MATH 511A, SOLUTIONS 8

1. The relations $bd = db$ and $bd = d^2b$ imply $d = 1$. Then $c^2 = dcd^{-1} = c$ implies $c = 1$. Now $b^2 = c^{-1}ac = a$, so a commutes with b. Then $a^2 = bab^{-1} = a$, so $a = 1$, and b has order at most 2. Summary: $a, c, d = 1$ and b has order at most 2. Since G is generated by a, b, c, d, it follows that $\#G \leq 2$. On the other hand we can check that there is a map $G \to \mathbb{Z}/2\mathbb{Z}$ sending a, c, d to 0 and b to 1. Hence $\#G = 2$.

2. Let G be a finite group, and let S be the set underlying G. Let T be the (finite) set of all symbols xyz^{-1} for elements $x, y, z \in S$ such that $xy = z$ in G. We claim that $G \cong \langle S \mid T \rangle$.

Certainly there is a surjective homomorphism $\langle S \mid T \rangle \to G$. Indeed, consider the homomorphism $\phi : F(S) \to G$ sending $\phi(x) = x$ for all $x \in S$. Since the image of the word xyz^{-1} under ϕ is $xyz^{-1} = 1$ in G, we see that $T \subset \ker(\phi)$, so we have a homomorphism $\langle S \mid T \rangle \to G$.

To complete the proof, let us show that $\#\langle S \mid T \rangle = \#G$. Let $w \in \langle S \mid T \rangle$ be written as a word in S. If the word is a product of at least two symbols (elements of S or inverses of elements of S), then we can always replace two symbols with one symbol. As an example, if $x, y \in S$ then $y^{-1}x^{-1} = z^{-1}(xyz^{-1})^{-1} = z^{-1}$, where $z \in S$ is the element such that $xy = z$ in G. Thus every word can be reduced to a word of length at most one. Moreover, since $eee^{-1} \in T$, the word e is equivalent to the empty word. Also, if $xy = e$, then the word x^{-1} is equivalent to $x^{-1}(xye^{-1}) = ye^{-1} = y$. Hence every word of length at most one is equivalent to the word x for some $x \in S$. Therefore $\#\langle S \mid T \rangle = \#S = \#G$.

3. Solution 1: Write $X = A \cup (X \setminus A)$. By definition $F(X)/N = \langle X \,|\, A \rangle$. By von Dyck's theorem there exists a map $f : \langle X \,|\, A \rangle \to F(X \setminus A)$ by sending $xN \mapsto 1$ if $x \in A$ and $xN \mapsto x$ if $x \in X \setminus A$.

On the other hand, by the universal property of free groups there exists a map $g : F(X \setminus A) \to \langle X \,|\, A \rangle$ sending $x \mapsto xN$ for all $x \in X \setminus A$. It is easy to check that $f \circ g$ is the identity on $F(X)/N$ and that $g \circ f$ is the identity on $F(X \setminus A)$, hence both maps are isomorphisms and $F(X)/N$ is free (and isomorphic to $F(X \setminus A)$).

Solution 2. We begin with a lemma.

Lemma: If a group G is generated by a set S, and $h, h' : G \to H$ are two homomorphisms such that $h(s) = h'(s)$ for all $s \in S$, then $h = h'$.

Proof. Let K be the subset of G consisting of all elements x for which $h(x) = h'(x)$. It is easy to check that K is a subgroup of G. Since $S \subset K$ and S generates G, it follows that $K = G$, and so $h = h'$. □

We wish to prove that F/N is the free group on the basis $X \setminus A$ — or, more precisely, on the basis $\{xN : x \in X \setminus A\}$. Let G be an arbitrary group, and let f be any map of sets from $X \setminus A \to G$. We must show that f extends to a unique homomorphism $g : F/N \to G$ such that $g(xN) = f(x)$ for $x \in X \setminus A$.

Extend f to a function $\widetilde{f} : X \to G$ by setting $\widetilde{f}(a) = 1$ if $a \in A$. By the defining property of F, the function $\widetilde{f}$ extends to a homomorphism $\widetilde{g} : F \to G$. Since $\widetilde{f}(a) = 1$ if $a \in A$, we have $A \subset \ker(\widetilde{g})$, and therefore $N \subset \ker(\widetilde{g})$. So, we have a homomorphism $g : F/N \to G$, obtained by sending $g(wN) = \widetilde{g}(w)$ if $w \in F$. In particular

$$g(xN) = \widetilde{g}(x) = \widetilde{f}(x) = f(x)$$

if $x \in X \setminus A$, as desired.

To show that the extension g is unique, by the Lemma it is enough to show that the set $\{xN : x \in X \setminus A\}$ generates F/N. Here is one way to see this: certainly $\{xN : x \in X\}$ generates F/N (this follows immediately from the fact that X generates F), but every coset aN for $a \in A$ is just the identity coset in F/N.

4. Throughout this problem we suppose that F is free on the set X.

(i) If $w \in F$ is not the identity, we prove by induction on the length of w as a reduced word that w does not have finite order. For the base case, if the length of w is 1, then $w = x$ or $w = x^{-1}$ for some $x \in X$. Then $w^n = xx \cdots x$ or $x^{-1}x^{-1} \cdots x^{-1}$, and this is a reduced word, so $w^n \neq 1$.

Now suppose the result is true for words of length at most $\ell - 1$, and suppose w has length ℓ. Write w as a reduced word $w = xw'y$, where w' has length $\ell - 2$. Recall that w^n is obtained by juxtaposing n copies of w. If $w^n = 1$, then this juxtaposition must not be a reduced word, i.e. two adjacent symbols in the word must be inverse to one another. Since w was itself reduced, and the only new juxtaposition is yx, it follows that x and y must be inverse to one another. Therefore w is conjugate to w'. Since w has finite order, so does w'. Since w' is a shorter word, by our induction hypothesis $w' = 1$, so $w = 1$ as well. This contradicts our assumption that w has length ℓ, and the induction follows.

(ii) **Solution 1:** If $|X| = 1$, then F is certainly abelian (it is the cyclic group generated by the single element $x \in X$). On the other hand, if $|X| > 1$, let x, y be two elements in X. Let G be any non-abelian group, and let $a, b \in G$ be two elements such that $ab \neq ba$. By the defining property of F, there exists a homomorphisms $f : F \to G$ such that $f(x) = a$ and $f(y) = b$. Since $f(xy) \neq f(yx)$, we know that $xy \neq yx$.

Solution 2: If $x, y \in X$ are two elements, then xy and yx are distinct reduced words, so they are not the same element in F.

(iii) Suppose $\#S > 1$. Let $w \in F(S)$ be a reduced word of nonzero length n, and suppose that the first character of the word w is either a or a^{-1}, where $a \in S$. Choose $b \in S$ with $b \neq a$. We will prove that $bw \neq wb$.

Suppose $bw = wb$. Since b is not the inverse of the first character of w, the concatenation bw is reduced. Therefore bw has length $n + 1$, and its first character is b. Since we have assumed $bw = wb$, it follows that the length of wb is $n + 1$, and so the concatenation wb is already reduced. But then the first character of wb is either a or a^{-1}, which is not equal to b. This is a contradiction. Hence $bw \neq wb$, and $w \notin Z(F(S))$.

5.

(i) To check that T has at most 12 elements, we prove that every element of T can be written in the form $a^i b^j$ with $0 \leq i \leq 5$ and $0 \leq j \leq 1$.

Since the set of elements of the form $a^i b^j$ with $0 \leq i \leq 5$ and $0 \leq j \leq 1$ is finite and contains a, b, it suffices to show that this set is closed under multiplication.

Using the relations $a^6 = 1$ and $b^2 = a^3$, it suffices to show that ba^i has the desired form. The relation $a^3 = abab$ implies $ba = a^2 b^{-1}$, so $bab^{-1} = a^2 b^{-2} = a^{-1}$. Hence $ba^i = a^{-i} b$, as desired.

(ii) Since C has order 3 and B has order 4, it follows that G has order at least 12. Let $A = CB^2 = -C$. Let us map $T \to G$ by sending $a \mapsto A$ and $b \mapsto B$. We observe that $A = -C$ has order 6, and calculate that $(AB)^2 = A^3 = (AB)^2 = -I$. Therefore our map $T \to G$ is a homomorphism, and it is surjective since the image contains both C and B. Since $\#G \geq 12$ and $\#T \leq 12$, the map is an isomorphism and both groups have order 12.

(iii) Since T has an element of order 6 but A_4 does not, T is not isomorphic to A_4. Since T has elements of order 4 (e.g. B) but D_{12} does not, T is not isomorphic to D_{12}.