Finite (Abelian) Groups and Sylow's Theorems

Dylan C. Beck

Direct Products

Given a finite collection $\{G_i\}_{i=1}^n$ of groups, the Cartesian product $\prod_{i=1}^n G_i = G_1 \times \cdots \times G_n$ is a group: one can easily verify that the group operation given componentwise by

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) \stackrel{\text{def}}{=} (g_1 h_1, \ldots, g_n h_n)$$

is closed and associative; the identity of $\prod_{i=1}^n G_i$ is $(e_{G_1}, \ldots, e_{G_n})$; and inverses are found in the obvious way. We refer to the group $\prod_{i=1}^n G_i$ as the **direct product** of $G_1, \ldots, G_n$. Given that each group G_i is finite (i.e., $|G_i| < \infty$), it follows that $|\prod_{i=1}^n G_i| < \infty$. Explicitly, we have that

$$\left| \prod_{i=1}^n G_i \right| = \prod_{i=1}^n |G_i|$$

by the Fundamental Counting Principle. Our aim is to understand the structure of $\prod_{i=1}^n G_i$.

Proposition 1. Given a group G with normal subgroups N and M such that $N \cap M = \{e_G\}$, we have that $nm = mn$ for all elements n in N and m in M.

Proof. Given any elements n in N and m in M, consider the element $n^{-1}m^{-1}nm$ of G. Our proof is complete once we establish that $n^{-1}m^{-1}nm = e_G$. By hypothesis that $N \trianglelefteq G$, it follows that $m^{-1}nm$ is in N so that $n^{-1}m^{-1}nm$ is in N. Likewise, by hypothesis that $M \trianglelefteq G$, we have that $n^{-1}m^{-1}n$ is in M so that $n^{-1}m^{-1}nm$ is in M. Consequently, we have that $n^{-1}m^{-1}nm = e_G$. □

Theorem 1. Given a group G with normal subgroups $N_1, \ldots, N_k$, if every element of G can be written uniquely as $n_1 \cdots n_k$ for some elements n_i in N_i, then we have that $G \cong \prod_{i=1}^k N_i$.

Proof. Consider the map $\varphi : \prod_{i=1}^k N_i \to G$ defined by $\varphi(n_1, \ldots, n_k) = n_1 \cdots n_k$. By hypothesis, we have that φ is a bijection. We must establish that φ is a group homomorphism, i.e.,

$$n_1 n_1' \cdots n_k n_k' = \varphi((n_1, \ldots, n_k)(n_1', \ldots, n_k')) = \varphi(n_1, \ldots, n_k)\varphi(n_1', \ldots, n_k') = n_1 \cdots n_k n_1' \cdots n_k'.$$

By Proposition 1, it suffices to show that $N_i \cap N_j = \{e_G\}$ for all pairs of integers $1 \leq i < j \leq k$. We leave it to the reader to establish that this is the case. □

Corollary 1. Given a group G with normal subgroups N and M such that $N \cap M = \{e_G\}$ and $G = NM$, we have that $G \cong N \times M$.

Proof. By Theorem 1, it suffices to show that every element of G can be written uniquely as nm for some elements n in N and m in M. We leave the details to the reader. □

Remark 1. Order in a direct product does not matter. Explicitly, we have that $G \times H \cong H \times G$.

Finite Abelian Groups

We say that a group G with the property that $gh = hg$ for all elements g, h in G is **abelian**. Consequently, a finite abelian group G is an abelian group such that $|G| < \infty$.

Remark 2. Every subgroup of an abelian group is normal. Explicitly, given an abelian group G with a subgroup H of G, we have that $gHg^{-1} = Hgg^{-1} = H$ for all elements g of G.

Our prototypical example of an abelian group is $(\mathbb{Z}, +)$; the quotient group $(\mathbb{Z}/n\mathbb{Z}, +)$ is a finite abelian group. By the Fundamental Theorem of Arithmetic, we have that $n = p_1^{e_1} \cdots p_k^{e_k}$ for some prime numbers p_i and non-negative integers e_i. Considering that

$$\left|\frac{\mathbb{Z}}{n\mathbb{Z}}\right| = n = p_1^{e_1} \cdots p_k^{e_k} = \prod_{i=1}^{k} \left|\frac{\mathbb{Z}}{p_i^{e_i}\mathbb{Z}}\right| = \left|\prod_{i=1}^{k} \frac{\mathbb{Z}}{p_i^{e_i}\mathbb{Z}}\right|,$$

there exists a bijection $\mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{k} \mathbb{Z}/p_i^{e_i}\mathbb{Z}$. One might naturally ask if there exists a bijective group homomorphism $\mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{k} \mathbb{Z}/p_i^{e_i}\mathbb{Z}$. We answer this in the affirmative.

Theorem 2. (The Fundamental Theorem of Finite Abelian Groups) Given a finite abelian group G, there exist (not necessarily distinct) primes p_i and non-negative integers e_i such that

$$G \cong \prod_{i=1}^{k} \frac{\mathbb{Z}}{p_i^{e_i}\mathbb{Z}}.$$

We refer to the prime powers $p_i^{e_i}$ as the **elementary divisors** of G.

Corollary 2. Given a finite abelian group G, there exist (not necessarily distinct) positive integers $n_1, \ldots, n_\ell \geq 2$ such that $n_i \mid n_{i+1}$ for each integer $1 \leq i \leq \ell - 1$ and

$$G \cong \prod_{i=1}^{\ell} \frac{\mathbb{Z}}{n_i\mathbb{Z}}.$$

We refer to the positive integers n_i as the **invariant factors** of G. We may adopt the shorthand $\mathbb{Z}/n\mathbb{Z} \stackrel{\text{def}}{=} \mathbb{Z}_n$ with the caveat that this notation will later become ambiguous. For the abelian group

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{25},$$

the elementary divisors are 2, 2, 2^2, 2^3, 3, 3, 5, and 5^2. By arranging the elementary divisors of G creatively, we can find the invariant factors. Explicitly, we have the following algorithm.

1.) Find the prime p that appears the most times in the direct product representation of G. Given that two or more primes appear an equal number of times, choose one arbitrarily.

2.) Create a row of all powers of p that appear in the representation of G, listing these powers in non-increasing order from right to left.

3.) Repeat the second step with the prime q that appears the second most times (or the same number of times as p) in the direct product representation of G.

4.) Continue this process until all primes appearing in the direct product representation of G have been written in a row. One should end with an upper-triangular array.

5.) By multiplying the elements of each consecutive column, we obtain the invariant factors of G.

By following this procedure with the group G at hand, we have the following array.

$$\begin{array}{cccc} 2 & 2 & 2^2 & 2^3 \\ & 3 & 3 & 3 \\ & & 5 & 5^2 \end{array}$$

By multiplying the elements of each consecutive column, we obtain the invariant factors of G: 2, 6, 60, 600. By Corollary 2, we have that $G \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{60} \times \mathbb{Z}_{600}$.

Conversely, one can obtain the elementary divisors from the invariant factors. Observe that

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{14} \times \mathbb{Z}_{98} \times \mathbb{Z}_{294}$$

is a finite abelian group with invariant factors 2, 2, $14 = 2 \cdot 7$, $98 = 2 \cdot 7^2$, and $294 = 2 \cdot 3 \cdot 7^2$. Consequently, we may build an upper-triangular array that contains the elementary divisors.

1.) Given the invariant factors n_i of G with $n_1 \,|\, n_2 \,|\, n_3 \,|\, \cdots \,|\, n_\ell$, express each invariant factor n_i as a product of distinct prime powers by the Fundamental Theorem of Arithmetic.

2.) Create an upper-triangular array whose ith column consists of the distinct prime powers $p_{i,1}^{e_{i,1}}, \ldots, p_{i,k}^{e_{i,k}}$ such that $n_i = p_{i,1}^{e_{i,1}} \cdots p_{i,k}^{e_{i,k}}$.

3.) We obtain the elementary divisors of G as the elements of the upper-triangular array.

By following this procedure with the group G at hand, we have the following array.

$$\begin{array}{ccccc} 2 & 2 & 2 & 2 & 2 \\ & & 7 & 7^2 & 3 \\ & & & & 7^2 \end{array}$$

We find that the elementary divisors of G are 2, 2, 2, 2, 2, 3, 7, 7^2, and 7^2. By Theorem 2, we have that $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{49} \times \mathbb{Z}_{49}$.

Ultimately, the Fundamental Theorem of Finite Abelian Groups implies that the structure of a finite abelian group G is uniquely determined (up to isomorphism) by its elementary divisors (or equivalently, its invariant factors). Further, we note that the elementary divisors of G are (not necessarily uniquely) determined by the unique prime factorization of $|G|$. One can (and should) prove that there are two unique (up to isomorphism) groups of order $4 = 2^2$: the Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$ and the cyclic group $\mathbb{Z}_4$ of order four. Each of these groups corresponds to a distinct **partition** of the integer 2. Generally, we define a partition of an integer n as a k-tuple $(n_1, \ldots, n_k)$ such that $n = \sum_{i=1}^{k} n_i$ and $1 \leq n_1 \leq n_2 \leq \cdots \leq n_k$. Considering that $2 = 1 + 1$ and $2 = 2$, there are two distinct partitions of 2. Consequently, there are two distinct abelian groups of order 4.

Q1a, August 2018. Consider a finite abelian group G. Given that $|G| = 14553000 = 2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11$, how many distinct (up to isomorphism) possibilities are there for the group G?

We have stated the Fundamental Theorem of Finite Abelian Groups without proof, but the tools that are used to in the proof are quite useful to understand on their own. We will also give explicit descriptions of the $\mathbb{Z}_{p_i^{e_i}}$ in the case of the finite cyclic group $\mathbb{Z}_n$ of order n.

We define first the positive integer $\text{ord}(g) = \inf\{k \geq 1 \,|\, g^k = e_G\}$ to be the **order** of g.

Remark 3. Given a finite group G and an element g of order r, we have that

(i.) r divides $|G|$ by Lagrange's Theorem and

(ii.) if $g^n = e_G$, then r divides n by the Euclidean Algorithm.

Explicitly, if we denote $\langle g \rangle$ by H, then we have that $|H| = r$ because the elements $g, g^2, \ldots, g^{r-1}$, and $g^r = e_G$ are all distinct. Consequently, we have that $|G| = |H|[G : H] = r[G : H]$ by Lagrange's Theorem. On the other hand, by the Euclidean Algorithm, we may write $n = pr + q$ for some integers p and $0 \leq q \leq r - 1$. Considering that $e_G = g^n = g^{pr+q} = g^{pr}g^q = (g^r)^p g^q = e_G^p g^q = g^q$ and $r = \text{ord}(g) = \min\{k \geq 1 \,|\, g^k = e_G\}$ by definition, we must have that $q = 0$ so that r divides n.

Proposition 2. Given positive integers m and n with $\gcd(m, n) = 1$, we have that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

Proof. Consider the element $g = (1, 1)$ of $\mathbb{Z}_m \times \mathbb{Z}_n$. Using additive notation, by definition, we have that $\text{ord}(g) = \min\{k \geq 1 \,|\, kg = e_G\} = \min\{k \geq 1 \,|\, k \equiv 0 \,(\text{mod } m) \text{ and } k \equiv 0 \,(\text{mod } n)\}$. Consequently, we have that $m \,|\, k$ and $n \,|\, k$ so that $\text{lcm}(m, n) \,|\, k$. Considering that

$$mn = \text{lcm}(m, n)\gcd(m, n) = \text{lcm}(m, n)$$

by hypothesis that $\gcd(m, n) = 1$, it follows that $mn \,|\, k$ so that $mn \leq k$. But it is always true for any element g of a finite group G that $\text{ord}(g) \leq |G|$, hence we have that $k \leq |\mathbb{Z}_m \times \mathbb{Z}_n| = mn$. We conclude therefore that $k = mn$ so that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic with generator $(1, 1)$ of order mn. Up to isomorphism, the unique cyclic group of order mn is $\mathbb{Z}_{mn}$, hence we must have that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$. □

Theorem 3. Given a positive integer $n = p_1^{e_1} \cdots p_k^{e_k}$ for some distinct primes p_i and non-negative integers e_i, we have that $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$.

Proof. We proceed by induction on the order n of $\mathbb{Z}_n$. Clearly, the claim holds (trivially) for the case that $n = 2$. We will assume inductively that Theorem 3 is true for all groups of order $\leq n$. By Proposition 2, we have that $\mathbb{Z}_n \cong \mathbb{Z}_r \times \mathbb{Z}_s$ for the relatively prime integers $r = p_1^{e_1}$ and $s = p_2^{e_2} \cdots p_k^{e_k}$, hence by induction, we conclude that $\mathbb{Z}_n \cong \mathbb{Z}_r \times \mathbb{Z}_s \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$. □

Given an abelian group G and a prime p, consider the set

$$G(p) = \{g \in G \,|\, \text{ord}(g) = p^n \text{ for some integer } n \geq 0\}.$$

Proposition 3. $G(p)$ is a subgroup of G.

Proof. Observe that $G(p)$ is nonempty: $\text{ord}(e_G) = 1 = p^0$. By the one-step subgroup test, it suffices to prove that if g and h are in $G(p)$, then gh^{-1} is in $G(p)$. We leave this to the reader. □

Proposition 4. Consider an abelian group G and an element g of G with $\text{ord}(g) < \infty$. We have that $g = g_1 \cdots g_k$ for some elements g_i in $G(p_i)$ for each distinct prime p_i such that $p_i \,|\, \text{ord}(g)$.

Proof. We proceed by induction on the number of primes k in the unique prime factorization of $\operatorname{ord}(g)$. Given that $k = 1$, we have that $\operatorname{ord}(g) = p^n$ for some prime p and non-negative integer n, from which it follows that g is in $G(p)$ by definition of $G(p)$.

We will assume inductively that Proposition 4 is true for all elements whose order is divisible by at most $k-1$ distinct primes. Given that $\operatorname{ord}(g) = p_1^{e_1} \cdots p_k^{e_k}$ for some distinct primes p_i and positive integers e_i, we may factor $\operatorname{ord}(g)$ as mn for $m = p_1^{e_1}$ and $n = p_2^{e_2} \cdots p_k^{e_k}$. By hypothesis that the p_i are distinct, we have that $\gcd(m, n) = 1$, hence by Bézout's Theorem, we find that

$$am + bn = 1$$

for some integers a and b. Consequently, we have that $g = g^{am+bn} = g^{am} g^{bn}$. Observe that

$$(g^{bn})^m = g^{bmn} = g^{b \operatorname{ord}(g)} = (g^{\operatorname{ord}(g)})^b = e_G^b = e_G,$$

from which it follows that g^{bn} is in $G(p_1)$. Likewise, we have that

$$(g^{am})^n = g^{amn} = g^{a \operatorname{ord}(g)} = (g^{\operatorname{ord}(g)})^a = e_G^a = e_G,$$

from which it follows that $\operatorname{ord}(g^{am}) \mid n$ so that $\operatorname{ord}(g^{am}) = p_2^{f_2} \cdots p_k^{f_k}$ for some distinct primes p_i and non-negative integers f_i. By induction, we may write $g^{am} = g_2 \cdots g_k$ for some elements g_i in $G(p_i)$ for each distinct prime p_i and $g^{bn} = g_1$ for some g_1 in $G(p_1)$ so that $g = g^{am} g^{bn} = g_1 g_2 \cdots g_k$. □

Theorem 4. Given a finite abelian group G, we have that $G \cong \prod_{i=1}^{k} G(p_i)$ for some distinct primes p_i that divide the order of G.

Proof. By Theorem 1, it suffices to show that every element of G can be written uniquely as $g_1 \cdots g_k$ for some elements g_i in $G(p_i)$, where $g_i = e_G$ if the prime p_i does not divide $\operatorname{ord}(g)$.

Consider two representations $g_1 \cdots g_k = h_1 \cdots h_k$ of an element g in G such that g_i and h_i are in $G(p_i)$. By hypothesis that G is abelian, we have that

$$g_1 h_1^{-1} = h_2 g_2^{-1} \cdots h_k g_k^{-1}.$$

By Proposition 2, $G(p_i)$ is a subgroup of G for each integer $1 \leq i \leq k$, hence $h_i g_i^{-1}$ is in $G(p_i)$ for each integer $2 \leq i \leq k$. By definition, for each integer $2 \leq i \leq k$, we have that $\operatorname{ord}(h_i g_i^{-1}) = p_i^{e_i}$ for some integer $e_i \geq 0$. Consider the integer $n = p_2^{e_2} \cdots p_k^{e_k}$. We have that

$$(g_1 h_1^{-1})^n = (h_2 g_2^{-1} \cdots h_k g_k^{-1})^n = (h_2 g_2^{-1})^n \cdots (h_k g_k^{-1})^n = e_G$$

by hypothesis that G is abelian and $\operatorname{ord}(h_i g_i^{-1}) = p_i^{e_i} \mid n$. But this implies that $\operatorname{ord}(g_1 h_1^{-1}) \mid n$. Considering that $\operatorname{ord}(g_1 h_1^{-1}) = p_1^{e_1}$ for some integer $e_1 \geq 0$, we must have that $e_1 = 0$ so that $g_1 h_1^{-1} = e_G$ or $g_1 = h_1$. Of course, we can repeat this to find that $g_i = h_i$ for all integers $2 \leq i \leq k$. □

Sylow's Theorems

Given a prime p and an integer $n \geq 0$, we say that a group of order p^n is a **p-group**. One refers to a subgroup of a p-group as a p-subgroup, as it is also a p-group by Lagrange's Theorem. Observe that every group contains at least one p-subgroup — namely, the trivial subgroup $\{e_G\}$.

Theorem 5. (Cauchy's Theorem for Finite Groups) Given a finite group G and a prime p that divides $|G|$, there exists an element g in G such that $\text{ord}(g) = p$.

Proof. Consider the set $X = \{(g_1, \ldots, g_p) \in \prod_{i=1}^{p} G \,|\, g_1 \cdots g_p = e_G\}$. Observe that $(g_1, \ldots, g_p)$ is uniquely determined by the $p-1$ elements $g_1, \ldots, g_{p-1}$ that can be chosen without restriction, hence we have that $|X| = |G|^{p-1}$ by the Fundamental Counting Principle. By hypothesis, $|G|^{p-1}$ is divisible by p. Given that $g_1 \cdots g_p = e_G$, it follows that $g_1 \cdots g_{p-1} = g_p^{-1}$ so that $g_p g_1 \cdots g_{p-1} = e_G$. Consequently, we have that $(g_{\sigma(1)}, \ldots, g_{\sigma(p)})$ is in X for each cyclic permutation σ of $\{1, \ldots, p\}$, from which it follows that $\mathbb{Z}/p\mathbb{Z}$ acts on X via $(n + p\mathbb{Z}) * (g_1, \ldots, g_p) = (g_{\sigma_n(1)}, g_{\sigma_n(2)}, \ldots g_{\sigma_n(p)})$, where $\sigma_n(i) = i - n \,(\text{mod } p)$. By the Orbit-Stabilizer Theorem, $|\mathcal{O}(x)|$ divides $|\mathbb{Z}/p\mathbb{Z}| = p$ for each x in X, hence we have that $|\mathcal{O}(x)| \in \{1, p\}$. By the Class Equation for Group Actions, we have that

$$|G|^{p-1} = |X| = \sum_{i=1}^{n} |\mathcal{O}(x_i)|$$

for some representatives x_i of the distinct cosets $G/\operatorname{Stab}_G(x_i)$. Considering that

$$\sum_{i=1}^{n} |\mathcal{O}(x_i)| = |G|^{p-1} \equiv 0 \,(\text{mod } p),$$

we conclude that the number of orbits of size 1 is a multiple of p. Put another way, we have that $|\text{Fix}_{\mathbb{Z}/p\mathbb{Z}}(X)|$ is a multiple of p. Observe that $(e_G, \ldots, e_G)$ is a fixed point of X under the specified action of $\mathbb{Z}/p\mathbb{Z}$, hence we have that $|\text{Fix}_{\mathbb{Z}/p\mathbb{Z}}(X)| \geq p$, i.e., there exists a nontrivial fixed point in X. By definition, there exists an element $(g_1, \ldots, g_p)$ of X such that $(g_{\sigma_n(1)}, \ldots, g_{\sigma_n(p)}) = (g_1, \ldots, g_p)$ for all integers $1 \leq n \leq p$. But we must have therefore that $(g_1, \ldots, g_p) = (g, \ldots, g)$ for some element g of G such that $g^p = e_G$, i.e., such that $\text{ord}(g) = p$. Our proof is therefore complete. □

Proposition 5. Given a finite abelian group G, the group $G(p)$ is a p-subgroup of G.

Proof. By Proposition 2, we have that $G(p)$ is a subgroup of G, hence it suffices to prove that $|G(p)| = p^n$ for some integer $n \geq 0$. On the contrary, we will assume that $|G|$ is divisible by some other prime q. By Cauchy's Theorem, there exists an element g in $G(p)$ of order q. Clearly, this is a contradiction: by definition, the elements of $G(p)$ all have order p^n for some integer $n \geq 0$. □

Given that $|G| = p^n m$ for some non-negative integer m such that $\gcd(p, m) = 1$, we refer to a subgroup of G of order p^n as a **Sylow p-subgroup** of G. We will denote by $\text{Syl}_p(G)$ the set of Sylow p-subgroups of G and by $n_p(G)$ the number of distinct Sylow p-subgroups of G.

Q1b, August 2018. Consider a finite abelian group G. Given a prime p that divides $|G|$, prove that G has a unique Sylow p-subgroup.

Theorem 6. (Sylow's Theorems) Consider a group G of order $p^n m$ such that $\gcd(p, m) = 1$.

1.) There exists at least one Sylow p-subgroup of G. Put another way, $\text{Syl}_p(G)$ is nonempty.

2.) If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists an element g in G such that $Q \subseteq gPg^{-1}$. Particularly, any two Sylow p-subgroups of G are conjugate in G.

3.) We have that $n_p(G) \equiv 1 \pmod{p}$ and $n_p(G) \mid m$.

Remark 4. Given that P is the unique Sylow p-subgroup of G, it follows that P is a normal subgroup of G. Explicitly, the group homomorphism $\chi_g : G \to G$ defined by $\chi_g(h) = ghg^{-1}$ is a bijection, hence we have that $|gPg^{-1}| = |P|$ so that gPg^{-1} is a Sylow p-subgroup of G. By hypothesis, therefore, we conclude that $gPg^{-1} = P$, and this holds for all g in G.

Remark 5. Given distinct Sylow p-subgroups P and Q of order p, we have that $P \cap Q = \{e_G\}$. Considering that $P \cap Q$ is a subgroup of both P and Q, it follows by Lagrange's Theorem that $|P \cap Q|$ divides $|P| = |Q| = p$ so that $|P \cap Q| \in \{1, p\}$. Considering that $P \neq Q$ by assumption, we must have that $|P \cap Q| = 1$. For if $|P \cap Q| = p$, then it would be true that $P = P \cap Q = Q$.

Using Sylow's Theorems. We call a group G **simple** if the only normal subgroups of G are the trivial subgroup $\{e_G\}$ and the group G itself. Prove that a group G of order 1365 cannot be simple.

Proof. Observe that $1365 = 3 \cdot 455 = 3 \cdot 5 \cdot 91 = 3 \cdot 5 \cdot 7 \cdot 13$ is the unique prime factorization of $|G|$. By Sylow's Theorems, we may make the following observations.

(i.) $n_3 \equiv 1 \pmod{3}$ and $n_3 \mid 5 \cdot 7 \cdot 13$ so that $n_3 \in \{1, 7, 13, 5 \cdot 7 \cdot 13\}$

(ii.) $n_5 \equiv 1 \pmod{5}$ and $n_3 \mid 3 \cdot 7 \cdot 13$ so that $n_5 \in \{1, 3 \cdot 7, 7 \cdot 13\}$

(iii.) $n_7 \equiv 1 \pmod{7}$ and $n_7 \mid 3 \cdot 5 \cdot 13$ so that $n_7 \in \{1, 3 \cdot 5\}$

(iv.) $n_{13} \equiv 1 \pmod{13}$ and $n_{13} \mid 3 \cdot 5 \cdot 7$ so that $n_{13} \in \{1, 3 \cdot 5 \cdot 7\}$

Given that any of these integers is 1, we are done by Remark 4. On the contrary, we will assume that none of these integers is 1. Consequently, we have that $n_3 \geq 7$, $n_5 \geq 21$, $n_7 = 15$, and $n_{13} = 105$. Observe that a Sylow p-subgroup of order p has $p-1$ elements of order p. By Remark 5, the distinct Sylow p-subgroups of order p intersect trivially, hence we have that

$$\#\{\text{elements of order } p \text{ in } G\} = (p-1)n_p.$$

We have therefore that there are $\geq 2 \cdot 7 + 4 \cdot 21 + 6 \cdot 15 + 12 \cdot 105$ elements of order 3, 5, 7, or 13. But this is impossible: we have that $|G| = 1365 < 1448 = 2 \cdot 7 + 4 \cdot 21 + 6 \cdot 15 + 12 \cdot 105$. □

Q1, August 2010. Prove that every group G of order 30 has a cyclic subgroup of order 15.

Q1, August 2011. Prove that the center of a non-abelian group G of order 21 is trivial.

Q4, August 2014. Consider a prime $p > 5$ such that $p \not\equiv 1 \pmod{5}$. Prove that any group G of order $15p$ contains a subgroup of order $5p$.

Q2, January 2015. Prove that a group G of order $435 = 3 \cdot 5 \cdot 29$ must be abelian.

Q1c, August 2015 Give an example of a group G with a normal subgroup H such that both H and G/H are nilpotent but G is not nilpotent.

Q1, January 2019. Given a group G such that $|G| = 15$, prove that G is cyclic.