CLASSIFYING GROUPS OF CERTAIN ORDERS

SHIHAN KANUNGO

ABSTRACT. We will first discuss the question of which integers n have exactly one group of order n, namely the cyclic group $\mathbb{Z}/n\mathbb{Z}$. We will see that these are the integers that are relatively prime to the Euler totient function $\phi(n)$. Then we discuss how many groups there are of order p^3 for each prime p. We end with a couple of interesting results and conjectures pertaining to groups of squarefree order.

1 INTRODUCTION

One of the first things we learn in abstract algebra is the notion of a cyclic group. For every positive integer n, we have the cyclic group $\mathbb{Z}/n\mathbb{Z}$, the group of integers modulo n. When n is prime, a simple application of Lagrange's theorem yields that this is the *only* group of order n. We may ask ourselves: what other positive integers have this property? That is, for which positive integers n is every group of order n cyclic?

This is not a new problem; the first solution is attributed to Burnside and has appeared in numerous papers. Dickson [4] determined in 1905 those n for which all groups of order n are abelian. The earliest proof focusing specifically on n for which all groups of order n are cyclic (not just abelian) was given by Szele [7] in 1947.

Definition 1.1. For $n \in \mathbb{N}$ let $f(n)$ denote the number of (isomorphism classes of) groups of order n.

QUESTION. Is there a good characterization of n such that $f(n) = 1$?

Considering $f(n)$ for small values of n we see that $f(2) = f(3) = 1$ because 2, 3 are primes. However, for $n = 4$ already we have $f(4) > 1$.

EXAMPLE. $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are non-isomorphic: they have different maximal orders for their elements: 4, and 2 respectively. In general, $f(p^2) > 1$ because $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ has p^2 elements, has no element of order p^2, and is therefore not cyclic.

More generally, if $p^2 \mid n$ for some prime p, and if $m = n/p^2$, then $f(n) > 1$ because

$$\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, \quad \text{and} \quad \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

are non-isomorphic groups of order n. Thus, at the very least we need n to be *squarefree*.

Definition 1.2. Integers that are divisible by no perfect square other than 1 are called *squarefree integers*. For example, $10 = 2 \cdot 5$ is squarefree, but $18 = 2 \cdot 3^2$ is not.

Observation 1.3. If $f(n) = 1$ then n must be squarefree.

However, the converse is false, since $f(6) = 2$.

EXAMPLE (The dihedral group D_3). D_3 has 6 elements and is generated by the two elements $\{\rho, \tau\}$ where ρ is counterclockwise rotation by $2\pi/3$, and τ is the reflection across the line $y = 0$. Moreover, we have the relation $\rho\tau = \tau\rho^{-1}$, so D_3 is not abelian.

In general, for any integer $n > 1$, the dihedral group D_n has $2n$ elements, and is generated by $\{\rho, \tau\}$ with $\rho\tau = \tau\rho^{-1}$. Thus D_n is not abelian, and $f(2n) > 1$. Thus, we get

Observation 1.4. If $f(n) = 1$, then either $n = 2$ or n must be a squarefree odd integer.

Once again, the converse is false, since $f(21) = 2$. This time, however, the reason is not so obvious. It is not straightforward to come up with a group of order 21 that is not isomorphic to $\mathbb{Z}/21\mathbb{Z}$. We need to introduce the notion of a semidirect product of groups.

2 The Semidirect Product

We start with a definition:

Definition 2.1. Let H and K be groups and let $\psi : K \to \mathrm{Aut}(H)$ be a homomorphism. Let $G = \{(h, k) : h \in H \text{ and } k \in K\}$. Define multiplication on G by

$$(h_1, k_1)(h_2, k_2) = (h_1\psi(k_1)(h_2), k_1k_2).$$

This multiplication makes G a group of order $|G| = |K||H|$, where the identity of G is (e_H, e_K), and $(h, k)^{-1} = (\psi(k^{-1})(h^{-1}), k^{-1})$ is the inverse of (h, k). The group G is called the **semidirect product** of H and K with respect to ψ (denoted by $H \rtimes_\psi K$).

REMARK (The semidirect product is the direct product if the homomorphism ψ is trivial). Suppose H and K are groups and $\psi : K \to \mathrm{Aut}(H)$ is the trivial homomorphism, i.e. $\psi(k) = \mathrm{id}$, for all $k \in K$. Then

$$(h_1, k_1)(h_2, k_2) = (h_1 \cdot \psi(k_1)(h_2), k_1k_2) = (h_1h_2, k_1k_2).$$

Hence $H \rtimes_\psi K \cong H \times K$.

The set of automorphisms of a group plays a central role in the study of semidirect products. The semidirect product is distinct from the direct product only if there is some non-trivial homomorphism $\psi : K \to \mathrm{Aut}(H)$, which only happens if $|K|$ divides $|\mathrm{Aut}(H)|$. Let us remind ourselves how to compute $|\mathrm{Aut}(H)|$ when H is a cyclic group.

Proposition 2.2. $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ *and this is an abelian group of order* $\phi(n)$.

Proof. See Problem 7, Chapter 5, of the textbook [6]. □

The way we will be using semidirect products is by showing that for some values of n, there is a group of order n that is isomorphic to a semidirect product of some two of its subgroups. The following proposition makes this idea concrete.

Proposition 2.3. *Suppose H and K are subgroups of group G such that $H \lhd G$, $H \cap K = \{e\}$, and $|G| = |H| \cdot |K|$. Then $G \cong H \rtimes_\psi K$ for some $\psi : K \to \mathrm{Aut}(H)$.*

NOTE: When this happens, K is said to be a *complement of H* in G.

We can now understand why $f(21) = 2$. This is because $21 = 3 \cdot 7$ and $3 \mid (7-1)$.

EXAMPLE (Groups of order pq with $p \equiv 1 \pmod{q}$). Let G be a group of order pq where $p > q$ are distinct primes. Then there is only one Sylow p-subgroup P, which is therefore normal. Let Q be a Sylow q-subgroup. Then Q is a complement of P in G, so G is a semi-direct product $P \rtimes_\psi Q$, for some homomorphism $\psi : Q \to \mathrm{Aut}(P)$. Since $q \mid (p-1)$, then $\mathrm{Aut}(P) \cong \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ has a unique subgroup of order q, and ψ can be an isomorphism from $\mathbb{Z}/q\mathbb{Z}$ to this subgroup. We can choose a generator for $\mathbb{Z}/q\mathbb{Z}$ to map to a specified element of order q in $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$. So there is, up to isomorphism, a unique semi-direct product which is not a direct product. In other words, the number of groups of order pq (up to isomorphism) is 2 if $q \mid (p-1)$, and 1 otherwise.

We can gather all these observations into one useful lemma.

Lemma 2.4. *If $n = pq$ where $p \mid (q-1)$ then there exists a semidirect product of the cyclic group of order p and the cyclic group of order q. In particular, $f(n) = 2$.*

Proof. Example above. □

It is easy to see that this can, in fact, be extended to any squarefree integer n.

Proposition 2.5. *If $n = p_1 p_2 \cdots p_k$ where the p_i are distinct primes and $p_i \mid (p_j - 1)$ for some $i \neq j$, then $f(n) > 1$.*

Proof. If $n = pqm$ where $p \mid (q-1)$ and $\gcd(pq, m) = 1$, then there is a (nontrivial) semidirect product $\mathbb{Z}/p\mathbb{Z} \rtimes_\psi \mathbb{Z}/q\mathbb{Z}$ and therefore $(\mathbb{Z}/p\mathbb{Z} \rtimes_\psi \mathbb{Z}/q\mathbb{Z}) \times \mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ are non-isomorphic groups of order n. □

This concludes our discussion about semidirect products. We will be using it in crucial ways throughout the rest of the discussion. We are now ready to state the answer to our question.

3 The Main Theorem

At the end of Section 1 we concluded that it was enough to restrict our attention to the odd, squarefree integers. In Section 2 we discovered that if n is squarefree and $p \mid (q-1)$ for some primes p, q dividing n, then we have a semidirect product in addition to the cyclic group of order n. This is the same as saying that if $f(n) = 1$ then $\gcd(n, \phi(n)) = 1$ where $\phi(n)$ is the Euler totient-function.

Lemma 3.1. *Let n be an integer. Then the following statements are equivalent:*

(a) *$n = p_1 p_2 \cdots p_k$ where the p_i are distinct primes and $p_i \nmid (p_j - 1)$ for $i \neq j$.*

(b) *$\gcd(n, \phi(n)) = 1$, where ϕ is the Euler ϕ-function.*

Proof. If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ then $\phi(n) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_k^{a_k-1}(p_1-1)(p_2-1)\cdots(p_k-1)$. □

Lemma 3.1 allows us to restate Proposition 2.5 as

Proposition 3.2. *If* $f(n) = 1$ *then* $\gcd(n, \phi(n)) = 1$.

... and this time the converse also holds! We thus obtain a tidy classification for integers n such that there is exactly one group of order n.

Theorem 3.3. *For a positive integer* n*, the only group of order* n *is the cyclic group* $\mathbb{Z}/n\mathbb{Z}$ *if and only if* $\gcd(n, \phi(n)) = 1$*, where* ϕ *denotes the Euler-phi function.*

Proposition 3.2 proves that the condition is necessary. It will take us quite a bit more work to prove that it is also sufficient. We will do so by first discovering that groups of squarefree order satisfying the conditions of the theorem possess a couple of "nice" properties, and then showing inductively that those properties force the group to be cyclic.

4 Groups Of Squarefree Order

We will build our group inductively, out of its subgroups. But what kind of subgroups should we look for? We have seen that abelian groups are one class of groups that we largely understand; in fact we have a precise classification of all finite abelian groups. Therefore we will try to decompose our group into abelian subgroups. Groups that permit such a subdivision are the solvable groups, so our first step is to show that any group of odd squarefree order is solvable.

Proposition 4.1. *Let* G *be a group of order* $p_1 p_2 \ldots p_k$*, where* $p_1, p_2, \ldots, p_k$ *are distinct primes. Then* G *is solvable.*

Proof. We use induction on the number of primes, s, dividing n. If $s = 1$, then G is a cyclic group, hence solvable. Assume that the claim holds for $s = k$ i.e. every group of order $p_1 p_2 \ldots p_k$ is solvable and suppose G is a group with $|G| = p_1 p_2 \ldots p_k p_{k+1}$.

Since Sylow subgroups for different primes p have prime order, a simple counting argument on the non-identity elements in each Sylow subgroup shows that some Sylow subgroup must be normal in G. Suppose H is a normal Sylow p_{k+1}-subgroup of G (after reordering, if necessary). Then G/H is a group of order $p_1 p_2 \cdots p_k$. By induction hypothesis G/H is solvable. The rest follows directly from the results of Problems 17, 18 of Chapter 5 of the textbook [6]: Since H is a cyclic subgroup of G, H is solvable. Since H and G/H are solvable, therefore G is also solvable. This establishes the claim. □

Proposition 4.1 guarantees that we have enough abelian subgroups inside G. Now we have to find a way to take two of them of the right size and "glue" them together. The way we imagine groups being built out of smaller pieces is that if G is a finite group and $H \lhd G$, then G is built out of H and G/H. Thus, we can break down a group into smaller pieces if it has a nontrivial normal subgroup of the right index.

Proposition 4.2. *Let G be a group of order $p_1p_2\dots p_k$, where $p_1, p_2, \dots, p_k$ are distinct primes. Then G has a normal subgroup of prime index.*

We will need the notion of a *commutator subgroup*. In Problem 6, Chapter 3 of the textbook [6], we learnt that the commutator subgroup $[G, G]$ of G is the subgroup generated by all elements of the form $[g, h] := ghg^{-1}h^{-1}$. We also showed that $G/[G, G]$ is always abelian. We will be using both these facts in the proof below.

Proof. By proposition 4.1, G is solvable, so commutator $G' = [G, G]$ is not equal to G. Then G' is either $\{e\}$ or a proper subgroup of G. If $G' = \{e\}$, then G is abelian. Suppose G' is a proper subgroup of G. Then (after reordering, if necessary) $|G'| = p_1p_2\cdots p_j$, where $1 \leqslant j < k$. So the quotient group G/G' is an abelian group of order $p_{j+1}\cdots p_k$. Therefore by Cauchy's theorem G/G' has a normal subgroup H/G' of order $p_{j+1}\cdots p_{k-1}$. Hence H is also a normal subgroup of G and $|H| = p_1p_2\cdots p_{k-1}$, so $[G : H] = p_k$. □

Now we have everything we need to prove Theorem 3.3.

5 Proof Of Theorem

Proof of Theorem 3.3. Suppose $\gcd(n, \phi(n)) = 1$. Then $n = p_1p_2 \cdot p_k$ for distinct primes p_i and $p_i \nmid (p_j - 1)$ for $i \neq j$. We show that $\mathbb{Z}/n\mathbb{Z}$ is the only group of order n. We use induction on k, the number of prime factors of n.

If $k = 1$ then $n = p_1$ i.e. n is a prime. Since every group of prime order is cyclic, $\mathbb{Z}/n\mathbb{Z}$ is the only group of order n. Assume that the result is true for $k = r$ i.e. for $n = p_1p_2\cdots p_r$, $\mathbb{Z}/n\mathbb{Z}$ is the only group of order n. We will show that the result is true for $k = r + 1$ i.e. for $n = p_1p_2\cdots p_{r+1}$. Let G be a group of order $n = p_1p_2\cdots p_{r+1}$.

By Proposition 4.2, G has a normal subgroup, H, of index p_i for some $i \in \{1, \dots, r+1\}$. After reordering, if necessary, we can assume that $H = \mathbb{Z}/m\mathbb{Z}$, where $m = p_1p_2\cdots p_r$ and $\gcd(m, \phi(m)) = 1$. Take $K = \mathbb{Z}/p_{r+1}\mathbb{Z}$ and consider the semi direct product of H and K. It exists, because semi direct product of any two groups exist. Since H is a cyclic group, so $|\operatorname{Aut}(H)| = (p_1 - 1)\cdots(p_r - 1)$. Then any homomorphism from K to $\operatorname{Aut}(H)$ must be a trivial homomorphism, because otherwise it would contradict $\gcd(n, \phi(n)) = 1$. Therefore the semi-direct product of H and K is actually just the direct product of H and K, which is a cyclic group of order $p_1p_2\cdots p_{r+1}$. Since H is the only group of order m, $\mathbb{Z}/n\mathbb{Z}$ is the only group of order $n = p_1p_2\cdots p_{r+1}$. □

Those n, for which $f(n) = 1$, are tabulated at `http://oeis.org/A003277`

1, 2, 3, 5, 7, 11, 13, 15, 17, 19, 23, 29, 31, 33, 35, 37, 41, 43, 47, 51, 53, 59, 61, 65, 67, 69, 71, 73, 77, 79, 83, 85, 87, 89, 91, 95, 97, 101, 103, 107, 109, 113, 115, 119, 123, 127, 131, 133, 137, 139, 141, 143, 145, 149, 151, 157, 159, 161, 163, 167, 173 ...

This concludes our discussion of integers n such that there is exactly one group (up to isomorphism) of order n. We now move on to explore how many groups there are of order p^3 for a given prime p.

6 Groups of Order p^3

For each prime p, we want to describe the groups of order p^3 up to isomorphism.

This was done for $p = 2$ by Cayley in 1854 and for odd p by Cole & Glover, Hölder, and Young independently in 1893.

From the cyclic decomposition of finite abelian groups, there are three abelian groups of order p^3 up to isomorphism: $\mathbb{Z}/p^3\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. These are nonisomorphic since they have different maximal orders for their elements: p^3, p^2, and p respectively. There are two nonabelian groups of order p^3 up to isomorphism. The descriptions of these two groups will be different for $p = 2$ and $p \neq 2$.

Theorem 6.1. *A nonabelian group of order 8 is isomorphic to D_4 or to Q_8.*

Example (The Quarternion Group Q_8). $Q_8 = \{1, -1, i, j, k, -i, -j, -k\}$ is the group of order 8 with the multiplication rules $-1 = i^2 = j^2 = k^2 = ijk$.
The element 1 represents the identity and $(-1)^2 = 1$ and -1 is in the center (so $(-1)i = i(-1) = -i$, $(-1)j = j(-1) = -j$, etc.). Then Q_8 has the following subsets:

$$\{1\}, \{1, -1\}, \{1, -1, i, -i\}, \{1, -1, j, -j\}, \{1, -1, k, -k\}, Q_8$$

Every subgroup of Q_8 is normal in Q_8. We know that if G is an abelian group then all subgroups of G are normal. However the group Q_8 is non-abelian and yet all of its subgroups are normal.

Theorem 6.2. *For primes $p \neq 2$, a nonabelian group of order p^3 is isomorphic to* $\mathrm{Heis}(\mathbb{Z}/p\mathbb{Z})$ *or G_p.*

$$\mathrm{Heis}(\mathbb{Z}/p\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}$$

and

$$G_p = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{Z}/p^2\mathbb{Z},\ a \equiv 1 \pmod{p} \right\} = \left\{ \begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} : m, b \in \mathbb{Z}/p^2\mathbb{Z} \right\}$$

Keith Conrad [2] summarizes what is known about the count of groups of small p-power order.

- There is one group of order p up to isomorphism ($\mathbb{Z}/p\mathbb{Z}$).
- There are two groups of order p^2 up to isomorphism: $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
- There are five groups of order p^3 up to isomorphism, but the explicit description of them is not uniform in p since the case $p = 2$ needs a separate treatment.

For groups of order p^4, the count is no longer uniform in p: there are 14 groups of order 2^4 and 15 groups of order p^4 for $p \neq 2$. This is due to Hölder and Young.

7 Further Results and Conjectures

One of the first mathematicians to make advances in the enumeration of finite groups was Otto Hölder. In 1893, he described groups of order p^3 and p^4. Shortly thereafter, he derived a remarkable formula for the number of groups of order n when n is square-free.

Theorem 7.1 (Hölder, 1895). *The number of groups of order n, where n is square-free is given by*

$$f(n) = \sum_{m \mid n} \prod_{p} \frac{p^{c(p)} - 1}{p - 1}$$

where p runs over all prime divisors of n/m and $c(p)$ is the number of prime divisors q of m that satisfy $q \equiv 1 \pmod{p}$.

A natural question that arises from Hölder's formula is: for n squarefree, can we relate $f(n)$ to n more explicitly? McIver and Neumann determined that $f(n) \leqslant n^4$ for n square-free. An even better bound, is known: $f(n) \leqslant \phi(n)$, where ϕ is Euler's ϕ-function. For squarefree $n = p_1 p_2 \cdots p_r$ and greater than 1, this last result implies that

$$f(n) \leqslant \phi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_r - 1) < n.$$

Furthermore, if n is even and squarefree, then $p_1 = 2$ and

$$f(n) \leqslant \phi(n) = 1(p_2 - 1) \cdots (p_r - 1) < \frac{n}{2}.$$

Another direction is to understand the asymptotic behavior of $f(n)$ when n is square-free. In this light, define

$$M := \limsup_{n \to \infty} \frac{\log f(n)}{\log n}$$

where the limit superior ranges just over squarefree integers n. Erdös, Murty, and Murty have shown that $M = 1$. Their proof uses Dirichlet's Theorem on primes in arithmetic progressions, among other techniques.

We mention one final, curious conjecture in the enumeration of finite groups:

Conjecture 7.2. *The group enumeration function is surjective.*

That is, for every positive integer m, the conjecture asserts that there exists n such that $f(n) = m$. This conjecture may well be resolved through consideration of squarefree n, largely because of Hölder's formula. Indeed, it has been verified that every m less than 10,000,000 is equal to $f(n)$ for some squarefree n.

References

[1] I. Ganev, Groups of a Square-Free Order, *Rose-Hulman Undergraduate Mathematics Journal:* **Vol. 11** (2010) : Iss. 1 , Article 7.
Available at: https://scholar.rose-hulman.edu/rhumj/vol11/iss1/7

[2] K. Conrad, Groups of Order p^3, *Expository Papers.*
https://kconrad.math.uconn.edu/blurbs/grouptheory/groupsp3.pdf

[3] K. Conrad, When Are All Groups of Order n Cyclic?, *Expository Papers.*
https://https://kconrad.math.uconn.edu/blurbs/grouptheory/allgrouporderncyclic.pdf

[4] L. E. Dickson, Definitions of a group and a field by independent postulates, *Trans. Amer. Math. Soc.* **6** (1905), 198-204. Online at http://www.ams.org/journals/tran/1905-006-02/S0002-9947-1905-1500706-2/S0002-9947-1905-1500706-2.pdf.

[5] S. K. Upadhyay and S. D. Kumar, Existence of a Unique Group of Finite Order, *The Mathematics Student* **81** (2012), 215-218.
Online at http://www.indianmathsociety.org.in/mathstudent2012.pdf.

[6] S. Rubinstein-Salzedo, Abstract Algebra, *self-published*

[7] T. Szele, Uber die endlichen Ordnungszahlen, zu denen nur eine Gruppe gehört, *Comm. Math. Helv.* **20** (1947), 265-267. Online at https://eudml.org/doc/138922.