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

12- Monday September 26, 2011.

Lemma 12.1: If P is a Sylow-p subgroup of G, it is the unique Sylow-p subgroup of $Q = N_G(P)$, and $N_G(Q) = Q$.
Proof: P is a normal subgroup $N_G(P)$, which has size $p^n b$ for a divisor b of a, so that P is a Sylow-p subgroup of $N_G(P)$, hence it is its only Sylow-p subgroup.

For $r \in N_G(Q)$, the conjugate P^r is a Sylow-p subgroup of Q^r, but $Q^r = Q$ by definition of $N_G(Q)$, so that P^r is a Sylow-p subgroup of Q, and it must then be P, but $P^r = P$ means $r \in N_G(P)$ by definition, so that $r \in Q$.

Lemma 12.2: If $|G| = 2p$ for a group G, with p an *odd prime*, then G is either isomorphic to $\mathbb{Z}_{2p}$ or to D_p.
Proof: The number n_2 of Sylow-2 subgroups is either 1 or p, and the number n_p of Sylow-p subgroups is 1. If $n_2 = 1$, one concludes as seen before that $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_p$, which is $\simeq \mathbb{Z}_{2p}$ by the Chinese remainder theorem.

If $n_2 = p$, one wants to show that $G \simeq D_p$. Let $N = \{e, \alpha, \alpha^2, \ldots, \alpha^{p-1}\} \triangleleft G$ be the Sylow-p subgroup, and let $H_j = \{e, b_j\}$, $j = 1, \ldots, p$ be the Sylow-2-subgroups, which are all conjugate, so that for each j there is k such that $\alpha\, H_j \alpha^{-1} = H_k$, i.e. $\alpha\, b_j \alpha^{-1} = b_k$. One cannot have $k = j$, since it would imply that b_j commutes with α hence with all elements of N, and then G would coincide with the product $H_j \times N$ generated by N and b_j, so that G would be Abelian (which only occurs if $n_2 = 1$); the same argument shows that $\alpha^\ell b_j \alpha^{-\ell} \neq b_j$ when ℓ is not a multiple of p, so that starting from b_1 and conjugating with α generates all the b_j, and one can then change the indexing so that $\alpha^\ell b_1 \alpha^{-\ell} = b_{1+\ell}$ for all ℓ. Since $N \triangleleft G$, one has $b_1 \alpha\, b_1^{-1} = \alpha^m$ for some $m \in \{2, \ldots, p-1\}$, since $m = 0$ would imply $\alpha = e$ and $m = 1$ would imply that b_1 and α commute; from $b_1 \alpha = \alpha^m b_1$, one deduces by induction that $b_1 \alpha^j = \alpha^{j\,m} b_1$ for all j, and then $b_{1+\ell} = \alpha^\ell b_1 \alpha^{-\ell} = \alpha^{\ell - \ell\, m} b_1$, which is $a^\ell b_1$ if one takes $a = \alpha^{1-m}$, which is a generator of N, and this gives the structure of D_p.

Lemma 12.3: If a group G has a normal subgroup N and a subgroup H such that $N \cap H = \{e\}$ and $N\,H = G$ (hence $H\,N = N\,H$),[1] then G is isomorphic to a semi-direct product $N \times_\psi H$ for the automorphism ψ from H into $Aut(N)$ given by $\psi_h(n) = h\,n\,h^{-1}$ for $n \in N, h \in H$.
Proof: Every $g \in G$ can be written in a unique way as $g = n\,h$ for some $n \in N, h \in H$, and the mapping $g \mapsto (n, h)$ is a bijection (but not an homomorphism in general). The definition of ψ by $\psi_h(n) = h\,n\,h^{-1}$ shows that $\psi \in Aut(N)$ because N is a normal subgroup. The product of $g_1 = n_1 h_1$ by $g_2 = n_2 h_2$ in G consists in writing $n_1 h_1 n_2 h_2$ and then wondering for which $n \in N, h \in H$ this product is $n\,h$, and since $n_1 h_1 n_2 h_2 = n_1 (h_1 n_2 h_1^{-1})\, h_1 h_2$, one has $n = n_1 (h_1 n_2 h_1^{-1}) \in N$ (because $h_1 n_2 h_1^{-1} \in N$ since N is normal) and $h = h_1 h_2 \in H$, and it is exactly what $(n_1, h_1) \star_\psi (n_2, h_2)$ gives.

Lemma 12.4: Let G be a finite *simple* group acting on a set X, then any orbit *not reduced to a point* has a size s such that $s! \geq |G|$.

If H is a *proper* subgroup of G (i.e. $H \neq G$), then the index i of H satisfies $i! \geq |G|$.
Proof: Let Y be an orbit not reduced to a point and having size $s > 1$, then the action restricted to Y is an homomorphism of G into S_Y (the group of bijection of Y onto itself), and its kernel is then a normal subgroup of G, which is then either $\{e\}$ or G, since G is simple. The kernel is not G, since it would imply $|Y| = 1$, so that it is $\{e\}$ and the mapping from G into S_Y is injective, so that S_Y contains an isomorphic copy of G, and this implies $|G| \leq |S_Y| = s!$.

One considers the action of G on the set X of left cosets of H by multiplication from the left. This action is an injective mapping from G into S_X, and the size of the orbit is the index i of H in G, and $|H| < |G|$ implies $i > 1$, so that by the first part one must have $i! \geq |G|$.

Remark 12.5: For a finite simple group, one has $n_p > 1$ for each prime p dividing $|G|$ since no Sylow p-subgroup can be a normal subgroup, but Lemma 12.4 gives a much stronger property, than $n_p! \geq |G|$ for each prime p dividing $|G|$.

[1] If G is finite, it is equivalent to $|N|\,|H| = |G|$.

Since the index of a subgroup cannot be too small, a finite simple group lacks large proper subgroups, and it is useful to observe that Lagrange's theorem says that if $|G| = n$, and $H \leq G$ with $|H| = d$, then d is a divisor of n, but that it is not true that for every divisor d of n there exists a subgroup of G of size d: the smallest value of n for which one has a counter-example is $n = 12$, since A_4 has order 12, but has no subgroup of order 6.

Indeed, A_4 has eight elements of order 3 which are the cyclic permutations of three elements in $\{1, 2, 3, 4\}$ (for example, the two ones fixing 1 are $(2\,3\,4)$ and its square $(2\,4\,3)$), and three elements of order 2, which are $(1\,2)\,(3\,4)$, $(1\,3)\,(2\,4)$, and $(1\,4)\,(2\,3)$, which with e form the normal subgroup N (isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$) mentioned before; if A_4 had a subgroup H of order 6, H could not be isomorphic to $\mathbb{Z}_6$, since no element of A_4 (or even of S_4) has order 6, so that H would be isomorphic to S_3, but S_3 has three elements of order 2 (the transpositions), hence H would contain the three elements of order 2 in A_4, and this would contradict Lagrange's theorem, since H would contain N which has order 4.

Remark 12.6: It will be shown in another lecture that A_n is simple for $n \geq 5$, so that since it has order $\frac{n!}{2}$, the smallest value of s for which $s! \geq |A_n|$ is n, hence for $n \geq 5$ the proper subgroups of A_n have index $\geq n$. For A_5, which has order 60, it implies that there is no subgroup of A_5 of order 15, 20, or 30 (the divisors d of 60 such that $d < 60$ and $\frac{60}{d} < 5$).

Remark 12.7: If p is prime, any group of order p is isomorphic to $\mathbb{Z}_p$, which is simple, so that one may wonder if 60 is the smallest composite integer n for which there exists a simple group of order n.

The structure theorem of finite Abelian groups will be shown in another lecture, and it says that a non-trivial finite Abelian group G is isomorphic to $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k}$ with $k \geq 1$ and d_i divides d_{i+1} for $i = 1, \ldots, k-1$, hence an Abelian group G is simple if and only if $G \simeq \mathbb{Z}_p$ for a prime p.

It will be shown in another lecture that if $n = p^k$ for a prime p and $k \geq 2$, and G has order n, its center $Z(G)$ is non-trivial (i.e. $\neq \{e\}$), and since $Z(G)$ is a characteristic subgroup of G, hence a normal subgroup of G, G is not simple.[2]

For $6 < n \leq 24$ and n composite having at least two prime divisors (since one is not interested in powers of primes), there is no group of order n which is simple: there cannot be more than two prime divisors since $2 \cdot 3 \cdot 5 = 30 > 24$, and if $n = p^\alpha q^\beta$ with primes $p < q$, one needs to have $n_p, n_q \geq 4$, so that because n_p divides q^β and n_q divides p^α, 2 and 3 must only appear with an exponent ≥ 2, and this constraint is sufficient for eliminating all these values of n.

For $24 < n \leq 120$ and n composite having at least two prime divisors, one must have $n_p \geq 5$ for each prime divisor p, so that for the integers of the form $p^\alpha q^\beta$ with primes $p < q$, 2 must only appear with an exponent ≥ 3, and 3 must only appear with an exponent ≥ 2: if I have made no errors, only 19 such integers (with exactly two distinct prime divisors) pass this first test,[3] and there are also 13 integers with three distinct prime divisors.[4] One then uses the more precise constraint of imposing on n_p the two congruences of the Sylow's theorem, for each prime divisor of n, and I find that the integers remaining after this test are 30 ($n_2 \in \{5, 15\}$, $n_3 = 10$, $n_5 = 6$), 56 ($n_2 = 7$, $n_7 = 8$), 60 ($n_2 \in \{5, 15\}$, $n_3 = 10$, $n_5 = 6$), 80 ($n_2 = 5$, $n_5 = 16$), 90 ($n_2 \in \{5, 9, 15, 45\}$, $n_3 = 10$, $n_5 = 6$), 105 ($n_3 \in \{5, 7, 35\}$, $n_5 = 21$, $n_7 = 15$), 112 ($n_2 = 7$, $n_7 = 8$), and 120 ($n_2 \in \{5, 15\}$, $n_3 = 10$, $n_5 = 6$). Then, one checks if the order of elements predicted by these values of n_p are compatible with the size of the group, and no simple group of order 30 exists, since $n_3 = 10$ implies the existence of exactly 20 elements of order 3, and $n_5 = 6$ implies the existence of exactly 24 elements of order 5, already too much for a group of order 30. That no simple group of order 56 exists is similar, since $n_7 = 8$ implies the existence of exactly 48 elements of order 7, so that only 8 elements remain, enough for just one Sylow 2-subgroup (of order 8). The smallest value of n is then 60.[5]

---

[2] To be complete, one should observe that $Z(G) = G$ means that G is Abelian.

[3] I find 35, 40, 45, 55, 56, 63, 65, 72, 77, 80, 85, 88, 95, 99, 104, 112, 115, 117, and 119.

[4] I find 30, 42, 60, 66, 70, 78, 84, 90, 102, 105, 110, 114, and 120.

[5] There is no simple group of order 80, since $n_5 = 16$ implies the existence of exactly 64 elements of order 5, so that only 16 elements remain, enough for just one Sylow 2-subgroup (of order 16). There is no simple group of order 105, since $n_5 = 21$ implies the existence of exactly 84 elements of order 5, $n_7 = 15$ implies the existence of exactly 90 elements of order 7, already too much for a group of order 105. That there are no simple groups of order 90, 112, or 120 is more technical to prove.

Remark 12.8: In order to understand which are the groups of order 12 (up to isomorphism), one starts with what Sylow's theorem implies. One has $n_2 = 1 \pmod 2$ and n_2 divides 3, so that $n_2 \in \{1, 3\}$, and one has $n_3 = 1 \pmod 3$ and n_3 divides 4, so that $n_3 \in \{1, 4\}$.

The case $n_2 = n_3 = 1$ implies the existence of a unique normal Sylow 2-subgroup H_2 (of order 4, hence isomorphic to either $\mathbb{Z}_4$ or to $\mathbb{Z}_2 \times \mathbb{Z}_2$), and of a unique normal Sylow 3-subgroup H_3 (of order 3, hence isomorphic to $\mathbb{Z}_3$), and since $H_2 \cap H_3 = \{e\}$ and $|G| = |H_2|\,|H_3|$, one deduces that G is isomorphic to $H_2 \times H_3$; this means that G is Abelian, and either isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_3$, which is isomorphic to $\mathbb{Z}_{12}$ by the Chinese remainder theorem, or isomorphic to $(\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_3$, which is isomorphic to $\mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_3)$, itself isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_6$ by the Chinese remainder theorem.

The case $n_2 = 3$ and $n_3 = 4$ cannot happen, because $n_3 = 4$ implies the existence of exactly 8 elements of order 3, so that only 4 elements remain, enough for just one Sylow 2-subgroup (of order 4).

Remark 12.9: A (non-Abelian) group G of order 12 with $n_2 = 1, n_3 = 4$ has a unique Sylow 2-subgroup H_2 (of order 4) which is a normal subgroup of G, and four Sylow 3-subgroups K_1, K_2, K_3, K_4 (of order 3). Since $H_2 \cap K_j = \{e\}$ by Lagrange's theorem, and $|G| = |H_2|\,|K_j|$, G is isomorphic to a (non-trivial) semi-direct product $H_2 \times_\psi \mathbb{Z}_3$ (since $K_j \simeq \mathbb{Z}_3$) for a (non-trivial) homomorphism ψ from $\mathbb{Z}_3$ into $Aut(H_2)$. In the case of A_4, the Sylow 2-subgroup is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, and since H_2 is either isomorphic to $\mathbb{Z}_4$ or to $\mathbb{Z}_2 \times \mathbb{Z}_2$, it is useful to observe that only the trivial homomorphism exists from $\mathbb{Z}_3$ into $Aut(\mathbb{Z}_4)$: indeed, $Aut(\mathbb{Z}_4)$ is isomorphic to the multiplicative group $\mathbb{Z}_4^*$ of units of the ring $\mathbb{Z}_4$ (the multiplicative group $\{1, 3\}$ modulo 4), i.e. isomorphic to the additive group $\mathbb{Z}_2$, and only the trivial homomorphism exists from $\mathbb{Z}_3$ into $\mathbb{Z}_2$; this shows that H_2 must be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Since $\mathbb{Z}_2 \times \mathbb{Z}_2$ has three elements (a, b, and c) of order 2 (which satisfy $a\,b = b\,a = c$, $b\,c = c\,b = a$ and $c\,a = a\,c = b$), one has an automorphism of $\mathbb{Z}_2 \times \mathbb{Z}_2$ for each permutation of a, b, and c, so that $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq S_3$; S_3 has a unique subgroup of order 3, which corresponds to the cyclic permutations, so that one non-trivial homomorphism ψ sends $1 \in \mathbb{Z}_3$ to the automorphism induced by the cyclic permutation $(a\,b\,c)$, and $2 \in \mathbb{Z}_3$ to the automorphism induced by the cyclic permutation $(a\,b\,c)^2 = (a\,c\,b)$. The other non-trivial homomorphism is ψ^2 (which is ψ^{-1} since ψ has order 3), i.e. sends $1 \in \mathbb{Z}_3$ to the automorphism induced by the cyclic permutation $(a\,c\,b)$, and $2 \in \mathbb{Z}_3$ to the automorphism induced by the cyclic permutation $(a\,b\,c)$.

Remark 12.10: A (non-Abelian) group G of order 12 with $n_2 = 3, n_3 = 1$ has three Sylow 2-subgroups L_1, L_2, L_3 (of order 4), and a unique Sylow 3-subgroup H_3 (of order 3) which is a normal subgroup of G. Since $H_3 \cap L_j = \{e\}$ by Lagrange's theorem, and $|G| = |H_3|\,|L_j|$, G is isomorphic to a (non-trivial) semi-direct product $\mathbb{Z}_3 \times_\psi L_j$ (since H_3 is isomorphic to $\mathbb{Z}_3$) for a (non-trivial) homomorphism ψ from L_j into $Aut(\mathbb{Z}_3)$, and L_j is either homomorphic to $\mathbb{Z}_4$ of to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Since $Aut(\mathbb{Z}_3)$ is isomorphic to the multiplicative group $\mathbb{Z}_3^*$ of non-zero elements of the field $\mathbb{Z}_3$ (the multiplicative group $\{1, 2\}$ modulo 3), i.e. isomorphic to the additive group $\mathbb{Z}_2$, a non-trivial homomorphism of a group Γ into $Aut(\mathbb{Z}_3)$ exists if and only if Γ has a subgroup N of index 2 (which is automatically a normal subgroup of Γ), so that N is sent to the identity of $Aut(\mathbb{Z}_3)$ and the other coset $a\,N$ (for $a \notin N$) is then to the other element of $Aut(\mathbb{Z}_3)$.