7510 HW 5

Duncan Wilkie

27 September 2022

4.2.14. *No finite group G of composite order n with the property that G has a subgroup of order k for each positive integer k dividing n is simple.*

Proof. The smallest prime p in the prime factorization of n is neither 1 nor n, since neither are prime. G has a proper subgroup of order p by definition; Corollary 5 implies this subgroup is normal. Therefore, G has a nontrivial normal subgroup, and is not simple. $\square$

4.3.5. *If the center of G is of index n, then every conjugacy class has at most n elements.*

Proof. The centralizer of any element and the center are normal subgroups, and the latter is a subgroup of the former. So, the third isomorphism theorem applies, and

$$(G/Z(G))/(C_G(s)/Z(G)) \cong G/C_G(s)$$

The order of the right side is the number of elements of the conjugacy class containing s. The numerator of the left side has order n by assumption; by Lagrange's theorem, we then have $|G : C_G(s)| \mid n$, implying the size of each conjugacy class $|G : C_G(s)| \leq n$. $\square$

4.3.13. *Find all finite groups with exactly 2 conjugacy classes.*

Proof. Consider a group G with the above property. Every element of the center corresponds to a singleton conjugacy class, and the identity is always in the center. If there are more than 2 elements in the center, then that's more than 2 conjugacy classes. If there are exactly 2 elements in the center, then there can be no other elements in the group, as they would belong to some other conjugacy classes, and the only group of order 2 is $\mathbb{Z}/2\mathbb{Z}$. If the only element of the center is the identity, and the other conjugacy class has some non-central representative s, the class equation yields

$$|G| = |Z(G)| + |G : C_G(s)| = 1 + |G : C_G(s)|$$

By Lagrange's theorem,

$$|G| = 1 + \frac{|G|}{|C_G(s)|} \Leftrightarrow |G| = \frac{1}{1 - \frac{1}{|C_G(s)|}}$$

The left side is integral, and if the right side is to be also,

$$|C_G(s)| - 1 \mid |C_G(s)| \Leftrightarrow -1 \equiv 1 \pmod{|C_G(s)|}.$$

The only modulus for which this holds is 2, so $|C_G(s)| = 2$. Accordingly, $|G| = 2$, so $G \cong \mathbb{Z}/2\mathbb{Z}$. Then G is Abelian and has 2 elements in its center, a contradiction.

The only group satisfying this property is then $\mathbb{Z}/2\mathbb{Z}$. $\square$

4.3.17. *Let A be a nonempty set and let X be any subset of S_A. Let*

$$F(X) = \{a \in A \mid \sigma(a) = a \text{ for all } \sigma \in X\}$$

be the set of elements fixed by X. Correspondingly, $M(X) = A - F(X)$ are the elements moved by X. Let $D = \{\sigma \in S_A \mid |M(\sigma)| < \infty\}$. Then D is a normal subgroup of S_A.

Proof. First, we show it's a subgroup. Suppose $\sigma, \tau \in S_A$ have $|M(\sigma)| = n$ and $|M(\tau)| = m$. Then $|M(\sigma\tau)| \leq n + m$, because if $\sigma(a) = a$ $(a \notin M(\sigma))$ and $\tau(a) = a$ $(a \notin M(\tau))$ then $\sigma\tau(a) = a$ $(a \notin M(\sigma\tau))$; equivalently, if it's moved by the composition, it must be moved by one of permutations, so $M(\sigma\tau) \subseteq M(\sigma) \cup M(\tau)$. Accordingly, $\sigma\tau \in D$. Secondly, $\sigma^{-1} \in D$, since $\sigma(a) = a \Leftrightarrow \sigma^{-1}(a) = a$, implying no element fixed by σ can be moved by σ^{-1} or $|M(\sigma^{-1})| \leq |M(\sigma)|$.

We now show it's closed under conjugation. Elements of D have cycle decompositions, of finite (although varying) length, since only elements of $M(\sigma)$ are written. By the argument in the text, which doesn't depend on properties of S_n other than that cycle decompositions are finite, $\tau\sigma\tau^{-1}$ has a cycle decomposition given by τ applied to each element of the cycle decomposition of σ. This implies that $\tau\sigma\tau^{-1}$ moves a finite number of elements: those appearing in its cycle decomposition. Therefore, D is normal. $\square$

4.3.29. *Let p be a prime and let G be a group of order p^α. Then G has a subgroup of order p^β for every β with $0 \leq \beta \leq \alpha$.*

Proof. If $\alpha = 0$, then $\beta = 0$, and $G = \langle 1 \rangle$ has a subgroup of order 1. This provides a base case. Suppose for induction that the theorem holds for all prime-power-order groups with exponent less than α. Then it is only necessary to show that G has a subgroup of order $p^{\alpha-1}$, since that subgroup has subgroups of order p^β for $0 \leq \beta \leq \alpha - 1$ by the induction hypothesis, which are subgroups of G themselves.

By Theorem 8, the center of G is nontrivial; it must have order p^γ for some γ with $1 \leq \gamma \leq \alpha - 1$ by Lagrange's theorem. Since the center is a normal subgroup, we can consider $G/Z(G)$, which has order $p^{\alpha-\gamma} < p^\alpha$. By induction, this has subgroups of all orders p^β for $0 \leq \beta \leq \alpha - \gamma$, and by the lattice isomorphism theorem, these are in bijective correspondence with subgroups of G containing $Z(G)$. This bijection has the property that for any $A, B \leq G$ that if $A \leq B$ then $|B : A| = |G/B : G/A|$, so taking $B = G/Z(G)$ and A to be the subgroup of order $p^{\alpha-\gamma-1}$, the corresponding subgroup of G has index p. By Lagrange's theorem applied to this subgroup, call it H,

$$p = \frac{|G|}{|H|} \Leftrightarrow |H| = \frac{|G|}{p} = p^{\alpha-1}$$

so there does indeed exist a subgroup of G of order $p^{\alpha-1}$. $\square$

4.5.13. *All groups of order 56 have a normal Sylow p-subgroup for some prime p dividing their order.*

Proof. Let G be a group of order 56. 56 factors as $2^3 \cdot 7$, so suppose no normal subgroups exist among the Sylow 2-subgroups and Sylow 7-subgroups. By the third part of Sylow's theorem, $n_2 = 1 + k \cdot 2$, $n_2 \mid 7$, $n_7 = 1 + k' \cdot 7$, and $n_7 \mid 8$. If $k, k' = 0$, the corresponding Sylow p-subgroup is normal. Therefore, we must take $k = 3 \Rightarrow n_2 = 7$ and $k' = 1 \Rightarrow n_7 \mid 8$, the former because 7 is prime and the latter from observing $n_7 \leq 8$. The Sylow 7-subgroups are disjoint but for the identity, since the intersection of any two of them is a subgroup of both 7-subgroups, and by Lagrange's theorem, the order of the intersection must divide 7, i.e. be 1. Therefore, the 8 7-subgroups have $8 \cdot 6 = 48$ distinct elements. By the same logic, the 7-subgroups and each of the 2-subgroups are disjoint but for the identity. The 7 Sylow 2-subgroups need not be disjoint with each other, but they all have order 8, so in the worst case that they're all the same, there are at least 8 elements in addition to those from the 7-subgroups, bringing the element total to 56 distinct elements. However, it can't happen that all 2-subgroups are the same; by assumption, $n_2 = 7 \neq 1$, so there's at least an additional element. This is too many elements, so at least one of the Sylow 2- or 7-subgroups of any group of order 56 is normal.

$\square$