Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

15- Monday October 3, 2011.

**Definition 15.1**: For a group $G$, the *center* $Z(G)$ is the set of elements which commute with all elements of $G$, so that $Z(G) = G$ if and only if $G$ is Abelian.

**Lemma 15.2**: $Z(G)\,char\,G$, and $N \leq Z(G)$ implies $N \lhd G$.[1]

In the $G$-action on $G$ by conjugation, $Z(G)$ is the kernel of the homomorphism from $G$ into $S_G$, and it is the set of fixed points.[2]

*Proof*: If $z \in Z(G)$ and $g \in G$, one has $z\,g = g\,z$, and if $\psi$ is any automorphism of $G$ one deduces that $\psi(z)\,\psi(g) = \psi(z\,g) = \psi(g\,z) = \psi(g)\,\psi(z)$, so that $\psi(z)$ commutes with all elements in $\psi(G)$, which is $G$, and this proves that $\psi(z) \in Z(G)$. Then, $\psi\big(Z(G)\big) \subset Z(G)$ for all $\psi \in Aut(G)$ implies $\psi\big(Z(G)\big) = Z(G)$ for all $\psi \in Aut(G)$,[3] i.e. $Z(G)$ is characteristic in $G$.

For $g \in G$, the conjugation $\psi_g$ is the identity on $Z(G)$ (since $\psi_g(x) = g\,x\,g^{-1} = x\,g\,g^{-1} = x$ for all $x \in Z(G)$), so that it is the identity on $N$, hence $\psi_g(N) = N$, and since it holds for all $g \in G$ it means $N \lhd G$.

An element $g \in G$ belongs to the kernel of the homomorphism from $G$ into $S_G$ if $h \mapsto h^g = g\,h\,g^{-1}$ is the identity mapping, i.e. $g\,h\,g^{-1} = h$ for all $h \in G$, which is $g\,h = h\,g$ for all $h \in G$, i.e. $g \in Z(G)$. If an element $a \in G$ is a fixed point of the action by conjugation, it means that $g\,a\,g^{-1} = a$ for all $g \in G$, i.e. $g\,a = a\,g$ for all $g \in G$, so that $a \in Z(G)$.

**Lemma 15.3**: If $G/Z(G)$ is cyclic, then $G$ is Abelian, so that $Z(G) = G$.

*Proof*: $Z(G)$ is a normal subgroup of $G$ by Lemma 15.2, and if the quotient is generated by $a\,Z(G)$, then $G = \{a^n z \mid n \in \mathbb{Z}, z \in Z(G)\}$, and since $(a^n z)\,(a^m z') = a^{n+m} z\,z' = (a^m z')\,(a^n z)$, $G$ is Abelian.

**Definition 15.4**: For a prime $p$, a *p-group* is a group (not necessarily finite) in which the order of every element is finite and is a power of $p$ (so that the trivial group $\{e\}$ is a $p$-group, and a non-trivial finite $p$-group has order $p^k$ for some $k \geq 1$ by Cauchy's theorem).

**Lemma 15.5**: If $G$ is a non-trivial finite $p$-group, then $p$ divides $|Z(G)|$, so that the center $Z(G)$ is not reduced to $\{e\}$.

*Proof*: In the action of $G$ by conjugation, the size of any orbit divides the order of $G$, so that it is a power of $p$. Because the size of an orbit is 1 only for the elements of $Z(G)$ by Lemma 15.2, and all other orbits have for size a multiple of $p$, the order of $Z(G)$ must be a multiple of $p$.

**Remark 15.6**: This shows the result mentioned before, that no simple group $G$ has order $p^k$ with $p$ prime and $k \geq 2$, since either $Z(G) \neq G$ and it is a non-trivial and proper normal subgroup, or $Z(G) = G$ in which case $G$ is Abelian, and has a normal subgroup of order $p$ by Cauchy's theorem.

**Lemma 15.7**: If $p$ is a prime, and $G$ is a group of order $p^2$, then $G$ is Abelian, and it is isomorphic to either $\mathbb{Z}_p \times \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$.

*Proof*: By Lemma 15.5, the order of $Z(G)$ is a multiple of $p$, so that $G/Z(G)$ has order 1 or $p$, hence it is either the trivial group or it is isomorphic to $\mathbb{Z}_p$, i.e. it is a cyclic group, so that $G$ is Abelian by Lemma 15.3. By Cauchy's theorem, there is an element $a \in G$ of order $p$, generating a subgroup $H$ of order $p$; let $b \notin H$, generating a subgroup $K$: if $K$ contains $H$ it must coincide with $G$,[4] in which case $G$ is cyclic and isomorphic to $\mathbb{Z}_{p^2}$, or $K$ has size $p$ with $H \cap K = \{e\}$, and $G = \{a^m b^n \mid m, n \in \{0, \ldots, p-1\}\}$ which is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

---

[1] Notice that Lemma 7.11, which says that $A\,char\,B \lhd C$ implies $A \lhd C$ does not apply here.

[2] An action of a group $G$ on a set $X$ is an homomorphism $\psi$ from $G$ into $S_X$ (the group of bijections of $X$ onto itself, with composition), so that the kernel of $\psi$ is a (normal) subgroup of $G$, while the set of fixed points is a subset of $X$, namely those $x \in X$ for which that stabilizer $Stab_x$ is $G$ (so that orbit of $x$ is reduced to $\{x\}$). Here $X = G$.

[3] Since $\psi$ is invertible, applying $\psi^{-1}$ to $\psi\big(Z(G)\big) \subset Z(G)$ gives $Z(G) \subset \psi^{-1}\big(Z(G)\big) \subset Z(G)$.

[4] By Lagrange's theorem, the order of a subgroup of $G$ can only be 1, $p$, or $p^2$.

**Remark 15.8**: A group $G$ of order $p^3$ is not necessarily Abelian, since there are two distinct non-Abelian groups of order 8, the dihedral group $D_4$ and the quaternion group $Q_8$.

**Remark 15.9**: It was mentioned that the only simple Abelian groups are the $\mathbb{Z}_p$ for $p$ prime as a consequence of the structure theorem of finite Abelian groups which will be proven in another lecture, and it says that a non-trivial finite Abelian group $G$ is isomorphic to some product $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ for some $k \geq 1$ with $n_i$ dividing $n_{i+1}$ for $i = 1, \ldots, k-1$: then, a product $G = K \times L$ of two non-trivial Abelian groups $K, L$ has $K \times \{e\}$ and $\{e\} \times L$ as normal subgroups, which are different from $\{e\}$ or $G$, so that it is not simple.

Actually, the structure theorem of finite Abelian groups is a particular case of the structure theorem of finitely generated Abelian groups, which are of the form $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \times \mathbb{Z}^r$ for an integer $r \geq 0$.

**Definition 15.10**: In a group $G$, the *commutator* of $g$ and $h$ is $[g, h] = g\,h\,g^{-1}h^{-1} = g\,(g^{-1})^h = h^g h^{-1}$. The subgroup generated by the set of commutators of $G$ is denoted $[G, G]$. The *derived subgroups* of $G$ are $G^{(0)} = [G, G]$, and then $G^{(n+1)} = [G^{(n)}, G^{(n)}]$ for $n \geq 0$.

**Lemma 15.11**: One has $[g, h] = e$ if and only if $g$ and $h$ commute. For every $g, h, a \in G$, one has $[g, h]^a = [g^a, h^a]$.
*Proof*: $[g, h] = e$ means $g\,h\,g^{-1}h^{-1} = e$, so that $g\,h\,g^{-1} = h$ and $g\,h = h\,g$. Actually, $x \mapsto x^a = a\,x\,a^{-1}$ is an automorphism of $G$, and for any homomorphism $\psi$ from $G$ into $G$ (endomorphism), one has $\psi([g, h]) = [\psi(g), \psi(h)]$: indeed, $\psi(x\,y) = \psi(x)\,\psi(y)$ for all $x, y \in G$, and $\psi(x^{-1}) = \big(\psi(x)\big)^{-1}$ for all $x \in G$, so that $\psi(g\,h\,g^{-1}h^{-1}) = \psi(g)\,\psi(h)\,\psi(g^{-1})\,\psi(h^{-1}) = \psi(g)\,\psi(h)\,\big(\psi(g)\big)^{-1}\big(\psi(h)\big)^{-1} = [\psi(g), \psi(h)]$.

**Lemma 15.12**: If $N \triangleleft G$, then $[g\,N, h\,N] = [g, h]\,N$, and $G/N$ is Abelian if and only if $N$ contains all commutators, i.e. $[G, G] \leq N$.
*Proof*: Because $N$ is a normal subgroup, $n_1 g = g\,n_2$ so that one can move an element of $N$ to the right almost as if it was in the center of $G$, but in doing so the element of $N$ changes name: $(g\,n_1)\,(h\,n_2)\,(g\,n_3)^{-1}(h\,n_4)^{-1} = g\,n_1 h\,n_2 n_3^{-1} g^{-1} n_4^{-1} h^{-1} = g\,h\,(n_5 n_2 n_3^{-1}) g^{-1} n_4^{-1} h^{-1} = g\,h\,g^{-1}(n_6 n_4^{-1}) h^{-1} = g\,h\,g^{-1}h^{-1} n_7 \in [g, h]\,N$; then, $n_7$ can be any element in $N$, by taking $n_1 = n_2 = n_3 = e$ and defining $n_4$ by $h\,n_4 = n_7^{-1} h$.

$G/N$ is Abelian if and only if $[g\,N, h\,N] = e\,N = N$ for all $g, h \in G$, i.e. if and only $[g, h]\,N = N$ for all $g, h \in G$, or $[g, h] \in N$ for all $g, h \in G$.

**Lemma 15.13**: $[G, G]\,char\,G$, so that $G^{(n)}\,char\,G^{(m)}$ if $0 \leq m \leq n$, hence $G^{(n)}\,char\,G$, which implies $G^{(n)} \triangleleft G$.
*Proof*: An element $a \in [G, G]$ has the form $a = [g_1, h_1]^{n_1} \cdots [g_k, h_k]^{n_k}$ for some $g_1, \ldots, g_k, h_1, \ldots, h_k \in G$, $n_1, \ldots, n_k \in \mathbb{Z}$, and $k \geq 1$, and for $\psi \in Aut(G)$ one has $\psi(a) = [\psi(g_1), \psi(h_1)]^{n_1} \cdots [\psi(g_k), \psi(h_k)]^{n_k} \in [G, G]$, so that $\psi([G, G]) \subset [G, G]$ for all $\psi \in Aut(G)$, hence $\psi([G, G]) = [G, G]$ for all $\psi \in Aut(G)$.

**Remark 15.14**: If $G$ is a non-Abelian simple group, then $[G, G] = G$, since $[G, G]$ is a normal subgroup of $G$, so that it must be either $\{e\}$ or $G$, but $[G, G] = \{e\}$ means that $G$ is Abelian.

Since $A_5$ is non-Abelian and simple, one has $[A_5, A_5] = A_5$, and then $[A_5, A_5] \subset [S_5, S_5] \subset A_5$ since $A_5 \triangleleft S_5$ with $S_5/A_5$ Abelian (isomorphic to $\mathbb{Z}_2$), so that $[S_5, S_5] = A_5$.

One has $\{e\} \triangleleft N \triangleleft A_4 \triangleleft S_4$, with $N = \{e, (1\,2)\,(3\,4), (1\,3)\,2 3\,4), (1\,4)\,(2\,3)\}$, and $N$ is Abelian ($\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$) so that $[N, N] = \{e\}$; $A_4/N$ is Abelian, isomorphic to $\mathbb{Z}_3$, so that $[A_4, A_4] \leq N$, and $S_4/A_4$ is Abelian, isomorphic to $\mathbb{Z}_2$, so that $[S_4, S_4] \leq A_4$, and let us show that $[A_4, A_4] = N$ and $[S_4, S_4] = A_4$. One has $[A_4, A_4] \neq \{e\}$ since $A_4$ is not Abelian, but because it is a characteristic subgroup of $A_4$ it cannot contain one element of order 2 without containing the two others since the three elements of order 2 are conjugate, hence $[A_4, A_4] = N$. One has $N = [A_4, A_4] \leq [S_4, S_4] \leq A_4$, and by Lagrange's theorem a subgroup $H$ satisfying $N < H \leq A_4$ must coincide with $A_4$, so one must only show that $N \neq [S_4, S_4]$: indeed, $N = [S_4, S_4]$ would imply that $S_4/N$ is Abelian, while it is isomorphic to $S_3$, because it cannot be isomorphic to $\mathbb{Z}_6$, since there would exist $a \in S_4$ with $a, \ldots, a^6$ belonging to six different $N$-cosets, contradicting the fact that in $S_4$ the order of an element is 1, 2, 3, or 4.

**Remark 15.15**: A group $G$ is called *solvable* if there exists a *subnormal series* $G_0 = \{e\} \triangleleft G_1 \triangleleft \cdots \triangleleft G_k = G$ with $G_i/G_{i-1}$ Abelian for $i = 1, \ldots, k$, and it can be shown that $G$ is solvable if and only a derived subgroup $G^{(n)}$ is $\{e\}$ (so that $S_4$ is solvable but not $S_5$), and then $G^{(n)} \triangleleft \cdots \triangleleft G^{(0)} = [G, G] \triangleleft G$ provides a *normal series*, i.e. one which besides $G_{i-1} \triangleleft G_i$ and $G_i/G_{i-1}$ Abelian for $i = 1, \ldots, k$, also satisfies $G_{i-1} \triangleleft G$ for $i = 2, \ldots, k-1$.