$ N is the kernel of some homomorphism $G \to H$.

- left cosets of a subgroup $H \le G$: $aH = bH \Leftrightarrow b \in aH \Leftrightarrow b^{-1}a \in H$.

- cosets of H partition G.

- If $N \trianglelefteq G$, definition of G/N. What are the elements? How do you multiply them? $(aNbN = abN)$

- Lagrange's Theorem (G finite, $H \le G \Rightarrow \frac{|G|}{|H|} = |G:H|$)

- Cauchy's Theorem (G finite abelian, p a prime dividing $|G|$ $\Rightarrow$ G has an element of order p)

Isomorphism Thm

- The first is the most important: $\varphi : G \to H$ a homomorphism $\Rightarrow G/\ker\varphi \cong \operatorname{im}\varphi$. (if $K = \ker\varphi$, the isomorphism $G/K \to \operatorname{im}\varphi$ is defined $aK \mapsto \varphi(a)$. Do you see why this is well-defined?)

- Understand the statements and proofs of the other iso theorems, but you don't need to memorize them.

The alternating group, or: "What's your sign?"

- Every elt of S_n has a sign: odd or even. How do you determine the sign of an element?

- the subgroup of even permutations of S_n is A_n. $A_n \trianglelefteq S_n$.

Group actions

- Definition. What is an action of G on a set A?

- If G acts on A, and $g \in G$, then $\sigma_g \in S_A$, defined $\sigma_g(a) = g \cdot a$.

- The map $G \to S_A$ defined $g \mapsto \sigma_g$ is a homomorphism, called the permutation representation of the action

- kernel of an action; action is faithful if $\ker = 1$. What does a faithful action look like?

- orbits: What are the orbits of an action? Action is transitive $\iff$ exactly one orbit

- $G_a :=$ stabilizer of a in G = $g \in G$ s.t. $g \cdot a = a$. $G_a \leq G$.

- $|G : G_a|$ = # of elements in the orbit of a

Groups acting by left multiplication

- G acts on itself by $g \cdot a = ga$; it's faithful + transitive.

- Get a homomorphism $G \to S_G$ that is injective (Cayley's Thm), so $G \cong$ image of $G \to S_G$

- G acts on left cosets of $H \leq G$ by $g \cdot aH = gaH$

- if A = set of left cosets of H, then we get a homomorphism $G \to S_A$

- If p is the smallest prime dividing $|G|$, then any subgroup of order p is normal

Groups acting by conjugation

- G acts on itself by conjugation: $g \cdot a = gag^{-1}$.
- a is conjugate to b $\Leftrightarrow$ $gag^{-1} = b$, some $g \in G$ $\Leftrightarrow$ a and b are in the same orbit under conjugation action (orbits in this case are called conjugacy classes)

- G acts on $P(G)$ by conjugation
- # of conjugates of $S \subseteq G$ = $|G : N_G(S)|$
- # of conjugates of $a \in G$ = $|G : C_G(a)|$
- $\{a\}$ is a conj. class $\Leftrightarrow$ $a \in Z(G)$.
- class equation: $g_1, \dots, g_r$ representatives of conj. classes not in the center $\Rightarrow$ $|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$.
- Group of order p^α $(\alpha \geq 1)$ has nontrivial center.

- two elements of S_n are conjugate $\Leftrightarrow$ their cycle decomp has the same # of cycles of each length.
  # of conj. classes of S_n = # of partitions of $\{1, \dots, n\}$ =

- $\tau(a_1 a_2 \dots a_r)\tau^{-1} = (\tau(a_1)\tau(a_2) \dots \tau(a_r))$

- If $\sigma, \tau \in A_n$, then if σ and τ are conj. in A_n, they are conj. in S_n, but not vice versa.

  e.g. in S_3, $(1\ 2\ 3)$ is conj. to $(1\ 3\ 2)$ since $(2\ 3)(1\ 2\ 3)(2\ 3)^{-1} = (1\ 3\ 2)$, but $(2\ 3) \notin A_n$, so they're not conj. in A_n.

GOOD LUCK!