2014 Algebra SEP $\sim$ Standard Group Theory Facts (by Evan Dummit)

- Suggested reading: Dummit/Foote chapters 1-6 (groups), and a skim of chapters 18-19 (group representations and characters).
- Examples you should be familiar with:
  - Abelian groups: finitely-generated abelian groups, fields, infinite direct sums and direct products of cyclic groups.
  - Nonabelian groups: The symmetric groups S_n and A_n, the dihedral groups $D_{2\cdot n}$, the quaternion group Q_8, the general and special linear groups $GL_n(R)$ and $SL_n(R)$ for a ring R (especially when R is a field or $\mathbb{Z}$).
- Basic facts about groups:
  - If G is a group, $|G|$ denotes the <u>order</u> of G, equal to the number of elements of G.
    - If $g \in G$, $|g|$ denotes the <u>order</u> of g, the order of the subgroup $\langle g \rangle$ generated by g, or equivalently, the smallest $n > 0$ for which $g^n = 1$ (or ∞ if g^n is never the identity for $n > 0$) .
  - If A is a subset of G, $C_G(A) = \left\{g \in G : gag^{-1} = a \text{ for all } a \in A\right\}$ is the <u>centralizer</u> of A in G, and is the set of elements of G which centralize (i.e., commute) with everything in A.
    - The <u>center</u> $Z(G)$ is the centralizer of G in G, the set of elements of G which commute with all of G.
  - If A is a subset of G, $N_G(A) = \left\{g \in G : gag^{-1} \in A \text{ for all } a \in A\right\}$ is the <u>normalizer</u> of A in G, and is the set of elements of G which normalize A.
    - A subgroup $N \subseteq G$ is <u>normal</u> in G if $N_G(N) = G$ – that is, if $ghg^{-1} \in N$ for every $g \in G$ and $h \in N$.
    - The element ghg^{-1} is the <u>conjugate</u> of h by g.
  - If $H \subseteq G$ is a subgroup, then the <u>left cosets</u> of H in G are the subsets $\{gH\}$ for $g \in G$, and the <u>right cosets</u> of H in G are the subsets $\{Hg\}$ for $g \in G$.
    - The left (resp., right) cosets partition G into equivalence classes, each of which has size equal to $|H|$. The number of cosets (which is equal to $\dfrac{|G|}{|H|}$ if H is finite) is called the <u>index</u> of H in G and denoted $|G : H|$.
    - The set of left cosets of H equals the set of right cosets of H if and only if H is normal in G.
    - (Lagrange) If $H \subseteq G$ is a subgroup, then $|H|$ divides $|G|$. As a corollary, for any $g \in G$, $|g|$ divides $|G|$.
    - (Cauchy) If G is finite and p divides $|G|$, then G contains an element of order p.
  - If N is normal, then the set of cosets of N in G forms the <u>quotient group</u> G/N, with group operation given by $(gN)(hN) = ghN$.
  - Isomomorphism theorems for groups:
    - First isomorphism theorem: If $\varphi : G \to H$ is a homomorphism, then $\text{im}(\varphi) \cong G/\ker(\varphi)$.
    - Second isomorphism theorem: If A and B are subgroups of G with $A \le N_G(B)$ then $AB/B \cong A/(A \cap B)$.
    - Third isomorphism theorem: If $H \subseteq K$ are subgroups of G, then $(G/H)/(K/H) \cong G/K$.
    - Lattice isomorphism theorem: If N is a normal subgroup of G, the (normal) subgroups of G/N are in bijection with the (normal) subgroups of G containing N.
  - (Fundamental theorem of finitely-generated abelian groups) If G is a finitely-generated abelian group, then G is isomorphic to the direct sum of $\mathbb{Z}^r$ and a finite number of cyclic groups $\mathbb{Z}/p_i^{a_i}\mathbb{Z}$ each of prime-power order.
  - An isomorphism of G with itself is called an <u>automorphism</u> of G, and the set of automorphisms $\text{Aut}(G)$ forms a group.
    - Conjugation by any $g \in G$ is an automorphism of G; such an automorphism is called an <u>inner automorphism</u> and the set of these is denoted $\text{Inn}(G)$.

        * $\text{Inn}(G)$ is a normal subgroup of $\text{Aut}(G)$, and the quotient $\text{Aut}(G)/\text{Inn}(G) = \text{Out}(G)$ is called the outer automorphism group of G.
    - A subgroup $H \subseteq G$ is called characteristic if it is fixed by every automorphism of G.
        * Characteristic subgroups are normal. If G has a unique subgroup of a given order, it is necessarily characteristic.
        * Normality is not transitive in general, but if K is a characteristic subgroup of H, and H is normal in G, then K is normal in G.
    - If G is a finite group of order n and p is a prime dividing n with p^k the largest power of p dividing n, then a subgroup of G of order p^k is called a Sylow p-subgroup of G.
        * (Sylow) Sylow p-subgroups of G exist, all Sylow p-subgroups of G are conjugate, and the number n_p of such subgroups is 1 modulo p, and n_p also equals the index of the normalizer of (any) Sylow p-subgroup.
        * G has a unique p-Sylow subgroup P iff $n_p = 1$ iff P is normal iff P is characteristic.
        * There are a number of consequences of Sylow's Theorem, many of which stem from analyzing possible values for the number of p-Sylow subgroups.
        * For a basic example, if $p < q$ are primes with p not dividing $q - 1$, then any group of order pq is abelian (since there can only be one q-Sylow and one p-Sylow subgroup).
    - If $G = HK$ where H and K are both normal subgroups with $H \cap K = 1$, then G is the (internal) direct product of H and K: $G \cong H \times K$.
    - If H and K are groups and $\phi : K \to \text{Aut}(H)$ is a homomorphism with $\cdot$ denoting the left action of K on H associated to ϕ, the semidirect product of H and K (with respect to ϕ), denoted $H \rtimes_\phi K$, is the group of pairs (h, k) with multiplication given by $(h_1, k_1)(h_2, k_2) = (h_1\, k_1 \cdot h_2,\, k_1k_2)$.
        * $H = \{(h, 1)\}$ and $K = \{(1, k)\}$ are naturally subgroups of $G = H \rtimes_\phi K$, and $H \cap K = 1$.
        * Furthermore, H is normal in G and $G = HK$, but K is not normal in G unless ϕ is trivial (in which case the semidirect product is merely the direct product).

- Basic facts about group actions
    - If G is a group and A is a set, a group action of G on A is a map $\cdot : G \times A \to A$ such that $1 \cdot a = a$ for all $a \in A$ and $g \cdot (h \cdot a) = gh \cdot a$ for all $g, h \in G$.
        * Equivalently, a group action of G on A is a homomorphism $\phi : G \to S_A$, where S_A is the symmetric group on the set A – this homomorphism is the permutation representation associated to the group action.
        * The kernel of the action is the set of elements of G which act trivially on all of A. An action is faithful if its kernel is trivial.
        * For each $a \in A$, the stabilizer of a in G is the subgroup of G consisting of the $g \in G$ with $g \cdot a = a$.
        * The orbit of a under G is the set of $b \in A$ for which there exists $g \in G$ with $b = g \cdot a$.
        * (Orbit-Stabilizer) For each $a \in A$, the number of elements in the orbit of a under G equals the index of the stabilizer of a in G.
    - If H is any subgroup of G, G acts on the left cosets of H by left multiplication. The corresponding permutation representation gives a homomorphism $\varphi : G \to S_{|G:H|}$.
        * This action is transitive and the stabilizer of xH is xHx^{-1}.
        * The kernel of the action is the normal core of H, defined as $\text{core}(H) = \cap_{x \in G} xHx^{-1}$; it is the largest normal subgroup of G contained in H.
        * (Cayley) Every group is isomorphic to a subgroup of a symmetric group, given explicitly by the left-multiplication action of G on itself.
        * If $|G| = n$ and p is the smallest prime dividing $|G|$, then any subgroup H of index p is normal. (This follows from considering the action of G on the p cosets of H.)
    - G acts on the subsets of G by conjugation. (In particular, G acts on its subgroups by conjugation.)
        * The orbits of the conjugation action of single-element subsets of G are called the conjugacy classes of G. The conjugacy classes partition G.

    * Two permutations in S_n are conjugate iff they have the same cycle type. (When passing to A_n, each conjugacy class in S_n either stays a conjugacy class, or splits into two conjugacy classes.)
    * The number of conjugates of any subset S in G is equal to $|G : N_G(S)|$.
    * (Class Equation) If G is a finite group, then $|G| = |Z(G)| + \sum |G : C_G(g_i)|$, where the g_i are representatives of the non-central conjugacy classes.
    * If P is a p-group, then $Z(P) \neq 1$. (This follows from taking the class equation mod p.) In particular, groups of order p^2 are abelian, by using the standard fact that if $G/Z(G)$ is cyclic, then G is abelian.

- Basic facts about simple groups / solvable groups / group series:
  - A nontrivial group G is simple if it contains no nontrivial normal subgroups.
    * $\mathbb{Z}/p\mathbb{Z}$ for prime p are (clearly) the only abelian simple groups.
    * A_n is simple for $n \geq 5$. $PSL_n(\mathbb{F}_q)$ is simple for all $n \geq 2$ and all q, except for $(n, q) = (2, 2)$ and $(2, 3)$.
    * The finite simple groups have been classified.
  - A sequence of subgroups $1 = N_0 \leq N_1 \leq \cdots \leq N_k = G$ is called a composition series for G if N_i is normal in N_{i+1} and N_{i+1}/N_i is a simple group for each i. The quotient groups N_{i+1}/N_i are called the composition factors of G.
    * (Jordan-Hölder) If G is a nontrivial finite group, it has a composition series, and the composition factors are unique up to rearrangement.
  - A group G is solvable if it has a composition series each of whose factors is abelian.
    * If N is normal in G, then G is solvable if and only if N and G/N are solvable.
    * (Feit-Thompson) Finite groups of odd order are solvable.
    * (Burnside) Finite groups of order $p^a q^b$ for primes p and q and positive integers a, b are solvable.
    * (P. Hall) A finite G is solvable if and only if for each divisor n of $|G|$ with $\gcd(n, |G|/n) = 1$, G has a subgroup of order n.
    * The Feit-Thompson and Burnside theorems are often stated about the nonexistence of simple groups of those orders; in fact they prove that such groups are actually solvable.
  - The upper central series for a group G is the chain of subgroups $1 = Z_0(G) \leq Z_1(G) \leq \cdots$, defined inductively as $Z_0(G) = 1$, $Z_1(G) = Z(G)$, and for $i \geq 1$, $Z_{i+1}(G)$ is the preimage in G of the center of $G/Z_i(G)$ under the quotient map.
    * Each group $Z_i(G)$ is characteristic in G.
  - A group is nilpotent if $Z_c(G) = G$ for some c; the smallest such c is called the nilpotence class of G.
    * Abelian groups are (trivially) of nilpotence class 1. A p-group of order p^a is nilpotent, and of nilpotence class at most $a - 1$.
    * A finite group G is nilpotent iff each Sylow p-subgroup is normal, iff G is the direct product of its Sylow p-subgroups.
  - If $a, b \in G$, then the commutator of a and b is defined as $[a, b] = a^{-1}b^{-1}ab$. If H_1 and H_2 are subgroups of G, then the commutator of H_1 and H_2 is defined to be the subgroup generated by all commutators $[h_1, h_2]$ for $h_1 \in H_1$ and $h_2 \in H_2$.
    * The commutator subgroup of G is $[G, G]$. If A is any abelian quotient of G, then the quotient map $\varphi : G \to A$ factors through the commutator subgroup.
  - The lower central series for a group G is the chain of subgroups $G = G^0 \geq G^1 \geq \cdots$, defined inductively by $G^0 = G$, $G^1 = [G, G]$, and $G^{i+1} = [G, G^i]$.
    * Each of the terms G^i is characteristic in G.
    * A group is nilpotent (recall: if its upper central series stabilizes at G) if and only if its lower central series eventually stabilizes at 1. More generally, if G has nilpotence class c, then $G^{c-i} \leq Z_i(G)$, and the lower and upper central series both stabilize at the same level.
  - The derived series (or commutator series) for G is the sequence of subgroups $G = G^{(0)} \geq G^{(1)} \geq \cdots$, where $G^{(1)} = [G, G]$ and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$.

    - Despite the notation, after the first term $G^{(1)} = G^1$, the derived and lower central series are not generally equal.
    - A group G is solvable if and only if $G^{(n)} = 1$ for some n.

- Basic facts about representations of groups:
  - If V is a vector space over a field F, a homomorphism $\rho : G \to GL(V)$ is called a (linear) representation of G. If ρ is injective, the representation is faithful.
    - Choosing a basis for V yields a matrix representation of $\rho : G \to GL_n(F)$ where $n = \dim_F(V)$.
  - The group ring FG is defined to be the finite sums of the form $\sum \alpha_i g_i$ where $\alpha_i \in F$ and $g_i \in G$, where multiplication is defined via $(\alpha g) \cdot (\beta h) = \alpha\beta(gh)$ and extended linearly. The group ring is commutative iff G is abelian.
  - Linear representations, as pairs (ρ, V) are (categorically) equivalent to FG-modules. Note that an FG-module is actually an F-algebra.
  - (Maschke) If G is finite and F has characteristic not dividing $|G|$, then if V is any FG-module and U any submodule of V, then U is a direct summand of V (i.e., there exists W such that $V = U \oplus W$).
  - (Artin-Wedderburn) If R is a semisimple ring with minimum condition (in particular, if $R = FG$ is a group ring where $\text{char}(F)$ does not divide $|G|$), then $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ where the D_i are division rings containing F.
    - Thus, if G is a finite group, then every complex representation of G is a direct sum of irreducible complex representations.
    - Furthermore, if G has r conjugacy classes, then G has exactly r inequivalent irreducible complex representations of degrees $n_1, \cdots, n_r$, where $\sum n_i^2 = |G|$ and each n_i divides $|G|$.
    - If A is abelian, then all irreducible complex representations are 1-dimensional, and any representation of A is equivalent to a diagonal representation.
    - In general, the number of 1-dimensional representations of G is $|G/[G, G]|$, because every abelian quotient of G factors through $[G, G]$.
  - If $\rho : G \to GL_n(F)$ is a representation of G, the character $\chi : G \to F$ associated to ρ is a set map defined as $\chi(g) = \text{tr}(\rho(g))$.
    - If G is a finite group, then its characters are sums of roots of unity (since the eigenvalues of $\rho(g)$ are roots of unity) and hence are algebraic integers.
    - A character is a class functions (i.e., it takes the same value on all elements in a conjugacy class of G), but it is not necessarily an additive or multiplicative homomorphism into F.
    - A character is irreducible if the underlying representation is irreducible.
    - Two equivalent representations have the same characters, and conversely if two representations have the same character then they are equivalent.
    - The character table of a finite group lists the values of the irreducible characters of the group on each conjugacy class of G.

- Useful tricks:
  - For a Sylow problem, make a list of the possible Sylow numbers for each prime dividing the order of the group, and see if there are any immediate possibilities that don't work (e.g., if the group is simple, 1 never works, and other small values can often be ruled out by looking at the permutation representation). Then look at the possible sizes of the normalizers (and possibly centralizers) of the Sylow subgroups to see if they provide any information.
  - For problems involving simple groups, a standard method of attack is to try to work by contradiction and show that some piece of information will force the existence of a normal subgroup (e.g., one of the Sylow numbers must be 1, or some homomorphism has a nontrivial kernel).
  - In general if you are stuck and not sure how to use one of the hypotheses, try considering examples of groups where the given hypothesis doesn't hold to see what goes wrong with the conclusion – this may help you see where the hypothesis might be needed. Thinking about the standard group actions (left multiplication on cosets of a subgroup, conjugation of subgroups, and conjugacy classes) is often useful as well.

- If there is a normal subgroup, you will probably want to examine what happens in the quotient group. (This is good general advice for rings and modules too!)
- For representations of finite groups, it is often useful to consider the linear-algebraic properties of the corresponding matrices (in particular: their eigenvalues and Jordan forms). An advanced knowledge of representation theory is generally not needed, although understanding the basic properties of characters of finite groups is likely to be useful.
- Semidirect products are in theory an official qualifying exam topic, but they are unlikely to appear since they are not always covered in the algebra courses. (But it would still be good to know what they are since they make good examples.)