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

16- Wednesday October 5, 2011.

Remark 16.1: The reason for the definition of solvability of a group comes from Galois theory, and is related to the question of which polynomial equations can be solved by radicals. RUFFINI had found a way to prove that there exist polynomials of degree 5 with integer coefficients whose roots cannot be expressed by radicals, but his "proof" contained a gap, which ABEL filled. GALOIS went further and explained how (in principle) one can discover if a given polynomial $P \in \mathbb{Z}[x]$ (i.e. with integer coefficients) and of any degree ≥ 5 has its roots expressed by radicals or not: there is a natural field extension K of $\mathbb{Q}$ to consider, the smallest field ($\subset \mathbb{C}$) containing $\mathbb{Q}$ and the roots of P (called a *splitting field extension* of P over $\mathbb{Q}$), and one then considers the group G of automorphisms of K fixing $\mathbb{Q}$ (the *Galois group* $Aut_{\mathbb{Q}}(K)$), and there is a correspondence between the subgroups of G and the intermediate fields between $\mathbb{Q}$ and K; then, the fact that one can go from $\mathbb{Q}$ to K by successively adding m-th roots taken in the successive extensions expresses exactly the property that G is solvable.

For a polynomial $P \in \mathbb{Z}[x]$ of degree 5 which has three real roots and two (conjugate) non-real roots, one then shows that the Galois group is isomorphic to S_5, which is not solvable, hence has its roots which cannot be expressed by radicals.

Remark 16.2: For proving the characterization mentioned before (that a group G is solvable if and only if a derived group $G^{(n)}$ must be $\{e\}$) there are a few natural observations: one starts from a subnormal series $(G_i, i = 0, \ldots, k)$ which witnesses that G is solvable, and one proves that if $H \leq G$ the sequence $(H_i = G_i \cap H, i = 0, \ldots, k)$ is a subnormal series in H, which then witnesses that H is solvable; if N is a normal subgroup of G (with π the projection of G onto G/N), one proves that the sequence $(G_i^* = \pi\, G_i \simeq G_i N/N, i = 0, \ldots, k)$ is a subnormal series in G/N, which then witnesses that G/N is solvable. Then, if G is a group which contains a normal subgroup N which is solvable (witnessed by a subnormal series $(N_i, i = 0, \ldots, k)$) with G/N solvable (witnessed by a subnormal series $(Q_j, j = 0, \ldots, \ell)$), one proves that G is solvable by considering $M_j = \pi^{-1} Q_j$ (with π the projection of G onto G/N) and noticing that $M_j \triangleleft M_{j+1}$ and that M_{j+1}/M_j is isomorphic to Q_{j+1}/Q_j, and then $N_0 \leq \ldots \leq N_k = N = M_0 \leq M_1 \leq \ldots \leq M_\ell = G$ witnesses that G is solvable.

Remark 16.3: The Brauer–Fowler theorem,[1,2] proved in 1955, states that if a group G has even order > 2 then it has a proper subgroup H with $|H| > |G|^{1/3}$: BRAUER and FOWLER showed that if G has exactly m elements of order 2, and $n = \frac{|G|}{m}$, then G contains a proper subgroup H whose index (> 1) is either 2 or $< \frac{n\,(n+2)}{2}$, so that if v is the maximal order of a proper subgroup, then either $v = \frac{|G|}{2}$ or $2|G| < v^2(v+1)$. They also showed that G contains a proper (but possibly trivial) normal subgroup N with G/N isomorphic to a subgroup of S_u with either $u = 2$ or $u < \frac{n\,(n+2)}{2}$, so that either $[G\!:\!N] = 2$ or $[G\!:\!N] < \big(\frac{n\,(n+2)}{2}\big)!$; they deduced that if moreover G is simple, then $|G| < \big(\frac{n\,(n+1)}{2}\big)!$.

BRAUER and FOWLER also observed that there exist only a finite number of simple groups in which the centralizer $C_G(a)$ of an element a of order 2 (called an *involution*) is isomorphic to a given group, and this suggested that finite simple groups could be classified by studying the centralizers of their involutions, a program that was later realized in the classification of finite simple groups. Since their result only apply to groups of even order, they mentioned a conjecture that all groups of odd order are solvable.

Remark 16.4: It was BURNSIDE who had conjectured in 1911 that every non-Abelian finite simple group has even order,[3] and one of his best known contributions to group theory is his $p^a q^b$ theorem, that every

[1] Richard Dagobert BRAUER, German-born mathematician, 1901–1977. He worked in Toronto (Ontario), at University of Michigan, Ann Arbor, MI, and at Harvard University, Cambridge, MA. The Brauer–Fowler theorem is partly named after him.

[2] Kenneth Arthur FOWLER, American mathematician. He worked at San José State University, San José, CA. The Brauer–Fowler theorem is partly named after him.

[3] William BURNSIDE, English mathematician, 1852–1927. He worked at the Royal Naval College in Greenwich, England.

finite group whose order is divisible by fewer than three distinct primes is solvable.

A *CA group* is a group such that the centralizer of every non-trivial element is Abelian, and in 1957, SUZUKI showed that all CA groups of odd order are solvable,[4] and he later classified all the simple CA groups, and more generally all simple groups such that the centralizer of any involution has a normal 2-Sylow subgroup.[5]

A *CN group* is a group such that the centralizer of every non-trivial element is *nilpotent*, and in 1960 FEIT,[6] HALL,[7] and THOMPSON showed that every CN group of odd order is solvable.[8] Their proof, similar to SUZUKI's proof, was about 17 pages long, which at the time was thought to be very long for a proof in group theory.

In 1963, FEIT and THOMPSON proved what can be thought of as the next step in this process, the Feit–Thompson theorem: they showed that there is no (non-cyclic) simple group of odd order such that every proper subgroup is solvable, and this proves that every finite group of odd order is solvable, as a minimal counter-example must be a simple group such that every proper subgroup is solvable. Although the proof follows the same general outline as the CA theorem and the CN theorem, the details are much more complicated, and the article is 255 pages long!

Remark 16.5: A group G is called *nilpotent* if there exists a finite normal series (so that $G_i \lhd G$, implying $G_i \lhd G_{i+1}$) such that $G_{i+1}/G_i \leq Z(G/G_i)$ for $i = 0, \ldots, k-1$, and since the center of a group is Abelian, G_{i+1}/G_i is then Abelian, so that every nilpotent group is solvable.

Since an element a in a ring R is called *nilpotent* if $a^n = 0$ for some $n \geq 1$, one may wonder if using the same term is consistent: for $g \in G$, one has a mapping ad_g from G into G defined by $ad_g(x) = [g, x]$, and the definition implies that, for every $g \in G$, ad_g maps G_{i+1} into G_i for $i = 0, \ldots, k-1$,[9] so that $ad_{g_k} \circ \cdots \circ ad_{g_1}$ maps G onto $\{e\}$ for all $g_1, \ldots, g_k \in G$; however, there is no obvious ring structure in this context.

For a group G, the *ascending central series* is defined by $Z_0(G) = \{e\}$, $Z_{n+1}(G)/Z_n(G) = Z\big(G/Z_n(G)\big)$, and it satisfies $[G, Z_{n+1}(G)] \leq Z_n(G)$ for all $n \geq 0$, and the *descending central series* is defined by $L_1(G) = G$, $L_{n+1}(G) = [G, L_n(G)]$, and it satisfies $L_n(G)\, char\, G$ for all $n \geq 1$, so that $L_n(G) \lhd G$ for all $n \geq 1$, and $L_n/L_{n+1} \leq Z(G/L_{n+1})$. One then shows that a group G is nilpotent if and only if its ascending central series reaches G, or if and only if its descending central series reaches $\{e\}$.

Remark 16.6: If p is prime, any finite p-group G is nilpotent. If G is a nilpotent group, then $H < G$ implies $H < N_G(H)$. If G is a finite nilpotent group, and a prime p divides $|G|$, then it has a unique Sylow-p subgroup (which is then a normal subgroup of G). If G is a finite nilpotent group, then it is isomorphic to

[4] Michio SUZUKI, Japanese-born mathematician, 1926–1998. He worked at University of Illinois at Urbana-Champaign, IL.

[5] He also found in 1960 an overlooked family of simple groups of Lie type in the process, that are now called *Suzuki groups*, an infinite family of the only non-Abelian simple groups whose order is not divisible by 3: the smallest, of order 29,120, was the first simple group of order less than 1 million to be discovered since Dickson's list of 1900.

[6] Walter FEIT, Austrian-born mathematician, 1930–2004. He worked at Cornell University, Itaca, NY, and at Yale University, New Haven, CT. The Feit–Thompson theorem is partly named after him.

[7] Marshall HALL, American mathematician, 1910–1990. He worked OSU (Ohio State University) Columbus, OH, at Caltech (California Institute of Technology) Pasadena, CA, and at Emory University, Oxford, GA.

[8] John Griggs THOMPSON, American-born mathematician, born in 1932. He received the Fields Medal in 1970. He received the Wolf Prize in 1992, for his profound contributions to all aspects of finite group theory and connections with other branches of mathematics, jointly with Lennart CARLESON. He worked at the University of Chicago, Chicago, IL, University of Cambridge, Cambridge, England, holding the Rouse Ball professorship, and at University of Florida, Gainesville, FL. He received the Abel Prize in 2008 jointly with Jacques TITS, for their profound achievements in algebra and in particular for shaping modern group theory. The Feit–Thompson theorem is partly named after him.

[9] Because $G_{i+1}/G_i \leq Z(G/G_i)$ for $i = 0, \ldots, k-1$ is equivalent to $[G_{i+1}, G] \leq G_i$ for $i = 0, \ldots, k-1$, and of course if $H, K \leq G$ one writes $[H, K]$ for the subgroup generated by all the commutators $[h, k]$ with $h \in H, k \in K$. An important observation is that if $H \leq G$, $K \lhd G$ (which implies $H\,K = K\,H \leq G$), and if one has $[G, H] \leq K$, then $H\,K/K \leq Z(G/K)$.

the product of its Sylow subgroups. A direct product of a finite number of nilpotent groups is nilpotent. If G is a finite group, then G is nilpotent if and only if it is isomorphic to a product of finite p groups.

Remark 16.7: D_n is solvable for all $n \geq 3$, but it is nilpotent if only if n is a power of 2: one has $a^\alpha b = b\, a^{-\alpha}$ for all $\alpha \in \mathbb{Z}$, and one deduces that $[a^\alpha, a^\beta b] = a^{2\alpha}$ and $[a^\alpha b, a^\beta b] = a^{2\alpha - 2\beta}$ for all $\alpha, \beta \in \mathbb{Z}$. This shows that $L_1(D_n) = [D_n, D_n] = \{a^{2\gamma} \mid \gamma \in \mathbb{Z}\}$, which is Abelian, so that D_n is solvable. By induction $L_j(D_n) = \{a^{2^j \gamma} \mid \gamma \in \mathbb{Z}\}$ for $j \geq 1$, so that D_n is nilpotent if and only if n is a power of 2.

One can construct an infinite p-group G_1 which is nilpotent, and an infinite p-group G_2 which is not nilpotent.

Additional footnotes: BALL R.,[10] BONAPARTE,[11] Lennart CARLESON,[12] DICKSON,[13] EMORY,[14] FOURIER,[15] Misha GROMOV,[16] Jacques TITS.[17]

[10] Walter William Rouse BALL, English mathematician, 1850–1925. He worked in Cambridge, England. The Rouse Ball professorship at Cambridge, England, is named after him.

[11] Napoléon BONAPARTE (Napoleone BUONAPARTE), French general, 1769–1821. He became Premier Consul after his coup d'état in 1799, was elected Consul à vie in 1802, and he proclaimed himself emperor in 1804, under the name Napoléon I (1804–1814, and 100 days in 1815).

[12] Lennart Axel Edvard CARLESON, Swedish mathematician, born in 1928. He received the Wolf Prize in 1992, for his fundamental contributions to Fourier analysis, complex analysis, quasi-conformal mappings and dynamical systems, jointly with John G. THOMPSON, for his profound contributions to all aspects of finite group theory and connections with other branches of mathematics. He received the Abel Prize in 2006 for his profound and seminal contributions to harmonic analysis and the theory of smooth dynamical systems. He worked at Uppsala, Sweden, at UCLA (University of California at Los Angeles), Los Angeles, CA, and at the Royal Institute of Technology, Stockholm, Sweden.

[13] Leonard Eugene DICKSON, American mathematician, 1874–1954. He worked at the University of Chicago, Chicago, IL.

[14] John EMORY, American clergyman, 1789–1835. He was elected bishop of the Methodist Episcopal Church in 1832. Emory University, Oxford, GA, is named after him.

[15] Jean-Baptiste Joseph FOURIER, French mathematician, 1768–1830. He worked in Auxerre, in Paris, France, accompanied BONAPARTE in Egypt, was prefect in Grenoble, France, until the fall of Napoléon I, and worked in Paris again. The first of three universities in Grenoble, France, Université de Grenoble I, is named after him, and the Institut Fourier is its department of mathematics. Fourier series and Fourier integrals are named after him.

[16] Mikhail Leonidovich GROMOV, Russian-born mathematician, born in 1943. He received the Wolf Prize in 1993, for his revolutionary contributions to global Riemannian and symplectic geometry, algebraic topology, geometric group theory and the theory of partial differential equations, jointly with Jacques TITS, for his pioneering and fundamental contributions to the theory of the structure of algebraic and other classes of groups and in particular for the theory of buildings. He works at IHES (Institut des Hautes Études Scientifiques) at Bures sur Yvette, France, and at NYU (New York University), New York, NY.

[17] Jacques TITS, Belgian-born mathematicia, born in 1930. He received the Wolf Prize in 1993, for his pioneering and fundamental contributions to the theory of the structure of algebraic and other classes of groups and in particular for the theory of buildings, jointly with Mikhael GROMOV. He received the Abel Prize in 2008 jointly with John G. THOMPSON, for their profound achievements in algebra and in particular for shaping modern group theory. He worked at the Free University of Brussels, Bruxelles (Brussels), Belgium, in Bonn, Germany, and at Collège de France, Paris, France.