ALGEBRA TEST #2

This exam is due Friday, October 31. Do three of the problems. You may use your book, but you may not communicate with others concerning the exam. In order to receive full credit your answer must be **complete**, **legible** and **correct**.

I have neither given nor received aid on this exam.

Name:______________________________

1. Show that if N is a minimal normal subgroup of some finite group G, then N is isomorphic to a power S^k of a simple group S.

Let $M \prec N$ be a subgroup that maximal for being normal in N, and let $N/M = S$ be the simple quotient. The conjugation map $\gamma_g(x) = gxg^{-1}$ for $g \in G$ induces an automorphism of N. The kernel of the (surjective) composite map $N \xrightarrow{\gamma_g} N \xrightarrow{\nu} N/M$ is $g^{-1}Mg$, so $N/g^{-1}Mg \cong S$ for all $g \in G$. Thus we have a family of surjective homomorphisms $\nu \circ \gamma_g$ from N onto S, which may be combined into a single product map $\varphi\colon N \to S^{|G|}$ which, when followed by any coordinate projection onto S, is surjective. The kernel of φ is $\bigcap_{g \in G}(g^{-1}Mg)$, which is a normal subgroup of G that is properly contained in N, hence is $\{1\}$. Thus, φ embeds N into a power of a simple group S in such a way that each composition of φ with the coordinate projections is surjective. The result now follows from the more general statement: *If $\varphi\colon N \to \prod_{i=1}^{k} S_i$ is an embedding of a group into a finite product of simple groups in such a way that each composition of φ with a coordinate projection is surjective, then N is isomorphic to a product of some subset of the S_i's.*

This statement is proved by induction on the number of factors. Suppose k is the least number of factors for which the statement has not yet been proved, and that $\varphi\colon N \to \prod_{i=1}^{k} S_i$ is an embedding of the type described. Compose φ with projection onto the first $k-1$ factors, and let A be the kernel of this composition $N \xrightarrow{\varphi} \prod_{i=1}^{k} S_i \to \prod_{i=1}^{k-1} S_i$. Let B be the kernel of the composite $N \xrightarrow{\varphi} \prod_{i=1}^{k} S_i \to S_k$. If either $A = \{1\}$ or $B = \{1\}$ we are done by induction. We have $A \cap B = \ker(\varphi) = \{1\}$, so since A and B are nontrivial they must be incomparable. The incomparability implies that $A \vee B = AB$ properly contains B in $\mathrm{Norm}(N)$. But B is a maximal normal subgroup of N, so $AB = N$. Since A and B are complementary normal subgroups of N, $N \cong N/A \times N/B \cong N/A \times S_k$. The group N/A is isomorphic to a product of some subset of the groups $S_1, \ldots, S_{k-1}$, by induction, so we are done.

2. Describe the structural properties a group G must have if the free G-set $\langle G; G\rangle$ has a nontrivial direct factorization (meaning $\langle G; G\rangle \cong \mathbf{A} \times \mathbf{B}$ with $|A|, |B| > 1$). Then find a nonabelian finite group G such that $\langle G; G\rangle$ has no nontrivial direct factorization.

We have seen that the subgroup lattice of G is isomorphic to the congruence lattice of the free G-set $\langle G; G\rangle$ via the map $H \mapsto \theta_H$, where

$$\theta_H = \{(a, b) \in G^2 \mid a^{-1}b \in H\}.$$

The characterization of products states that direct factorizations correspond to pairs of permuting complementary congruences. From our first sentence, congruences θ_H and θ_K are complements iff H and K are complementary subgroups. The pair (a, b) lies in $\theta_H \circ \theta_K$ iff $a^{-1}b \in HK$, and lies in $\theta_K \circ \theta_H$ iff $a^{-1}b \in KH$. Thus θ_H and θ_K are permuting congruences iff H and K are permuting subgroups (i.e., $HK = KH$). Thus, the G-set $\langle G; G\rangle$ has a nontrivial direct factorization iff G has a pair of nontrivial proper permuting subgroups.

The 8-element quaternion group has no pair of nontrivial complementary subgroups, because all proper subgroups contain the center.

3. Let $\mathbf{F}_{Grp}(a, b)$ be the group freely generated by the set $X = \{a, b\}$. Show that the subset $\{ab, a^2b^2, a^3b^3, \ldots\}$ is an infinite independent subset of this group. Conclude that a free group generated by a countably infinite set is embeddable in a free group on two generators.

We must show that if $w(x_1, \ldots, x_n)$ is a nonidentity reduced word and $i_1, \ldots, i_n$ are distinct, then $w(a^{i_1}b^{i_1}, \ldots, a^{i_n}b^{i_n}) \neq 1$. We do this by induction on the length of w. The precise statement to prove by induction is: If w ends in the letter x_j, then the reduced form of $w(a^{i_1}b^{i_1}, \ldots, a^{i_n}b^{i_n})$ ends in exactly i_j b's, preceded by a or a^{-1}; if w ends in the letter x_j^{-1}, then the reduced form of $w(a^{i_1}b^{i_1}, \ldots, a^{i_n}b^{i_n})$ ends in exactly i_j a^{-1}'s, preceded by b or b^{-1}. The two cases are handled the same way, so assume we are in the first case where $w = w'x_j$. Since w is reduced, the word w' is reduced and cannot end in x_j^{-1}. This means that after substituting the a^nb^n's we get by induction that $w'(a^{i_1}b^{i_1}, \ldots, a^{i_n}b^{i_n})$ ends in a sequence of a^{-1}'s whose length is not i_j, or else ends in a sequence of b's. Neither case can affect the length of the final string of b's in

$$w(a^{i_1}b^{i_1}, \ldots, a^{i_n}b^{i_n}) = w'(a^{i_1}b^{i_1}, \ldots, a^{i_n}b^{i_n})a^{i_j}b^{i_j},$$

since after reduction the final sequence of i_j b's is still separated by the earlier letters by some a's or a^{-1}'s.

4. In this problem you will establish a fairly compact presentation of the symmetric group S_{n+1}. Take as generators $\tau_1, \ldots, \tau_n$ and as relations

- $\tau_i^2 = 1$ for all i.
- $(\tau_i\tau_{i+1})^3 = 1$ for all i (equivalently, $\tau_i\tau_{i+1}\tau_i = \tau_{i+1}\tau_i\tau_{i+1}$ for all i).
- $\tau_i\tau_j = \tau_j\tau_i$ if $|j-i| > 1$.

(a) Show that the group with this presentation has a homomorphism onto S_{n+1}.

(b) Show that the group with this presentation has at most $(n+1)!$ elements.

(Hint for (b): Use the relations and induction on n to show that any product of generators may be rewritten as a product of the same length or shorter in the form $\sigma\tau_n\tau_{n-1}\cdots\tau_{k+1}\tau_k$ for some k where σ is a product of generators not including τ_n.)

Let G_{n+1} be the group defined by the given presentation, $\langle X \mid R\rangle$. The function $f\colon X \to S_{n+1}$ defined by $\tau_i \mapsto (i\ i+1)$ preserves the relations, so extends uniquely to a homomorphism $\overline{f}\colon G_{n+1} \to S_{n+1}$. This homomorphism is surjective since it contains a generating set $f(X)$ in its image.

We prove by induction on n that any product of generators may be rewritten as a product of the same length or shorter in the form $\sigma\tau_n\tau_{n-1}\cdots\tau_{k+1}\tau_k$ for some k where σ is a product of generators not including τ_n. Since there are at most $n!$ choices for σ (by induction) and $n+1$ choices for the sequence following σ, this will prove $|G_{n+1}| \leq (n+1)!$. The cases $n = 0$ and $n = 1$ are obvious.

Now suppose that we have a shortest product of generators that represents a particular element $\pi \in G_{n+1}$. If τ_n occurs more than once, we can eliminate one of them without increasing length, as follows: if $\pi = \cdots\tau_n\rho\tau_n\cdots$ indicates two occurrences of τ_n in the string π with an intermediate string ρ with no τ_n's, then by induction we may assume that ρ contains at most one τ_{n-1}. If ρ contains no τ_{n-1}, then the relations allow us to bring the two τ_n's together and cancel them, leaving a shorter word. In the alternative case, we can move the two τ_n's adjacent to the τ_{n-1} to obtain $\pi = \cdots\tau_n\tau_{n-1}\tau_n\cdots = \cdots\tau_{n-1}\tau_n\tau_{n-1}\cdots$, which has fewer τ_n's. This process may be continued until there is only one τ_n. Now we may assume that $\pi = \alpha\tau_n\beta$ where α and β are free of τ_n. By induction we may assume $\beta = \sigma_1\tau_{n-1}\tau_{n-2}\cdots\tau_k$ with τ_n and τ_{n-1} not in σ_1, in which case we may rewrite $\pi = \alpha\tau_n\beta = \alpha\tau_n\sigma_1\tau_{n-1}\tau_{n-2}\cdots\tau_k = (\alpha\sigma_1)\tau_n\tau_{n-1}\tau_{n-2}\cdots\tau_k$ with τ_n not appearing in $\sigma := (\alpha\sigma_1)$.

5. Let $\mathbf{A} = \langle G/H; G \rangle$ be the G-set of left cosets of H under the action of left multiplication. Show that $\mathrm{Aut}(\mathbf{A}) \cong N_G(H)/H$.

Since G/H is 1-generated, any automorphism is determined by its action on the coset H. This means that for any other coset gH there can be at most one automorphism that maps H to gH. Isomorphisms of G-sets preserve stabilizers, so for an automorphism to map H to gH we must have $H = \mathrm{Stab}(H) = \mathrm{Stab}(gH) = gHg^{-1}$, or $g \in N_G(H)$. We argue that for every $g \in N_G(H)$ there is an automorphism that maps H to gH.

Choose $g \in N_G(H)$ and let $\rho_g \colon G/H \to G/H \colon aH \mapsto aHg^{-1}$ be *right multiplication by* g^{-1}. Since $g \in N_G(H)$ we have $\rho_g(aH) = a(Hg^{-1}) = ag^{-1}H$, so ρ_g maps left cosets to left cosets. The associative law implies that left multiplications commute with right multiplications, so ρ_g is a homomorphism. Since ρ_g has inverse $\rho_{g^{-1}}$ it is an automorphism. Since $\rho_g \circ \rho_k(H) = Hk^{-1}g^{-1} = H(gk)^{-1} = \rho_{gk}(H)$ the map $\varphi \colon N_G(H) \to \mathrm{Aut}(G/H) \colon g \mapsto \rho_g$ is a homomorphism. If $\alpha \in \mathrm{Aut}(G/H)$, and $\alpha(H) = gH$, then we pointed out in the previous paragraph that α is the only automorphism mapping H to gH, but since $\rho_{g^{-1}}$ is another we get that the map φ is surjective. $\ker(\varphi)$ consists of those $g \in N_G(H)$ such that $\rho_g = \mathrm{id}$, and these are the $g \in N_G(H)$ such that $H = \rho_g(H) = Hg$, i.e., the $g \in H$. By the first isomorphism theorem $N_G(H)/H = N_G(H)/\ker(\varphi) \cong \mathrm{im}(\varphi) = \mathrm{Aut}(G/H)$.

6. Show that a coproduct of a family $\{\mathbf{A}_j \mid j \in J\}$ of G-sets is $(\mathbf{A}, \{\iota_j\})$ where $\mathbf{A}$ is the disjoint union of the $\mathbf{A}_j$ and ι_j is inclusion.

The disjoint union $\cup A_i$ of G-sets is again a G-set, with the action of $g(x)$ on an element $a \in A_j \subseteq \cup A_i$ being the same as it was in $\mathbf{A}_j$. We take the inclusion maps $\iota_j \colon A_j \to \cup A_i$ to be the coprojections. For any family of homomorphisms $\varphi_j \colon \mathbf{A}_j \to \mathbf{B}$ we need to construct $\sqcup\varphi_i \colon \bigcup A_i \to \mathbf{B}$ which encodes the φ_i's. Define $\sqcup\varphi_i$ so that it equals φ_j on elements of A_j. This uniquely defines $\sqcup\varphi_i$ on $\cup A_i$. It is a homomorphism, since if $a \in A_j \subseteq \cup A_i$ and $g \in G$, then $\sqcup\varphi_i(g(a)) = \varphi_j(g(a)) = g(\varphi_j(a)) = g(\sqcup\varphi_i(a))$. Finally, $\sqcup\varphi_i \circ \iota_j(a) = \sqcup\varphi_i(a) = \varphi_j(a)$ for any $a \in A_j$, proving that $\sqcup\varphi_i \circ \iota_j = \varphi_j$ for any j.