**21-373, Algebraic Structures**, Department of Mathematical Sciences, Carnegie Mellon University
**Fall 2011**: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

17- Friday October 7, 2011.

**Definition 17.1**: If $X$ is a set, a *word* on $X$ is a finite sequence (possibly empty) from $X \times \mathbb{Z}$, and one writes $x_1^{n_1} \cdots x_k^{n_k}$ for the word whose entry $\#i$ is $(x_i, n_i)$.

A word is *reduced* if neither of the two following *reduction rules* applies: $a\, x^m x^n\, b$ is replaced by $a\, x^{m+n} b$, and $a\, x^0 b$ is replaced by $a\, b$, for any two words $a, b$ (possibly empty).

**Lemma 17.2**: Any word can be reduced by finitely many applications of the reduction rules, and the reduced word does not depend upon the order of the operations of reduction.
*Proof*: Each application of the reduction rules makes the length of the word decrease, so that only a finite number of reductions can be done; the empty word is reduced.

Various applications of the first reduction rule are independent, i.e. they can be done in any order. An application of the second reduction rule may have the effect that more successive powers of the same $x$ appear, but applying the first reduction rule to these powers of $x$ before or after applying the second reduction rule makes no difference, so that whatever the order of the operations of reduction, the result is always the same.

**Lemma 17.3**: The set $R$ of reduced word is a group for the operation where $a\, b$ is the reduced form of the *concatenation* $a \star b$ (made of $a$ on the left and $b$ on the right). It is called the *free group* on $X$,[1] and denoted $Fr(X)$.
*Proof*: Associativity applies to concatenation, i.e. $(a \star b) \star c = a \star (b \star c)$, and the reduced form is either the reduced form of $(a\, b) \star c$, which is $(a\, b)\, c$, or the reduced form of $a \star (b\, c)$, which is $a\, (b\, c)$, and these reduced forms are equal by Lemma 17.2, so that the operation is associative. The identity is the empty word, and the inverse of $x_1^{n_1} \cdots x_\ell^{n_\ell}$ is $x_\ell^{-n_\ell} \cdots x_1^{-n_1}$.

**Lemma 17.4**: (universal property) Identifying $x \in X$ with $i(x) = x^1 \in Fr(X)$, one has $\langle X \rangle = Fr(X)$, and for any group $G$ and any mapping $f$ from $X$ into $G$, there is a unique homomorphism $\psi(f)$ from $Fr(X)$ into $G$ which extends $f$. Moreover, these properties characterize $Fr(X)$ up to an isomorphism.
*Proof*: An element of $Fr(X)$ is either the empty word, or has the form $x_1^{n_1} \cdots x_\ell^{n_\ell}$ with $n_1, \ldots, n_\ell \in \mathbb{Z} \setminus \{0\}$, and $x_j \neq x_k$ whenever $|j - k| = 1$, and such an element belongs to $\langle X \rangle$, which then coincides with $Fr(X)$. If $F$ is an homomorphism from $Fr(X)$ into $G$ extending $f$, i.e. such that $F(x) = f(x)$ for every $x \in X$, then one must have $F(x_1^{n_1} \cdots x_\ell^{n_\ell}) = F(x_1^{n_1}) \cdots F(x_\ell^{n_\ell}) = \big(F(x_1)\big)^{n_1} \cdots \big(F(x_\ell)\big)^{n_\ell} = \big(f(x_1)\big)^{n_1} \cdots \big(f(x_\ell)\big)^{n_\ell}$, so that $F$ can only be given by the preceding formula, and one must check that this formula defines an homomorphism, which is the desired $\psi(f)$. For proving it, one notices that the same formula applies to all words even if they are not reduced, so that one automatically has $F(a \star b) = F(a)\, F(b)$ for all words, and then that the reduction rules do not affect the value of $F$, i.e. $F(a\, x^m x^n b) = F(a) \big(F(x)\big)^m \big(F(x)\big)^n F(b)$, which is $F(a) \big(F(x)\big)^{m+n} F(b)$, i.e. $F(a\, x^{m+n} b)$, and, similarly, that $F(a\, x^0 b) = F(a)\, e\, F(b)$, which is $F(a)\, F(b)$, i.e. $F(a\, b)$.

Denoting $i$ the injection of $X$ into $Fr(X)$, one has $\psi(f) \circ i = f$ for all $f$; one then assumes that there is another solution $\widetilde{X}$ of the universal problem, with $\widetilde{i}$ the injection of $X$ into $\widetilde{X}$ and $\widetilde{\psi}(f)$ the corresponding extension of $f$, so that one has $\widetilde{\psi}(f) \circ \widetilde{i} = f$ for all $f$. Then $\psi(\widetilde{i})$ is an homomorphism from $Fr(X)$ into $\widetilde{X}$, and $\widetilde{\psi}(i)$ is an homomorphism from $\widetilde{X}$ into $Fr(X)$, and they satisfy $\psi(\widetilde{i}) \circ i = \widetilde{i}$ and $\widetilde{\psi}(i) \circ \widetilde{i} = i$ on $X$; one deduces that $\psi(\widetilde{i}) \circ \widetilde{\psi}(i) \circ \widetilde{i} = \widetilde{i}$ on $X$, so that the two homomorphisms $\psi(\widetilde{i}) \circ \widetilde{\psi}(i)$ and $id$ (the identity mapping) coincide on $\widetilde{i}(X)$, and then on the subgroup it generates, i.e. $\widetilde{X}$; similarly $\widetilde{\psi}(i) \circ \psi(\widetilde{i})$ is $id$ on $Fr(X)$, so that $\psi(\widetilde{i})$ is an isomorphism from $Fr(X)$ onto $\widetilde{X}$, with inverse $\widetilde{\psi}(i)$.

**Lemma 17.5**: A mapping $f$ from $X_1$ into $X_2$ induces an homomorphism $\psi(f)$ from $Fr(X_1)$ into $Fr(X_2)$, such that $\psi(f) \circ i_1 = i_2 \circ f$, where $i_k$ is the injection of $X_k$ into $Fr(X_k)$. If $g$ is a mapping from $X_2$ into $X_3$ and $h = g \circ f$, then $\psi(h) = \psi(g) \circ \psi(f)$, so that a bijection $f$ from $X_1$ onto $X_2$ induces an isomorphism

[1] It is free of any relations, like those considered in Lemma 17.8.

$\psi(f)$ from $Fr(X_1)$ onto $Fr(X_2)$. If $|X| = n$, one speaks of $Fr(X)$ as *the free group on n elements*, so that if a group $G$ has a generating set $\{g_1, \ldots, g_n\}$, it is an homomorphic image of the free group on $n$ elements.
*Proof*: An homomorphism $\psi$ from a group $G_1$ into a group $G_2$ is uniquely determined by its values on a generating set $Z_1$ of $G_1$; here $G_k = Fr(X_k)$ and $Z_k = i_k(X_k)$. Because $\psi(h)$ and $\psi(g) \circ \psi(f)$ coincide on $i_1(X_1)$, which generates $Fr(X_1)$, they are equal. If $g = f^{-1}$, $h = id$ and $\psi(id) = id$ (where $id$ denotes the identity mapping on various sets). On then uses $X_1 = \{1, \ldots, n\}$, $X_2 = \{g_1, \ldots, g_n\}$ with $f(i) = g_i$, $i = 1, \ldots, n$.

**Lemma 17.6**: If for a group $G$ a subset $Y \subset G$ is stable by conjugation (i.e. for all $g \in G$, $y \in Y$ implies $y^g \in Y$), then $\langle Y \rangle \lhd G$. For $X \subset G$, the smallest $N \lhd G$ containing $X$ is $\langle Y_X \rangle$ for $Y_X = \bigcup_{g \in G} X^g$.
*Proof*: To prove that $\langle Y \rangle$ is a normal subgroup of $G$, one must show that $a \in \langle Y \rangle$ and $g \in G$ imply $a^g \in \langle Y \rangle$. Indeed, since $a = y_1^{n_1} \cdots y_k^{n_k}$ for some $y_1, \ldots, y_k \in Y$, $n_1, \ldots, n_k \in \mathbb{Z}$, and $k \geq 1$, one has $a^g = (y_1^g)^{n_1} \cdots (y_k^g)^{n_k}$, and because $Y$ is stable by conjugation one has $y_1^g, \ldots, y_k^g \in Y$, so that $a^g \in \langle Y \rangle$.

If $N$ is normal and contains $X$, then $N$ contains $X^g$ for all $g \in G$, i.e. $N$ contains $Y_X$, so that $N$ must contain $\langle Y_X \rangle$; on the other hand $Y_X$ is stable by conjugation (because $(X^g)^h = X^{g\,h}$), so that $\langle Y_X \rangle$ is normal subgroup of $G$, and it then is the smallest normal subgroup of $G$ containing $X$.

**Lemma 17.7**: For $E \subset Fr(X)$, let $N$ be the smallest normal subgroup of $Fr(X)$ containing $E$ (as in Lemma 17.6), then the quotient group $Fr(X)/N$ has a universal property: if $G$ is a group and $f$ is a mapping from $X$ into $G$ such that, whenever $x_1^{n_1} \cdots x_k^{n_k} \in E$ one has $\big(f(x_1)\big)^{n_1} \cdots \big(f(x_k)\big)^{n_k} = e$, then there is an homomorphism $\chi(f)$ from $Fr(X)/N$ into $G$ such that $\chi(f) \circ \pi = \psi(f)$, or $\chi(f) \circ \pi \circ i = f$, where $\pi$ is the projection from $Fr(X)$ onto $Fr(X)/N$.
*Proof*: The kernel of the homomorphism $F = \chi(f)$ contains all the words $x_1^{n_1} \cdots x_k^{n_k}$ which belong to $E$, and since it is a normal subgroup of $Fr(X)$, it must contain $N$. Then $F$ induces a map $\overline{F}$ from $Fr(X)/N$ into $G$ by $\overline{F}(a\,N) = F(a)$, and $\overline{F}$ is the desired $\chi(f)$.

**Lemma 17.8**: If $G = \langle g_1, \ldots, g_n \rangle$ (with not necessarily distinct $g_i$), and equations $E_1, \ldots, E_m$ hold in $G$, where each equation is of the form $\gamma_1^{n_1} \cdots \gamma_k^{n_k} = e$, where $\gamma_i \in \{g_1, \ldots, g_n\}$, $n_i \in \mathbb{Z}$ for $i = 1, \ldots, k$ (and $k \geq 1$); let $X = \{x_1, \ldots, x_n\}$ and $E^* \subset Fr(X)$ be the corresponding set of $y_1^{n_1} \cdots y_k^{n_k}$, where $y_i = x_j$ if $\gamma_i = g_j$, and let $N$ be the smallest normal subgroup of $Fr(X)$ containing $E^*$, then there is a surjective homomorphism from $Fr(X)/N$ onto $G$.
*Proof*: One defines $f$ from $X$ into $G$ by $f(x_i) = g_i$ for $i = 1, \ldots, n$, and Lemma 17.7 applies to $E^*$, and the desired homomorphism is $F = \chi(f)$, which is surjective because $F(x_i N) = g_i$ for $i = 1, \ldots, n$, and the $g_i$ generate $G$.

**Remark 17.9**: *Changing the notation* used before, $D_n$, the dihedral group of degree $n \geq 3$ (and order $2n$) is generated by $a$ and $b$, where $a$ is complex conjugation, and $b$ is multiplication by $e^{2i\,\pi/n}$, so that $a^2 = b^n = e$, and $D_n = \{e, b, \ldots, b^{n-1}, a, a\,b \ldots, a\,b^{n-1}\}$, with the relation $b^k a = a\,b^{-k}$ for all $k \in \mathbb{Z}$.

In the complex plane $\mathbb{C}$, the property $c\,a = a\,c^{-1}$ is true if $a$ is complex conjugation and $c$ is multiplication by any complex number $\rho$ of modulus 1, since $\rho^{-1} = \overline{\rho}$, and for any $z \in \mathbb{C}$ one has $c\,a(z) = \rho\,\overline{z} = \overline{\overline{\rho}\,z} = \overline{\rho^{-1}\,z} = a\,c^{-1}(z)$. Since $a^2 = e$, and $c\,a = a\,c^{-1}$ is equivalent to $a\,c\,a\,c = e$, it is useful to deduce the consequences in a purely algebraic way.

**Lemma 17.10**: If in a group $G$ one has $a^2 = e$ and $a\,b\,a\,b = e$,[2] then $a\,b^k = b^{-k}a$ for all $k \in \mathbb{Z}$ (equivalently $b^\ell a = a\,b^{-\ell}$ for all $\ell \in \mathbb{Z}$), and more generally, $a^{\alpha_1} b^{\beta_1} \cdots a^{\alpha_m} b^{\beta_m} = a^\alpha b^\beta$ with $\alpha = \alpha_1 + \ldots + \alpha_m \pmod 2$, and $\beta = (-1)^{\alpha_2 + \ldots + \alpha_m}\beta_1 + (-1)^{\alpha_3 + \ldots + \alpha_m}\beta_2 + \ldots + (-1)^{\alpha_m}\beta_{m-1} + \beta_m$.
*Proof*: Multiplying $a\,b\,a\,b = e$ by $b^{-1}a$ on the right, one deduces that $a\,b = b^{-1}a$, which after multiplying by $a$ on the left and on the right gives $a\,b^{-1} = b\,a$. Then, one uses induction for deducing that $a\,b^k = b^{-k}a$ for $k \geq 1$ from $a\,b = b^{-1}a$, and similarly $a\,b^{-k} = b^k a$ for $k \geq 1$ is deduced from $a\,b^{-1} = b\,a$: indeed, $a\,b^k = b^{-k}a$ implies $a\,b^{k+1} = (a\,b^k)\,b = (b^{-k}a)\,b = b^{-k}(b^{-1}a) = b^{-(k+1)}a$. Then, in a general term $a^{\alpha_1} b^{\beta_1} \cdots a^{\alpha_m} b^{\beta_m}$ one can push all the powers of $a$ to the left, and a power $b^\gamma$ will stay $b^\gamma$ if the sum of powers of $a$ to the right of it is even, or be changed into $b^{-\gamma}$ if the sum of powers of $a$ to the right of it is odd.

**Remark 17.11**: One deduces that if $G = \langle a, b \rangle$, with $a^2 = e$ and $a\,b\,a\,b = e$, then $G = \{b^k, k \in \mathbb{Z}\} \bigcup \{a\,b^\ell \mid \ell \in \mathbb{Z}\}$ and for all $k, \ell \in \mathbb{Z}$ one has $b^k\,b^\ell = b^{k+\ell}$, $b^k\,(a\,b^\ell) = a\,b^{-k+\ell}$, $(a\,b^k)\,b^\ell = a\,b^{k+\ell}$, $(a\,b^k)\,(a\,b^\ell) = b^{-k+\ell}$.

[2] With $a \neq b$, it happens if $G$ contains a copy of $\mathbb{Z}_2 \times \mathbb{Z}_2$, or a copy of $D_n$ for some $n \geq 3$.

**Lemma 17.12**: If $X = \{x_1, x_2\}$, then the smallest normal subgroup $N$ of $Fr(X)$ containing $x_1^2$ and $x_1x_2x_1x_2$ is made up of the words $x_1^{\alpha_1}x_2^{\beta_1}\cdots x_1^{\alpha_m}x_2^{\beta_m}$ (reduced so that no exponent is 0 except perhaps $\alpha_1$ if the word starts with a power of $x_2$, or $\beta_m$ if the word ends with a power of $x_1$) such that $\alpha_1 + \ldots + \alpha_m = 0 \pmod 2$ and $(-1)^{\alpha_2+\ldots+\alpha_m}\beta_1 + (-1)^{\alpha_3+\ldots+\alpha_m}\beta_2 + \ldots + (-1)^{\alpha_m}\beta_{m-1} + \beta_m = 0$.
*Proof*: If $N$ is any normal subgroup of $Fr(X)$, and if $s\,t \in N$ for two words $s, t \in Fr(X)$, and $u \in N$, then $s\,u\,t \in N$, since it is $(s\,u\,s^{-1})\,(s\,t)$ and $s\,u\,s^{-1} \in N$ since $N \triangleleft Fr(X)$. One assumes then that $x_1^2$ and $x_1x_2x_1x_2$ belong to $N$, and one has $x_2x_1x_2x_1 = x_1^{-1}(x_1x_2x_1x_2)x_1 \in N$ since $N \triangleleft Fr(X)$. Using $s = t = x_1x_2$ and $u = x_2x_1x_2x_1$ gives $x_1x_2^2x_1x_2x_1^2x_2 \in N$, and inserting $x_1^{-2}$ to cancel $x_1^2$ gives $x_1x_2^2x_1x_2^2 \in N$, and by induction $x_1x_2^kx_1x_2^k \in N$ for $k \geq 1$; by conjugation with $x_1^{-1}$, one deduces that $x_2^kx_1x_2^kx_1 \in N$ since $N \triangleleft Fr(X)$, and by inversion one deduces that the same holds with $k$ replaced by $-k$. One can then replace a piece of a word $x_2^\beta x_1$ by $x_1x_2^{-\beta}$, by inserting $x_1^2$ on the left and $x_1x_2^{-\beta}x_1x_2^{-\beta}$ on the right, giving $x_1^2(x_2^\beta x_1)\,x_1x_2^{-\beta}x_1x_2^{-\beta}$, which is $x_1x_2^{-\beta}$ after insertions of $x_1^{-2}$ and cancellations; this gives a way to start from an element of $N$ and create other elements of $N$ by pushing the $x_1$ to the left, so that their total number must be even, and no $x_2$ should be left. Finally, one checks that the family considered is stable by multiplication and inversion, so that it defines a subgroup, and that it is stable by conjugation by $x_1$ or by $x_2$ (hence by any element of $Fr(X)$), so that it is a normal subgroup of $Fr(X)$.

**Remark 17.13**: If $G = \langle a, b\rangle$, and $a^2 = e$, $b^n = e$, $a\,b\,a\,b = e$, then $G = \{e, b, \ldots, b^{n-1}, a, a\,b, \ldots, a\,b^{n-1}\}$, and $G$ is isomorphic to $D_n$ if one adds $e \neq a \neq b \neq e$ and $n \geq 3$.[3] More generally, $a^{\alpha_1}b^{\beta_1}\cdots a^{\alpha_m}b^{\beta_m} = a^\alpha b^\beta$ if $\alpha = \alpha_1 + \ldots + \alpha_m \pmod 2$, and $\beta = (-1)^{\alpha_2+\ldots+\alpha_m}\beta_1 + (-1)^{\alpha_3+\ldots+\alpha_m}\beta_2 + \ldots + (-1)^{\alpha_m}\beta_{m-1} + \beta_m \pmod n$. This follows from Lemma 17.10 if one notices that $b^\beta$ only depends upon what $\beta$ is modulo $n$.

[3] If $e \neq a \neq b \neq e$ and $n = 2$, then $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. If $a = e \neq b$, or if $a = b \neq e$, then $G \simeq \mathbb{Z}_2$ if $n$ is even, and $G = \{e\}$ if $n$ is odd. If $a \neq b = e$, then $G \simeq \mathbb{Z}_2$. If $a = b = e$, then $G = \{e\}$.