Algebra-I, Fall 2011. Solutions to Midterm #2.

1. Given a finite group G and a positive integer n, denote by $a_n(G)$ the number of elements of G of order n and by $b_n(G)$ the number of elements of G of order dividing n. The goal of this problem is to prove the following theorem:

Theorem A: If G and H are finite abelian groups and $a_n(G) = a_n(H)$ for all n, then G is isomorphic to H.

(a) Let G and H be finite groups. Prove that $a_n(G) = a_n(H)$ for all $n \iff b_n(G) = b_n(H)$ for all n.
(b) Suppose that $G = X \times Y$. Prove that $b_n(G) = b_n(X)b_n(Y)$.
(c) Suppose that G and H are finite abelian groups s.t. $a_n(G) = a_n(H)$ for all n. Prove that there exists a non-trivial group C s.t. $G \cong A \times C$ and $H \cong B \times C$ for some groups A and B. **Hint:** Use the classification theorem in invariant factors form.
(d) Now use (a),(b) and (c) to prove Theorem A.

Solution: (a) "$\Rightarrow$" Since $b_n(K) = \sum_{d|n} a_d(K)$ for any group K, the equality $a_n(G) = a_n(H)$ for all n implies that $b_n(G) = b_n(H)$ for all n

"$\Leftarrow$" We use induction on n. The base case is clear since $b_1(K) = a_1(K) = 1$ for any group K. Assume now that $a_m(G) = a_m(H)$ for all $m < n$ and $b_n(G) = b_n(H)$. Since $a_n(K) = b_n(K) - \sum_{d|n, d<n} a_d(K)$ for any group K, we conclude that $a_n(G) = a_n(H)$.

(b) For a group K let $B_n(K) = \{k \in K : k^n = 1\} = \{k \in K : o(k) \text{ divides } n\}$, so that $b_n(K) = |B_n(K)|$. Given $(x, y) \in X \times Y$, we have $(x, y)^n = 1 \iff x^n = 1$ and $y^n = 1$. Therefore, $B_n(X \times Y) = B_n(X) \times B_n(Y)$ as sets, and so $b_n(X \times Y) = |B_n(X \times Y)| = |B_n(X) \times B_n(Y)| = b_n(X)b_n(Y)$.

(c) **Note:** To make the assertion of (c) valid we need to assume that G (and hence also H) is non-trivial. Consider the IFF decomposition $G = \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$ where $2 \le n_k \mid n_{k-1} \mid \ldots \mid n_1$. Then in the notations of (b), $B_{n_1}(G) = G$ and G contains an element of order n_1 (e.g. any generator of $\mathbb{Z}_{n_1}$). Thus, the largest invariant factor of G (which we denoted by n_1) is equal to the largest order of an element of G.

Since $a_n(G) = a_n(H)$ for all n, applying the same argument to H, we conclude that the largest invariant factor of H is equal to n_1. Thus, $G = A \times C$ and $H = B \times C$ where $C = \mathbb{Z}_{n_1}$ and A (resp. B) is the product of the remaining factors in IFF decomposition of G (resp. H).

(d) We use induction on $|G|$. First note that G and H have the same order since $|K| = \sum_{n \in \mathbb{N}} a_n(K)$ for any group K.
Thus, in the base case $|G| = 1$ we have $|H| = 1$, so $G \cong H$. Assume now that $|G| > 1$. Then by (c), $G = A \times C$ and $H = B \times C$ where C is non-trivial. By (a), $b_n(G) = b_n(H)$ for all n, whence $b_n(A) = b_n(G)/b_n(C) = b_n(H)/b_n(C) = b_n(B)$ by (b), and then using (a) again we get $a_n(A) = a_n(B)$ for all n. Since C is non-trivial, $|A| < |G|$, so by induction hypothesis $A \cong B$, and therefore $G = A \times C \cong B \times C = H$.

2. Let G be a finite group
(a) Prove that G is nilpotent if and only if G contains a normal subgroup of order m for any m dividing $|G|$.
(b) Prove that G is cyclic if and only if G contains a unique subgroup of order m for any m dividing $|G|$.
Note: Of course, the forward direction in (b) is well known, so you can assume it without proof.

Note: [DF, 6.1] contains some results from which (a) and (b) follow almost immediately. We will give a proof of (a) and (b) using the main properties of nilpotent groups.

Solution: (a) "$\Rightarrow$" Since G is nilpotent, it is a direct product of its Sylow subgroups $P_1, \ldots, P_k$. If we are given a normal subgroup Q_i of P_i for each i, then $Q_1 \times \ldots \times Q_k$ is normal in $P_1 \times \ldots \times P_k = G$. Thus, to prove (a) it suffices to show that for any group P of order p^m, with m prime, and any $0 \le l \le m$, there exists a normal subgroup Q of P of order p^l.

We prove the latter assertion by induction on m. The base case $m = 1$ is clear. Assume now that the assertion is true for all p-groups of order less than p^m, and suppose that $|P| = p^m$. We know that $Z(P)$ is non-trivial, so $|Z(P)| = p^s$ for some $s > 0$. Note that $Z(P)$ contains a subgroup of order p^t for every $t \le s$ (e.g. by Sylow theorems), and every subgroup of $Z(P)$ is normal in P, so if $l \le s$, we can find a normal subgroup of P of order p^l inside $Z(P)$. Suppose now that $l > s$. Then $0 < l - s < m - s$, so by the induction hypothesis, $P/Z(P)$ contains a normal subgroup of order p^{l-s}. By the lattice isomorphism theorem, the full preimage of this subgroup in P is a normal subgroup of order p^l.

"$\Leftarrow$" Suppose that $|G| = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ where $p_1, \ldots, p_k$ are distinct primes. By assumption, for each $1 \le i \le k$, G contains a normal subgroup P_i of order $p_i^{\alpha_i}$. But then each P_i is a normal Sylow p_i-subgroup of G. Thus, all Sylow subgroups of G are normal, so G is a direct product of its Sylow subgroups and therefore nilpotent.

(b) As remarked above, we shall only prove the reverse direction.

Suppose that $|G| = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. Then by assumption H contains a unique subgroup of order $p_i^{\alpha_i}$ for each i, so each Sylow p_i-subgroup of G is normal, and as in (a) we conclude that G is nilpotent, so $Z(G) \neq \{1\}$.

We proceed by induction on $|G|$. Consider two cases.

Case 1: G is abelian. If G is not cyclic, then its IFF decomposition has at least two terms: $G = \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$ where $2 \leq n_k \mid n_{k-1} \mid \ldots \mid n_1$ and $k \geq 2$. Since $n_2 \mid n_1$, $\mathbb{Z}_{n_1}$ contains a subgroup isomorphic to $\mathbb{Z}_{n_2}$, and therefore G contains two distinct subgroups isomorphic to $\mathbb{Z}_{n_2}$, contrary to our assumption.

Case 2: G is non-abelian. Then the quotient $G/Z(G)$ is non-cyclic. Since $|G/Z(G)| < |G|$, by induction hypothesis $G/Z(G)$ contains two distinct subgroups of the same order. The preimages of these two subgroups in G yield two distinct subgroups of G of the same order, again contrary to our assumption.

3. In all parts of this problem G is a finite group.
(a) Prove that G has a simple quotient (that is, G has a quotient which is a simple group).
(b) Suppose that G is perfect, that is, $[G, G] = G$. Prove that G has a non-abelian simple quotient.
(c) Once again, let G be an arbitrary finite group. Prove that G has a unique normal subgroup K such that K is perfect and G/K is solvable.

Note: For the assertion of the problem to be valid, we need to assume that G is non-trivial.

Solution: (a) Since G is finite and non-trivial, it has a maximal normal subgroup N, that is, a maximal element of the set of **proper** normal subgroups of G, ordered by inclusion. Then G/N is simple. If not, G/N contains a proper non-trivial normal subgroup, so by the lattice isomorphism theorem there is a proper normal subgroup of G which strictly contains N, contradicting the assumption that N is maximal.

(b) For any normal subgroup N of any group G we have $[G/N, G/N] = [G, G]N/N$. If G is perfect, $[G, G]N = GN = G$, so any quotient of G is perfect. Thus, by (a), G has a perfect simple quotient, call it Q. Since simple groups are non-trivial and a non-trivial abelian group cannot be perfect, Q is simple non-abelian.

(c) The derived series $\{G^{(n)}\}$ is descending, and since G is finite, there exists

$N \in \mathbb{N}$ s.t. $G^{(n)} = G^{(N)}$ for all $n \geq N$. We claim that $K = G^{(N)}$ has the required property. Indeed, $[K, K] = [G^{(N)}, G^{(N)}] = G^{(N+1)} = K$, so K is perfect. On the other hand, $(G/K)^{(N)} = G^{(N)}K/K = K/K = \{1_{G/K}\}$, so G/K is solvable.

Now we prove uniqueness. Let L be any perfect normal subgroup s.t. G/L is solvable. Since L is perfect, we have $L = L^{(n)}$ for all n. In particular, $L = L^{(N)} \subseteq G^{(N)} = K$. And since G/L is solvable, $(G/L)^{(n)} = \{1\}$ for some n. Since $(G/L)^{(n)} = G^{(n)}L/L$, we get $L \supseteq G^{(n)} = K$. Combining the two inclusions, we conclude that $L = K$.

4. Prove that there are precisely 5 isomorphism classes of groups of order 20. Include all the details.

Solution: We will use the following two results in the proof:

Lemma A: *Let P and Q be groups and ϕ, ψ homomorphisms from Q to* $\mathrm{Aut}(P)$. *Suppose that there exists $\theta \in \mathrm{Aut}(Q)$ s.t. $\phi\theta = \psi$. Then $P \rtimes_\psi Q \cong P \rtimes_\phi Q$.*

Lemma B: *Let p and q be distinct primes, P be a finite p-group and Q a finite q-group, and let ϕ, ψ be homomorphisms from Q to* $\mathrm{Aut}(P)$. *Suppose that* $\mathrm{Ker}\phi \not\cong \mathrm{Ker}\,\psi$. *Then $P \rtimes_\psi Q \not\cong P \rtimes_\phi Q$.*

Lemma A was proved in class (Lecture 10) and Lemma B is proved by the same argument as the assertion of the hint from [DF, Problem 7(c), p. 185] (=Problem 3 from HW#5).

So, let G be a group of order 20. Since $n_5(G) \equiv 1 \mod 5$ and $n_5(G) \mid 4$, we must have $n_5(G) = 1$, so 5-Sylow subgroup of G is normal. Hence $G = P \rtimes Q$ where P is the 5-Sylow of G and Q is a 2-Sylow of G, so $G \cong \mathbb{Z}_5 \rtimes_\phi Q$ for some $\phi : Q \to \mathrm{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_4$.

Case 1: $Q \cong \mathbb{Z}_4$. In this case a homomorphism $\phi : Q \to \mathbb{Z}_4$ is uniquely determined by $\phi(\bar{1})$ (and there are no restrictions on $\phi(\bar{1})$), so there exist four homomorphisms $\phi_i : Q \to \mathbb{Z}_4$, with $i = 0, 1, 2, 3$, given by $\phi_i(\bar{1}) = [\,\bar{i}\,]$.

The homomorphisms ϕ_0, ϕ_1 and ϕ_2 yield non-isomorphic groups by Lemma B since $\mathrm{Ker}\phi_0 \cong \mathbb{Z}_4$, $\mathrm{Ker}\phi_1$ is trivial and $\mathrm{Ker}\phi_2 \cong \mathbb{Z}_2$. On the other hand, $\mathbb{Z}_5 \rtimes_{\phi_1} Q \cong \mathbb{Z}_5 \rtimes_{\phi_3} Q$ by Lemma A since $\phi_3 = \phi_1\theta$ where $\theta \in \mathrm{Aut}(\mathbb{Z}_4)$ is given by $\theta(x) = -x$.

Case 2: $Q \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. In this case for any homomorphism $\phi : Q \to \mathbb{Z}_4$ we have $\mathrm{Im}\phi \subseteq \langle \bar{2} \rangle \cong \mathbb{Z}_2$, so $|\mathrm{Im}\phi| \leq 2$ and thus ϕ is entirely determined by its kernel. Moreover, any non-trivial subgroup of Q occurs as the kernel of some $\phi : Q \to \mathbb{Z}_4$, so there exists 3 possibilities for a non-trivial ϕ, call them ϕ_1, ϕ_2, ϕ_3, whose kernels are $\langle(\bar{1}, \bar{0})\rangle$, $\langle(\bar{0}, \bar{1})\rangle$ and $\langle(\bar{1}, \bar{1})\rangle$, respectively.

Since $\mathrm{Aut}(Q) \cong GL_2(\mathbb{Z}_2)$ acts transitively on Q, for any $i, j \in \{1, 2, 3\}$ there exists $\theta \in \mathrm{Aut}(Q)$ s.t. $\theta^{-1}\mathrm{Ker}\phi_i = \mathrm{Ker}\phi_j$. Since $\theta^{-1}\mathrm{Ker}\phi_i = \mathrm{Ker}(\phi_i\theta)$, by the previous paragraph $\phi_j = \phi_i\theta$. Hence by Lemma A, ϕ_1, ϕ_2 and ϕ_3 yield isomorphic groups. On the other hand, the trivial homomorphism and ϕ_1 yield non-isomorphic groups by Lemma B (or simply because one group is abelian and the other is not).

Thus, we have three isomorphism classes of groups of order 20 in Case 1 and two isomorphism classes in Case 2. Any group from Case 1 cannot be isomorphic to any group from Case 2 since they have non-isomorphic Sylow 2-subgroups. Thus, we proved that there are $3+2=5$ isomorphism classes of groups of order 20.

5. Let X be a finite set and $F = F(X)$ the (standard) free group on X.

Definition: An element $g \in F$ is called cyclically reduced (with respect to X) if the reduced word representing g is of the form $x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ (with $x_i \in X$, $\varepsilon_i = \pm 1$) where $x_n^{\varepsilon_n} \neq (x_1^{\varepsilon_1})^{-1}$.

(a) Prove that any element $g \in F$ is conjugate to a cyclically reduced element.

(b) Prove that if $f \in F$ and $n \in \mathbb{N}$, then f^n is cyclically reduced if and only if f is cyclically reduced.

(c) Prove that if $f, g \in F$ and $f^n = g^n$ for some $n \in \mathbb{N}$, then $f = g$. Explain the argument in detail. **Hint:** First consider the case when f is cyclically reduced and then treat the general case.

(d) Now prove that if $f, g \in F$ and $f^n = g^m$ for some $n, m \in \mathbb{N}$, then f and g commute. **Hint:** Use (c).

Solution: (a) Let $g = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ with $x_i \in X$ and $\varepsilon_i = \pm 1$. Let k be the largest non-negative integer s.t. $k \leq n/2$ and $x_i^{\varepsilon_i} = (x_{n+1-i}^{\varepsilon_{n+1-i}})^{-1}$ for all $1 \leq i \leq k$. Then $g = aba^{-1}$ where $a = \prod_{i=1}^{k} x_i^{\varepsilon_i}$ and $b = \prod_{i=k+1}^{n-k} x_i^{\varepsilon_i}$, and by construction b is cyclically reduced.

(b) In parts (b)-(d), to avoid any ambiguity in the notations, given $u, v \in F(X)$, by uv we denote the concatenation of u and v (without cancellations). Given a (possibly) non-reduced word u, by $[u]$ we shall denote the unique reduced word equivalent to u. In this notation (b) is restated as follows:

If f is reduced, then f is cyclically reduced $\iff$ $[f^n]$ is cyclically reduced

Given a word $u = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ we shall refer to $x_1^{\varepsilon_1}$ (resp. $x_n^{\varepsilon_n}$) as the first (resp. last) factor of u.

Now take $f \in F(X)$ and write $f = aba^{-1}$ as in part (a). Then $[f^n] = [(aba^{-1})^n] = [ab^n a^{-1}]$. The word $ab^n a^{-1}$ is reduced – if not, then one of the words ab, ba^{-1} or bb would not be reduced, which is impossible – ab and ba^{-1} are reduced since they are subwords of the reduced word f and bb is reduced since b is cyclically reduced. Thus, $[f^n] = ab^n a^{-1}$.

"$\Rightarrow$" Assume that f is cyclically reduced. Then $a = e$, the empty word and hence $[f^n] = b^n = f^n$. Thus, the first (resp. last) factor of f coincides with the first (resp. last) factor of $[f^n]$. So $[f^n]$ is cyclically reduced since f is cyclically reduced.

"$\Leftarrow$" Now assume that f is not cyclically reduced. Then $a \neq e$, so the first factor of $[f^n]$ is the first factor of a and the last factor of $[f^n]$ is the last factor of a^{-1}. Since the last factor of a^{-1} is the inverse of the first factor of a, we conclude that $[f^n]$ is not cyclically reduced.

(c) First assume that f is cyclically reduced. Then by (b), $[f^n]$ is cyclically reduced, so $[g^n]$ is cyclically reduced and again by (b) g is cyclically reduced. In this case, as follows from the proof of (b), $f^n = [f^n] = [g^n] = g^n$, so $f^n = g^n$ (as words).

Assume that $f = x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}$ and $g = y_1^{\delta_1} \dots y_m^{\delta_m}$, with $x_i, y_i \in X$ and $\varepsilon_i, \delta_i = \{\pm 1\}$. Then

$$f^n = \underbrace{x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k} \cdot \ldots \cdot x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}}_{n \text{ times}} \text{ and}$$

$$g^n = \underbrace{y_1^{\delta_1} \dots y_m^{\delta_m} \cdot \ldots \cdot y_1^{\delta_1} \dots y_m^{\delta_m}}_{n \text{ times}}.$$

Since $f^n = g^n$ as words, we know that $x_i^{\varepsilon_i} = y_i^{\delta_i}$ (and so $x_i = y_i$ and $\varepsilon_i = \delta_i$) for $i \leq \min\{m, k\}$. Moreover, $nk = \mathit{length}(f^n) = \mathit{length}(g^n) = nm$, so $k = m$. Combining the last two results, we conclude that $f = g$.

Now we treat the general case. By (a), $f = aba^{-1}$ where b is cyclically reduced. Then $[g^n] = [f^n] = [(aba^{-1})^n] = ab^n a^{-1}$, so $b^n = [a^{-1} g^n a] = [(a^{-1} g a)^n]$. Hence $b = [a^{-1} g a]$ by the special case proved above, and therefore $g = [a(a^{-1} g a) a^{-1}] = [aba^{-1}] = [f] = f$.

(d) Assume that $[f^n] = [g^m]$. Then $[(fgf^{-1})^m] = [fg^m f^{-1}] = [ff^n f^{-1}] = [f^n] = [g^m]$. Hence by (c), $[fgf^{-1}] = [g]$, so $[fg] = [gf]$.