Dan Lyness
Calum Shearer
Andrew Doumont

(5.1.9) Let G be a simple group of order m and let p be a prime dividing m. If the class number of G exceeds m/p^2, then the Sylow p-subgroups of G are abelian.

Proof. Let G be a simple group of order m and let p be a prime dividing m. If p^2 does not divide m, then the Sylow p-subgroups of G are of order p and must be abelian as desired. Therefore, we will assume that p^2 divides m. We will also assume that the class number, r, of G exceeds m/p^2.

We can write

$$m = d_1^2 + \cdots + d_r^2$$

where each d_i is the degree of a irreducible character of G. Additionally, we know that $d_1 = 1$. Therefore, we have

$$m = 1 + d_2^2 + \cdots + d_r^2.$$

Since $r > m/p^2$ and m/p^2 is an integer (since p^2 divides m), we must also have that

$$r - 1 \geq m/p^2.$$

Assume, by way of contradiction, that $d_2, \ldots, d_r \geq p$. Then

$$\begin{aligned} m &= 1 + d_2^2 + \cdots + d_r^2 \\ &\geq 1 + (r-1)p^2 \quad (\text{since } d_i \geq p) \\ &\geq 1 + \left(\frac{m}{p^2}\right) p^2 \quad (\text{since } r - 1 \geq m/p^2) \\ &\geq 1 + m. \end{aligned}$$

This is a contradiction, so we must have $d_i < p$ for some $i \neq 1$.

Now, let ρ be the representation associated with the character χ_i and let P be a Sylow p-subgroup. Consider the restriction ρ_P. Notice first that ρ_P must be faithful. In fact, ρ is faithful since it is not the trivial representation, and G is simple which implies the kernel of the representation must be trivial. Additionally ρ_P must have equivalent degree to ρ since by (2) of the "Basic Properties of Characters of Finite Groups" handout, $\chi_i(1)$ is the degree of χ_i, which will be the same for the character of ρ and of ρ_P.

Now, the character χ of ρ_P can be written as the sum of irreducible characters

$$\chi = \psi_1 + \cdots + \psi_t.$$

Since the degree of each ψ_i must divide the order of P, they are each either of degree 1 or degree p. But if any are of degree p then we will arrive at a contradiction since then the degree of χ will be greater than p. Therefore, each ψ_i must have degree one and so each is a linear character. Therefore, P is abelian since P has a faithful representation whose character decomposes into linear characters.

□