Combinatorics of Simple Groups

James B. Wilson

July 18, 2003

1 Combinatorial Rules for Simplicity

Theorem 1.1 *If $|G| = p^i m$ with $(p, m) = 1$, then G is simple only if*

$$p^i \mid (m-1)!.$$

Proof: Suppose P is a Sylow-p-subgroup of G. Then G acts on $[G : P] = m$ cosets. Hence as G is simple, G is embedded in S_m. So $p^i m$ divides the order $m!$ which implies $p^i|(m-1)!$. □

Definition 1.2 *Let p be a prime dividing the order of $|G|$. Then define $r_p(G)$ to be the number of Sylow-p-subgroups of G.*

Theorem 1.3 *Let G be non-abelian and p a divisor of $|G|$. If G is simple then the following must all be true:*

(i) $r_p \equiv 1 \pmod p$

(ii) $r_p \neq 1$

(iii) $2|G| \leq (r_p - 1)!$ *or* $G \cong A_{r_p}$.

(iv) $2k|(r_p - 1)!$ *where* $|G| = r_p \cdot k$, *or* $G \cong A_{r_p}$.

Proof: The first two are a result of the Thrid and Second Sylow theorem.

For (iii) consider group actions. By the second Sylow theorem we know all Sylow-p-subgroups are conjugate. Moreover, G must therefore act transitively on the Sylow-p-subgroups by conjugation. This gives a homomorphism $f : G \to S_{r_p}$. However if G is to be simple then it is clear that f has a trivial kernel so that G is embedded in S_{r_p}.

Since $A_{r_p} \trianglelefteq S_{r_p}$ so that indeed $G \cap A_{r_p} \trianglelefteq G$. So either $A_{r_p} \cap G = G$ or $A_{r_p} \cap G = \mathbf{0}$. Suppose the intersection is trivial. Then

$$2 = [S_{r_p} : A_{r_p}] \geq [G \vee A_{r_p} : A_{r_p}] = [G : A_{r_p} \cap G] = |G|.$$

We are not interested in such small groups so we presume that G does not intersect trivially.

Suppose $p \neq 3$ we know $r_p \neq 4$. Hence we have the rule that A_{r_p} is simple so indeed we have that $[A_{r_p} : G] \geq r_p$ or that $G = A_{r_p}$. Thus

$$r_p \leq \frac{r_p!}{2|G|}; \qquad |G| \leq \frac{(r_p - 1)!}{2}.$$

Moreover,

$$|G| \left| \frac{r_p!}{2} \right. \qquad \frac{|G|}{r_p} \left| \frac{(r_p - 1)!}{2} \right. .$$

Finally, suppose $p = 3$ and that $r_3 = 4$. Then G is embedded in A_4 as it is simple. Note 12 divides the order of G by assumption so indeed $G = A_4$ which is not simple. So when $p = 3$ it follows $r_3 \neq 4$. So as the test $|G| \leq \frac{(r_p-1)!}{2}$ rules out this case we may avoid adding it to the list. $\square$

We must ensure we have sufficient elements to equipe a group G with the given arrangement of Sylow-p-subgroups. This falls to the following theorem.

Theorem 1.4 *If $|G| = p_1^{i_1} \cdots p_n^{i_n}$ then the following must be true:*

$$|G| \geq 1 + \sum_{j=1}^{n} r_{p_j} p_j^{i_j - 1}(p_j - 1) - \sum_{j=1}^{n} p_j^{i_j - 1}.$$

Example: A group of order 60 may be simple. First we have $2^2|(15-1)!$ and $3|(20-1)!$ as well as $5|(12-1)!$. Theorem-1.1 is satisfied.

Now we use Theorem-1.3

- By (i) we have $r_2 = 1, 3, 5, 15$. Yet (ii) eliminates 1, while (iii) eliminates 3. If $r_2 = 5$ then it is possible that $G = A_5$ in which case we are done. So suppose instead $r_2 = 15$. We check with (iv) and are satisfied.
- By (i) we have $r_3 = 1, 4, 10$. However (ii) eleminates 1, and (iii) eliminates 4 leaving $r_3 = 10$. (iv) also is satisfied.
- Finally $r_5 = 1, 6$ by (i), but we exclude 1 by (ii). Note that (iii) and (iv) work for $r_5 = 6$.

Using $r_2 = 5$ we are satisified that G is simple. However using $r_2 = 15$ we have a problem in Theorem-1.4

$$2^1(1 + 15(2-1)) + 3^0(1 + 10(3-1)) + 5^0(1 + 6(5-1)) = 78$$

Thus $r_2 = 5$, $r_3 = 10$ and $r_5 = 6$. $\square$

2 Non-Simplicity of $2^i p$ Groups

	3	5	7	11	13
2	$r_3 = 1$	$r_5 = 1$	$r_7 = 1$	$r_{11} = 1$	$r_{13} = 1$
2^2	$2^2 \nmid (3-1)!$	$r_5 = 1$	$r_7 = 1$	$\vdots$	$\vdots$
2^3	$\vdots$	$r_5 = 1$	$1.3.iii, p = 2$		
2^4		$2^4 \nmid (5-1)!$	$1.3.iii, p = 2$		
2^5		$\vdots$	$2^5 \nmid (7-1)!$		
2^6			$\vdots$		
2^7				$\vdots$	
2^8				$r_{11} = 1$	
2^9				$2^9 \nmid (11-1)!$	$\vdots$
2^{10}				$\vdots$	$r_{13} = 1$
2^{11}					$2^{11} \nmid (13-1)!$
$\vdots$					$\vdots$

3 Non-Simplicity of $2^i p^2$ Groups

	3^2	5^5	7^2	11^2	13^2
2	$r_3 = 1$	$r_5 = 1$	$r_7 = 1$	$r_{11} = 1$	$r_{13} = 1$
2^2	$2^2 \nmid (3-1)!$	$r_5 = 1$	$r_7 = 1$	$\vdots$	$\vdots$
2^3	$\vdots$	$r_5 = 1$	$1.3.iii, p = 2$		
2^4		$2^4 \nmid (5-1)!$	$1.3.iii, p = 2$		
2^5		$\vdots$	$2^5 \nmid (7-1)!$		
2^6			$\vdots$		
2^7				$\vdots$	
2^8				$r_{11} = 1$	
2^9				$2^9 \nmid (11-1)!$	$\vdots$
2^{10}				$\vdots$	$r_{13} = 1$
2^{11}					$2^{11} \nmid (13-1)!$
$\vdots$					$\vdots$