University of Nevada, Reno

Finding Minimal n-Power Extensions of Groups

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Mathematics

by

William D. Taylor

Dr. Valentin Deaconu/Thesis Advisor

May, 2010

**UNIVERSITY
OF NEVADA
RENO**

We recommend that the thesis
prepared under our supervision by

WILLIAM D. TAYLOR

entitled

Finding *n*-Power Extensions of Groups

be accepted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE

Valentin Deaconu, Ph.D., Advisor

Swatee Naik, Ph.D., Committee Member

Federico Guerrero, Ph.D., Graduate School Representative

Marsha H. Read, Ph.D., Interim Graduate Dean

May, 2010

Abstract

In this paper we consider the group-theoretic analogue of Galois Theory. That is, given a group G and a natural number n, we find groups H such that G can be embedded into H in such a way that every element of G has an nth root in H. It is not difficult to see (and we prove) that given any group G and natural number n such an extension of G exists. In this paper, we attempt to find the smallest order of such an extension, which we will call the minimal n-index of G. We answer the question completely for cyclic groups. Further, we examine certain ways of constructing new groups from old, in particular the direct and semidirect product, and determine how these constructions interact with the minimal n-index of G. We conclude with some conjectures regarding the minimal n-index and some questions to inspire further research.

Contents

1 Introduction

One of the most natural questions that arises when an algebraic object is explored is the question of solvability of equations. Under what conditions, we ask, can a certain type of equation or system of equations be solved? This question is examined by high school students in the case when we are dealing with the real or complex numbers. More advanced subjects allow for the same questions to be asked of different algebraic structures. Galois Theory in particular is reminiscent of our efforts in this paper, and indeed this paper could be thought of as a generalization of Galois Theory, in that we are studying groups rather than fields. Unfortunately, this generalization means we must do without much of the structure afforded us by fields.

In this paper we will be looking at the solvability of the equation $X^n = g$ where $n \in \mathbb{N}$ is a fixed natural number and g is an element in a given group G. As in the real numbers, this equation is often unsolvable for certain values of g. For instance, in the dihedral group D_8, there is no transformation that when squared yields a reflection. We can "fix" this by thinking of the group G as sitting inside a larger group, in much the same way that we think of the real numbers as sitting inside the complex. However, we will not require as much as is given by the extension from $\mathbb{R}$ to $\mathbb{C}$. What we will be looking for is a group H "containing" G such that every element of G has an nth root in H.

2 Definitions and Notation

We will have some standard notation that we will use as shorthand for more unwieldly statements that would become tedious to write repeatedly. Our desire to be consistent and write all groups multiplicatively prompts us to abandon the traditional notation for cyclic groups, namely $\mathbb{Z}_m$ for finite and $\mathbb{Z}$ for infinite cyclic groups. Since these groups, when written in the traditional manner, are almost always written additively, rather than attempting to constantly keep track of whether we are in an additive or multiplicative case, or (perhaps worse) use the traditional notation with a nontraditional operation, we will simply abandon the old notation and use a new one.

Notation 1. In all but one subsection, groups in this paper will be written multiplicatively. Additionally, certain groups will have particular symbols that will be used consistently. C_m will be the cyclic group of order m; $C_m a$ will be the cyclic group of order m with generator a (where a will vary). Similarly, C_∞ will be the infinite cyclic group, and $C_\infty a$ the infinite cylic group with generator a. We will use D_m to indicate the dihedral group of order $2m$, i.e. the group of symmetries of a regular m-gon.

We now define the basic terms upon which our entire discussion will be based.

Definition 1. Let G be a group and $n \in \mathbb{N}$ be a natural number.

- Let $\Omega_n(G) = \{g \in G \mid \exists(x \in G)(x^n = g)\}$ be the set of elements in G which have nth roots.
- The group G will be called *n-divisible* if $\Omega_n(G) = G$. The group G will be called *divisible* if G is n-divisible for all $n \in \mathbb{N}$.
- If H is a group such that $G \cong G' \leq H$ and $G' \subset \Omega_n(H)$, then G is said to be *n-divisible in H* and H is said to be an *n-power extension* of G . If G is n-divisible in H for all $n \in \mathbb{N}$, we say G is *divisible in H*, and H is a *power extension* of G.

- If H is a group and G is n-divisible in H, then any injective homomorphism $f : G \to H$ such that $f(G) \subset \Omega_n(H)$ is called an *n-embedding of G into H*, or simply an *n-embedding* if the groups are understood. We will sometimes combine many of the previous definitions by simply writing $f : G \hookrightarrow_n H$, which will mean that f is an n-embedding of G into H.

- If $f : G \hookrightarrow_n H$ and $[H : f(G)] = m$, then H is said to be an n-power extension of order m. Let

$$\mu_n(G) = \min_{f,H} \{[H : f(G)] \mid f : G \hookrightarrow_n H\} \in \mathbb{N} \cup \{\infty\}.$$

  This is called the *minimal n-index of G*.

- If G is a group and H is a power extension of G, then any injective homomorphism $f : G \to H$ such that $f(G) \subset \Omega_n(H)$ for all $n \in \mathbb{N}$ is called a *power embedding of G into H*.

Intuitively, $\mu_n(G)$ indicates how much bigger an n-power extension of G has to be. When G is a finite group, say of order m, then $m \cdot \mu_n(G)$ is the smallest size that any n-extension of G can be. The following Lemma is immediate from the definiton and basic properties of groups.

Lemma 1. For any group G that possesses an n-power extension, $\mu_n(G) \geq 1$.

Much of this paper will be devoted to finding the values of $\mu_n(G)$ for various families of groups. This will tell us how hard we have to work to have nth roots of everything in G. Many of our proofs and examples will be constructive. In some cases, we will not be able to give exact values of $\mu_n(G)$, but will be able to place bounds on it.

We must begin by making the argument that the definition of minimal n-index is well-defined for every group G. We begin by recalling the definition of a presentation of a group. The following definiton is adapted from [Dum]. Recall that for any set G and subset $S \subset G$, smallest subgroup of G that contains all the elements of S is called the subgroup generated by S and is denoted $\langle S\rangle$.

Definition 2. Let G be a group and let S be a subset of G. If $S \subset G$ and $\langle S\rangle = G$, then a *presentation* of G is a pair $\langle S : R\rangle$, where R is a set of words in $F(S)$ (the free group on S) such that the normal closure of $\langle R\rangle$ in $F(S)$ (i.e. the smallest normal subgroup of $F(S)$ containing $\langle R\rangle$) equals the kernel of the homomorphism $\pi : F(S) \to G$, where π acts as the identity on the elements of S. The elements of S are called *generators* and those of R are called *relations* of G.

Intuitively, S gives the "building blocks" for the group G and R tells how those blocks combine together. The elements of R are of the form $s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_m^{\alpha_m}$ for some $s_i \in S$ and $\alpha_i \in \mathbb{Z}$. The fact that this word is in R means that in the group G, $s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_m^{\alpha_m} = 1$. The relations in R are sometimes written as equations rather that as words. In addition, when the numbers of generators and relations are small, the presentation of G is often written as $\langle s_1, s_2, \ldots, s_m : r_1, r_2, \ldots, r_k\rangle$, with the elements of S and R listed. Many times, we abuse the notation slightly and write that a group is equal to its presentation, e.g. $G = \langle S : R\rangle$. This should in general cause no confusion.

For example, a presentation of the finite cyclic group C_m is $\langle a : a^m\rangle$. The infinite cyclic group has no relations. In this case, we write a dash in the second coordinate of the presentation notation, as so: $C_\infty = \langle a : -\rangle$. By way of further example, the dihedral group D_m has the presentation $D_m = \left\langle r, s : r^m = s^2 = 1, rs = sr^{-1}\right\rangle$. This notation, involving the equations in the second coordinate, is a convenient way to write and understand the relations. In order to write this according to the technical definition, we would solve each of the equations for the identity 1 on one side, and then the other side of the equation would be the word in R. So for this example, we might write $G = \langle S : R\rangle$, where $S = \{s, r\}$, $R = \left\{r^m, s^2, rsrs^{-1}\right\}$.

This digression into presentations will be of use to us in the next very important proposition but we will not use it much later in the paper.

Proposition 2. Let G be a group. There exists an n-power extension H of G.

Proof. Let $G = \langle S : R \rangle$ be a presentation of G. Let $A = \left\{ a_g \mid g \in G \right\}$ be a set indexed by the elements of G. Form the group $H = \langle S, A : R, P \rangle$, where $P = \left\{ a_g^n g^{-1} \mid g \in G \right\}$. Then G naturally embeds into H and by construction, every element of G has an nth root in H. Therefore H is an n-power extension of G. □

The first family of groups we will consider is finite groups. Our first theorem gives us an important bound on $\mu_n(G)$ for finite groups G.

Proposition 3. If G is finite and $n \in \mathbb{N}$, then $\mu_n(G) < \infty$.

Proof. See Section 3 of [Lyn]. □

We will see in a few pages that $\mu_n(C_\infty) < \infty$, and therefore that the converse of Proposition 3 is in general false. Another very important class of groups is the class of abelian groups. The next proposition gives us a similar result to Proposition 3 for this class of groups.

Proposition 4. If G is abelian and $n \in \mathbb{N}$, then there exists an abelian n-power extension of G.

Proof. Since G is abelian, it is a $\mathbb{Z}$-module (for an excellent introduction to module theory, see [Dum]). Corollary 10.37 from [Dum] implies that therefore G is a submodule of some injective $\mathbb{Z}$-module H. Since $\mathbb{Z}$ is a Principal Ideal Domain, Proposition 10.36 (2) from [Dum] shows that H is divisible, i.e. that the equation $x^r = h$ is solvable for all $r \in \mathbb{Z}$, $h \in H$. In particular the equation $x^n = g$ is solvable for all $g \in G \subset H$. Therefore H is an n-power extension of G. □

One technique that we will use several times throughtout this paper is essentially a building up of necessary conditions for H to be an n-power extension of G. The first requirement is that we need an injective homomorphism $f : G \rightarrow H$. This will often give severe restrictions on the structure of H. Once we have constrained H in this way, we can determine what conditions need to be met in order for us to have $f : G \hookrightarrow_n H$. As was shown above, this is always possible. However, as we shall see especially in the section on semidirect products that if we add more conditions besides these on the structure of H, we may find that there is no possible n-power extension satisfying these conditions.

Next we give a potentially useful proposition that can sometimes allow us to prove that a particular group H is *not* a minimal n-power extension of G.

Proposition 5. If $f : G \hookrightarrow_n H$, $N \lhd H$, and $N \cap f(G) = \{1\}$, then $\overline{f} : G \hookrightarrow_n H/N$, where $\overline{f}(g) = f(g)N$.

Proof. We must show that $\overline{f}$ is a monomorphism and for every $g \in G$, $\exists xN \in H/N$ such that $(xN)^n = \overline{f}(g) = gN$. The second condition is clearly satisfied, since if $f : G \hookrightarrow_n H$, there exists $x \in H$ such that $x^n = f(g)$. Clearly, then $(xN)^n = x^n N = f(g)N = \overline{f}(g)$. If $\overline{f}(g) = 1N$, then $f(g) \in N$. Since $f(G) \cap N = \{1\}$, $f(g) = 1$, and since f is injective, $g = 1$. So $\overline{f}$ is a monomorphism. □

Note that this proposition implies that if the hypotheses are satisfied, then $\mu_n(G) \leq [H/N : \overline{f}(G)]$, and further, if $[H : f(G)]$ is finite, then $\mu_n(G) < [H : f(G)]$.

3 Cyclic Groups

3.1 Finite Cyclic Groups

Cyclic groups are in a way the simplest of all groups. They have only a single generator and a very simple presentation. What is also beneficial about cyclic groups is that their structure can often be described using number-theoretic machinery, allowing for more theorems and techniques to be applied to the problem of finding n-power extensions. In later sections we will often consider cyclic groups as special cases for more development. Cyclic groups have a very simple structure, and because of this it is only necessary to look at cyclic extensions of cyclic groups when attempting to find n-power extensions.

Proposition 6. Suppose G is a cyclic group with generator a and $f : G \hookrightarrow_n H$. Then there exists a cyclic group $C \leq H$ such that $f : G \hookrightarrow_n C$. The group C is finite if and only if G is finite.

Proof. Choose $x \in H$ such that $x^n = f(a)$. Let $C = \langle x \rangle$. Then C is a cyclic group. $f(G) \leq C$, since for any $k \in \mathbb{Z}$, $f(a^k) = (x^n)^k = x^{nk} \in C$. Further, C_m is n-divisible in C: Let $a^k \in C_m$, then $x^k \in C$ and $(x^k)^n = (x^n)^k = a^k$. If G is finite, say of order m, then $x^{nm} = f(a)^m = f(a^m) = f(1) = 1$. So $|C| = |\langle x \rangle| \leq mn$, i.e. C is finite. If G is infinite, then since G embeds into C, we know C is infinite. □

So we have determined that we may restrict our attention entirely to cylic groups for the purposes of this discussion. We now turn to some number theoretic results that will drive our later discussion. Our first proposition is an elementary result, proved here for completeness' sake. It will be the basis on which many of the theorems in this paper rest.

Proposition 7. Let $G = C_m a$. The equation $x^n = a^k$ is solvable in G if and only if $(m,n) \mid k$.

Proof. Suppose $\exists x \in G$ such that $x^n = a^k$. Then $x = a^q$ for some $q \in \mathbb{Z}$, so $a^k = (a^q)^n = a^{qn}$. This implies that $k \equiv qn (\operatorname{mod} m)$. So $k = qn + pm$ for some $p \in \mathbb{Z}$. Since $(m,n) \mid m,n$, we conclude $(m,n) \mid k$.

Now suppose $(m,n) \mid k$. Let $p,q \in \mathbb{Z}$ such that $pm+qn = (m,n)$, and set $k' = \frac{k}{(m,n)}$. Let $x = a^{k'q}$. Then

$$x^n = a^{k'qn} = a^{k'((m,n)-pm)} = a^{k'(m,n)}a^{-k'pm} = a^k\left(a^{-k'p}\right)^m = a^k.$$

So the equation $x^n = a^k$ is solvable. □

The following corollary to this proposition gives us our first concrete result regarding $\mu_n(G)$, for a family of groups G.

Corollary 8. Let $G = C_m a$. Then $\Omega_n(G) = G$ if and only if $(m,n) = 1$. In particular, if $(m,n) = 1$, $\mu_n(C_m) = 1$.

Proof. Suppose $\Omega_n(G) = G$. Then the equation $x^n = a = a^1$ is solvable. By Proposition 7, $(m,n) \mid 1$, i.e. $(m,n) = 1$.

Suppose $(m,n) = 1$. Then the equation $x^n = a^1 = a$ is solvable since $(m,n) = 1 \mid 1$. Let $b \in G$ such that $b^n = a$. Let $a^k \in G$. Then $\left(b^k\right)^n = (b^n)^k = a^k$. Therefore the equation $x^n = a^k$ is solvable for all k, i.e. $\Omega_n(G) = G$. □

Now we will start thinking in terms of mapping a cyclic group into another one. A homomorphism from one cyclic group to another is determined entirely by where the generator of the first group is sent. If we want the homomorphism to be injective, we must ensure that there are no "repeats," i.e. no pairs of elements in the base group that map to the same element in the target group. The next proposition gives the conditions for this precisely.

Proposition 9. If $\phi : C_m a \to C_h b$ is given by $\phi(a) = b^k$, then ϕ is a monomorphism if and only if $m \cdot (h,k) \mid h \mid mk$.

Proof. Suppose ϕ is a monomomorphism. We will show that $m \cdot (h,k) \mid h \mid mk$.

First, note that

$$b^{mk} = (b^k)^m = (\phi(a))^m = \phi(a^m) = \phi(1) = 1,$$

so $h = \text{ord}(b) \mid mk$ (where $\text{ord}(b)$ denotes the order of b, i.e. the smallest $\alpha \in \mathbb{N}$ such that $b^\alpha = 1$).

Since ϕ is injective, we know $\ker\phi = 1$, i.e. if $\phi(a^q) = b^{kq} = 1$, $a^q = 1$. In other words, if $h \mid kq$, then $m \mid q$. Let $q = \frac{h}{(h,k)}$. Then $h \mid h \cdot \frac{k}{(h,k)} = kq$. Therefore $m \mid q$, and so $m \cdot (h,k) \mid q \cdot (h,k) = h$.

Therefore $m \cdot (h,k) \mid h \mid mk$

Now suppose $m \cdot (h,k) \mid h \mid mk$. Let $\phi : C_m a \to C_h b$ be defined by $\phi(a^q) = b^{kq}$. To see that this map is well-defined, suppose $a^{q_1} = a^{q_2} \in G$. Then $q_1 \equiv q_2 (\text{mod}\, m)$, so $m \mid (q_1 - q_2)$, implying

$$h \mid mk \mid k(q_1 - q_2) = (kq_1 - kq_2).$$

So $kq_1 \equiv kq_2 (\text{mod}\, h)$. Therefore

$$\phi(a^{q_1}) = b^{kq_1} = b^{kq_2} = \phi(a^{q_2}).$$

So ϕ is well-defined.

If $a^{q_1}, a^{q_2} \in G$, then

$$\phi(a^{q_1}a^{q_2}) = \phi(a^{q_1+q_2}) = b^{k(q_1+q_2)} = b^{kq_1}b^{kq_2} = \phi(a^{q_1})\phi(a^{q_2}),$$

so ϕ is a homomorphism.

Suppose $\phi(a^q) = b^{kq} = 1$. Then $h \mid kq$, which implies $\frac{h}{(h,k)} \mid \frac{k}{(h,k)}q$. Since $\frac{h}{(h,k)}$ is coprime to $\frac{k}{(h,k)}$, this shows that $\frac{h}{(h,k)} \mid q$. However, since $m \cdot (h,k) \mid h$, we know $m \mid \frac{h}{(h,k)}$. Therefore

$m \mid q$, that is, $a^q = 1$. So ϕ is injective.

Therefore $G \cong \phi(G) \leq H$. □

This proposition completely answers the question of whether a homomorphism from one cyclic group to another is injective. However, when studying n-power extensions of cyclic groups, is it enough to only consider other cyclic groups as potential extensions? The following proposition proves that this is indeed the case.

In a previous paragraph, it was noted that if $(m,n) = 1$, then $\mu_n(C_m) = 1$. The first inclination might be to suppose that $\mu_n(C_m) = (m,n)$ in all cases. However, this is not the case: Consider the group C_2, and suppose $n = 4$. Then $(m,n) = 2$. A cyclic extension of C_2 of order 2 could only be C_4. However, $x^4 = 1$ for all $x \in C_4$. Therefore C_4 cannot possibly be a 4-power extension of C_2. However, C_8 is a 4-power extension of C_2. Essentially, the problem we ran into with C_4 was that there was not enough “room” in C_4 for the 4th powers to take on the structure they needed. Upon reflection, it is logical to suppose that the minimal 8-power extension of C_2 would be C_{16}, the minimal 16-power extension would be C_{32}, and so forth. What about a 3-power extension of C_2? Since $x^3 = x$ for all $x \in C_2$, we see that C_2 is its own 3-power extension, i.e. $\mu_3(C_2) = 1$. In fact we already knew this since $(2,3) = 1$. But what about a 6-power extension? Notice that any 6-power extension of a group is a 2-power extension, so we know $\mu_6(C_2) \neq 1$. However, it can easily be verified that C_4 is a 6-power extension of C_2. So it would seem that the only part of n that has an effect on $\mu_n(C_m)$ is that part that is not coprime to n. The follwing results make these intuitions precise.

Definition 3. For a prime $p \in \mathbb{N}$ and positive integer $n \in \mathbb{N}$, let $v_p(n)$ be the p-adic valuation of n, i.e. $v_p(n) = k$, where $n = p^k m$, $m \in \mathbb{N}$, and $p \nmid m$. Note then that

$$n = \prod_{p \text{ prime}} p^{v_p(n)}.$$

Definition 4. Let $K : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be given by

$$K(m,n) = \prod_{\substack{p \text{ prime} \\ p|m}} p^{v_p(n)}$$

Theorem 10. Consider $C_m a$. Then the smallest group H such that $C_m a$ is n-divisible in H is the cyclic group of order $m \cdot K(m,n)$ with generator b under the inclusion map $a \mapsto b^{K(m,n)}$. In other words, $\mu_n(C_m) = K(m,n)$.

Proof. By Proposition 6, the smallest group H such that $C_m a$ is n-divisible in H must be cyclic, i.e. $H = C_h b$ for some $h \in \mathbb{N} \cup \{\infty\}$ and generator b. Furthermore, the inclusion map from $C_m a$ to H will be given by $a \mapsto b^k$ for some $k \in \mathbb{N}$. If h is finite, then by Proposition 9, we must have $m \cdot (h,k) \mid h \mid mk$. Also, in order for C_m to be n-divisible in H, we must have $(h,n) \mid k$ by Proposition 7. So we wish to find the smallest h such that we can find a k that satisfies these conditions. By rewriting these conditions using the p-adic valuation notation above, the conditions $m \cdot (h,k) \mid h \mid mk$ and $(h,n) \mid k$ become

$$\forall p \text{ prime}, \quad v_p(m) + \min\{v_p(h), v_p(k)\} \leq v_p(h) \leq v_p(m) + v_p(k)$$

$$\text{and} \quad \min\{v_p(h), v_p(n)\} \leq v_p(k).$$

Note that if $v_p(m) = 0$, setting $v_p(h) = v_p(k) = 0$ satisfies both inequalities. If $v_p(m) > 0$, then $v_p(m) + v_p(h) > v_p(h)$. Therefore the first condition implies that we must have $v_p(k) < v_p(h)$ and $v_p(m) + v_p(k) \leq v_p(h) \leq v_p(m) + v_p(k)$, i.e. $v_p(h) = v_p(m) + v_p(k)$. This also implies that $v_p(h) > v_p(k)$, so the second condition requires that $v_p(n) \leq v_p(k)$. Therefore the smallest possible value of $v_p(k)$ is $v_p(n)$.

In summary, we have that

$$v_p(k) = \begin{cases} 0 & v_p(m) = 0 \\ v_p(n) & v_p(m) > 0 \end{cases},$$

and so

$$k = \prod_{p \text{ prime}} p^{v_p(k)} = \prod_{\substack{p \text{ prime} \\ p|m}} p^{v_p(n)} = K(m,n).$$

Similarly, we have

$$v_p(h) = \begin{cases} 0 & v_p(m) = 0 \\ v_p(m) + v_p(n) & v_p(m) > 0 \end{cases},$$

yielding

$$h = \prod_{p \text{ prime}} p^{v_p(h)} = \prod_{\substack{p \text{ prime} \\ p|m}} p^{v_p(m)+v_p(n)} = \prod_{\substack{p \text{ prime} \\ p|m}} p^{v_p(m)} \cdot \prod_{\substack{p \text{ prime} \\ p|m}} p^{v_p(n)} = m \cdot K(m,n).$$

This completes the proof. □

This theorem gives a complete description of $\mu_n(C_m)$ for all $m, n \in \mathbb{N}$.

3.2 Infinite Cyclic Groups

The case of infinite cyclic groups is somewhat simpler. Since an infinite group can only embed into an infinite group, the natural group to embed C_∞ into is C_∞ itself. This turns out to be the case, and the natural monomorphsim $C_\infty a \to C_\infty b$ given by $a \mapsto b^n$ turns out to be the best possible mapping in terms of minimizing the index of the image of the map.

Proposition 11. $\mu_n(C_\infty) = n$.

Proof. By Proposition 6, the smallest n-power extension of $C_\infty a$ is the infinite cylic group $C_\infty b$. Suppose $f : C_\infty a \hookrightarrow_n C_\infty b$. Notice that $\Omega_n(C_\infty b) = \{b^{kn} \mid k \in \mathbb{Z}\}$. Then since

$f(C_\infty a) \subseteq \Omega_n(C_\infty b)$, we have that $[C_\infty b : f(C_\infty a)] \geq [C_\infty b : \Omega_n(C_\infty b)] = n$. However, if it is the case that $f(a) = b^n$, then $f(C_\infty a) = \Omega_n(C_\infty b)$. Therefore $\mu_n(C_\infty) = n$. □

We now have our final piece of information regarding cyclic groups. In the next section we will use this proposition to give bounds on $\mu_n(G)$ for all finitely generated Abelian groups G and positive integers n.

4 Direct Products

If G is a direct or semidirect product, there is a natural type of embedding that respects the factors of the products.

Definition 5. If G is a direct or semidirect product with factors A and B, and H is a direct or semidirect product with factors J and K, then H is called a *factorable n-power extension* of G if there exists $h : G \hookrightarrow_n H$ such that $h(A) \subseteq J$ and $h(B) \subseteq K$. In the case that G and H are semidirect products, we require that the normal factor maps into the normal factor.

Notice that in this case h can be "factored" into two functions $f : A \to J$ and $g : B \to K$ such that $f = h|_A$ and $g = h|_B$. In the case of direct products, the existence of a factorable n-embedding is easily shown. However, in the case of semidirect products, the question is not as easily answered. We are sometimes interested only in $[H : h(G)]$ for factorable n-power extensions H of G.

Definition 6. If G is a direct or semidirect product, then let

$$\mu_n^F(G) = \min_{f,H} \{[H : f(G)] \mid f : G \hookrightarrow_n H \text{ and } f \text{ is factorable}\}.$$

Note that $\mu_n^F(G)$ is only defined for groups G that have factorable n-power extensions. Our first Lemma involving this new function is obvious:

Lemma 12. If G has a factorable n-power extension, then $\mu_n^F(G) \geq \mu_n(G)$.

The direct product is a tool by which many groups can be described. In particular, finitely generated Abelian groups can be expressed as direct products of cyclic groups, which we examined in detail in the last section.

Our first theorems tell us that we may obtain bounds on $\mu_n(G \times H)$ if we know $\mu_n(G)$ and $\mu_n(H)$.

Proposition 13. If $f : A \hookrightarrow_n H$ and $g : B \hookrightarrow_n J$, then $(f,g) : A \times B \hookrightarrow_n H \times J$.

Proof. Let $h = (f,g) : A \times B \to H \times J$. Then since f and g are monomorphisms, h is a monomorphism. Further, let $(a,b) \in A \times B$. Then by assumption, $\exists x \in H$, $y \in J$ such that $x^n = f(a)$ and $y^n = g(b)$. So

$$h(a,b) = (f(a),g(b)) = (x^n,y^n) = (x,y)^n.$$

Therefore $h : A \times B \hookrightarrow_n H \times J$. □

Corollary 14. Any direct product has a factorable n-power extension.

Proof. Let $G = A \times B$ be a direct product. By Proposition 2, A and B have n-power extensions H and J with n-embeddings $f : A \hookrightarrow_n H$ and $g : B \hookrightarrow_n J$. By Proposition 13, $(f,g) : A \times B = G \hookrightarrow_n H \times J$. By construction, (f,g) is a factorable n-embedding of G □

The following corollary gives an upper bound on $\mu_n(A \times B)$ by calculating $\mu_n^F(A \times B)$, assuming we know $\mu_n(A)$ and $\mu_n(B)$.

Corollary 15. $\mu_n^F(A \times B) = \mu_n(A) \cdot \mu_n(B)$.

Proof. Suppose $h : A \times B \hookrightarrow_n H \times J$ is a factorable n-embedding for some groups H and J such that $[H \times J : h(A \times B)] = \mu_n^F(A \times B)$. Then $h = (f,g)$ for some monomorphisms $f : A \to H$ and $g : B \to J$. Let $a \in A$, and choose $(h,j) \in H \times J$ such that $(h,j)^n = h(a,1)$. Then $(h^n, j^n) = (f(a),1)$, so $h^n = f(a)$. Therefore $f : A \hookrightarrow_n H$. Similarly, $g : B \hookrightarrow_n J$. Notice that

$$[H \times J : h(A \times B)] = [H \times J : f(A) \times g(B)] = [H : f(A)] \cdot [J : g(B)] \geq \mu_n(A) \cdot \mu_n(B).$$

However, if we choose H', J' and f', g' so that $f' : A \hookrightarrow_n H'$ and $g' : B \hookrightarrow_n J$ and further that $[H' : f'(A)] = \mu_n(A)$ and $[J' : g'(B)] = \mu_n(B)$, then $h' = (f', g')$ is an n-embedding of $A \times B$

into $H' \times J'$ and

$$[H' \times J' : h'(A \times B)] = [H' : f'(A)] \cdot [J' : g'(B)] = \mu_n(A) \cdot \mu_n(B).$$

Therefore $\mu_n^F(A \times B) = \mu_n(A) \cdot \mu_n(B)$.

□

We can find a lower bound on $\mu_n(A \times B)$ by noting that any n-embedding of $A \times B$ into H is also an n-embedding of A and B individually into H.

Proposition 16. $\mu_n(A \times B) \geq \max\left(\frac{\mu_n(A)}{|B|}, \frac{\mu_n(B)}{|A|}\right)$.

Proof. If $\mu_n(A \times B)$ is infinite, the statement holds. So suppose $f : A \times B \hookrightarrow_n H$ and

$$[H : f(A \times B)] = \mu_n(A \times B) < \infty.$$

Further suppose that B has finite order. Then $f|_A$ is an n-embedding of A into H. Therefore, since $\mathrm{Im}(f_A) = f(A \times \{1\})$, we must have that $[H : A \times \{1\}] \geq \mu_n(A)$. However, we must also have that $[H : f(A \times B)] = [H : f(A \times \{1\})]/|B|$, since for every coset of $f(A \times B)$ in H, there will be $|B|$ cosets of $f(A \times \{1\})$ in H, namely those cosets which differ by an element of $f(B)$. Therefore

$$\mu_n(A \times B) = [H : f(A \times B)] = \frac{[H : f(A \times 1)]}{|B|} \geq \frac{\mu_n(A)}{|B|}.$$

A symmetric argument holds and shows that $\mu_n(A \times B) \geq \frac{\mu_n(B)}{|A|}$ if A is finite.

If both A and B have infinite order, then the statement of the proposition simply says that $\mu_n(A \times B) \geq 0$, which we already know since $\mu_n(A \times B) \geq 1$ by Lemma 1. □

We end this section with an application of our theorems to the case of finitely generated Abelian groups.

Corollary 17. Let G be a finitely generated Abelian group, and let $G = C_\infty^r \times C_{p_1^{\alpha_1}} \times \cdots \times C_{p_m^{\alpha_m}}$ be the elementary divisor decomposition of G. Then

$$\mu_n(G) \leq n^r \cdot \prod_{i=1}^{m} p_i^{v_{p_i}(n)},$$

where $v_{p_i}(n)$ is the p_i-adic valuation of n, as per Definition 3.

Proof. The result follows from repeated applications of Corollary 15 as follows: Note that $\mu_n(C_\infty \times C_\infty) = \mu_n(C_\infty) \cdot \mu_n(C_\infty) = n^2$. Suppose that $\mu_n\left(C_\infty^k\right) \leq n^k$ for some $k \in \mathbb{N}$. Then

$$\mu_n\left(C_\infty^{k+1}\right) = \mu_n\left(C_\infty^k \times C_\infty\right) \leq \mu_n\left(C_\infty^k\right) \cdot \mu_n(C_\infty) \leq n^k \cdot n = n^{k+1},$$

so by induction, $\mu_n(C_\infty^r) \leq n^r$.

Similarly, $\mu_n\left(C_{p_1^{\alpha_1}}\right) = K(p_1^{\alpha_1}, n) = p_1^{v_{p_1}(n)}$, and by induction we can show that

$$\mu_n\left(C_{p_1^{\alpha_1}} \times \cdots \times C_{p_m^{\alpha_m}}\right) \leq \prod_{i=1}^{m} p_i^{v_{p_i}(n)}.$$

Combining these two results using Corollary 15 yields the desired result. □

5 Semidirect Products

We now generalize slightly and consider the problem of finding factorable n-power extensions of a semidirect product. Suppose A and B are groups and let $\phi : B \to \operatorname{Aut}(A)$ be a homomorphism. We wish to know under what conditions we can find groups H and J, functions $f : A \to H$, $g : B \to J$ and a homomorphsim $\psi : J \to \operatorname{Aut}(H)$ such that $(f,g) : A \rtimes_{\phi} B \hookrightarrow_{n} H \rtimes_{\psi} J$. We begin by seeing whether the function (f,g) can even be constructed so that it is a monomorphism. Note that this immeditately requires that f and g be each monomorphic.

Proposition 18. Suppose A, B, H, and J are groups, $f : A \to H$ and $g : B \to J$ are monomorphisms, and $\phi : B \to \operatorname{Aut}(A)$ and $\psi : J \to \operatorname{Aut}(H)$ are homomorphisms. Then $(f,g) : A \rtimes_{\phi} B \to H \rtimes_{\psi} J$ is a monomorphism if and only if for all $a \in A$, $b \in B$, $\psi_{g(b)}\big(f(a)\big) = f\big(\phi_b(a)\big)$.

Proof. Let $h = (f,g) : A \rtimes_{\phi} B \to H \rtimes_{\psi} J$.

Suppose h is a monomorphism. Then for all $a \in A$, $b \in B$,

$$h\big((1,b)(a,1)\big) = h\big(\phi_b(a), b\big) = \Big(f\big(\phi_b(a)\big), g(b)\Big)$$

and

$$h(1,b)h(a,1) = \big(1, g(b)\big)\big(f(a), 1\big) = \Big(\psi_{g(b)}\big(f(a)\big), g(b)\Big).$$

Since h is a homomorphism, these two pairs are equal, and so we must have that

$$\psi_{g(b)}\big(f(a)\big) = f\big(\phi_b(a)\big).$$

Now suppose that for every $a \in A$, $b \in B$, we have $\psi_{g(b)}\big(f(a)\big) = f\big(\phi_b(a)\big)$. Suppose

$(a,b),(c,d) \in A \rtimes_\phi B$. Then

$$\begin{aligned}
h\big((a,b)(c,d)\big) &= h\big(a\phi_b(c),bd\big) \\
&= \Big(f\big(a\phi_b(c)\big),g(bd)\Big) \\
&= \Big(f(a)f\big(\phi_b(c)\big),g(b)g(d)\Big) \\
&= \Big(f(a)\psi_{g(b)}\big(f(c)\big),g(b)g(d)\Big) \\
&= \big(f(a),g(b)\big)\big(f(c),g(d)\big) \\
&= h(a,b)h(c,d).
\end{aligned}$$

So h is a homomorphism. Since f and g are injective, h is injective. So h is a monomorphism. □

We now begin to discuss the possibility of $(f,g) : A \rtimes_\phi B \hookrightarrow_n H \rtimes_\psi J$. The primary problem that arises when dealing with semidirect products as opposed to direct products is that raising a pair $(x,y) \in H \rtimes_\psi J$ to the nth power does not behave nicely in the first coordinate. Even if it happens to be the case that $f : A \hookrightarrow_n H$, this is usually not sufficient (or even necessary) for $H \rtimes_\psi J$ to be an n-power extension of $A \rtimes_\phi B$. However, the fact that we are raising (x,y) to a power and not, say, multiplying it by various other pairs, allows us to describe our results in a somewhat simpler fashion. The next notation is a convenience that will help to make the following computations more comprehendable. It describes the action of multiplication in a semidirect product in a compact way.

Definition 7. For a given semidirect product $H \rtimes_\psi J$, $h,x \in H$ and $j \in J$, let

$$\lambda_{h,j}\,(\,x\,) \;=\; h\,\psi_j\,(\,x\,).$$

Then notice that for $(h,j),(h',j') \in H \rtimes_\psi J$, $(h,j)(h',j') = \big(\lambda_{h,j}(h'),jj'\big)$.

Further, for $j \in J$, $h \in H$ and $n \in \mathbb{N}$, let

$$\Lambda_n(h,j) = \lambda_{h,j}^n(1) = \underbrace{h\psi_j\Big(h\psi_j\big(\cdots h\psi_j(h)}_{n\,h'\text{s}}\cdots\big)\Big).$$

Note that $\lambda_{h,j}(\Lambda_n(h,j)) = \Lambda_{n+1}(h,j)$.

Lemma 19. If $(x,y) \in H \rtimes_\psi J$, then $(x,y)^n = (\Lambda_n(x,y), y^n)$.

Proof. We prove by induction on n.

Base Case: Suppose $n = 1$. Then since

$$\Lambda_1(x,y) = \lambda_{x,y}(1) = x\psi_y(1) = x1 = x$$

and $y^1 = y$, we have $(x,y)^1 = (x,y) = \big(\Lambda_n(x,y), y^1\big)$.

Inductive step: Suppose $(x,y)^k = \big(\Lambda_k(x,y), y^k\big)$ for some $k \in \mathbb{N}$. Then

$$\begin{aligned} (x,y)^{k+1} &= (x,y)(x,y)^k \\ &= (x,y)\Big(\Lambda_k(x,y), y^k\Big) \\ &= \Big(\lambda_{x,y}\big(\Lambda_k(x,y)\big), y^{k+1}\Big) \\ &= \Big(\Lambda_{k+1}(x,y), y^{k+1}\Big). \end{aligned}$$

So the inductive step is proved. □

Corollary 20. $(h,j)^n = (x,y)$ if and only if $j^n = y$ and $\Lambda_n(h,j) = x$.

The problem of finding a factorable n-power extensions of $A \rtimes_\phi B$ has therefore been restated as finding H, J, $f : A \to H$, $g : B \to J$, and ψ such that for all $(a,b) \in A \rtimes_\phi B$, we can find $(h,j) \in H \rtimes_\psi J$ such that $f(a) = \Lambda_n(h,j)$ and $g(b) = j^n$. Note that this requires that $g : B \hookrightarrow_n J$. This problem is nontrivial in general, and we will find that even in the simplest case, when A and B are both cyclic groups, such an extension may not exist.

6 Semidirect Products of Finite Cyclic Groups

We now restrict our attention to the case where we begin with a group $G = C_{m_1}a \rtimes_{\phi} C_{m_2}b$ and with to n-embed it into a group $H = C_{\ell_1}c \rtimes_{\psi} C_{\ell_2}d$. The cyclic nature of the groups involved will allow us to express the conditions for n-embedding in number-theoretic terms.

We wish to construct functions $f : C_{m_1} \to C_{\ell_1}$ and $g : C_{m_2} \to C_{\ell_2}$ such that f and g are monomorphisms. Let $r \in \{1, \ldots, \ell_1 - 1\}$ and $s \in \{1 \ldots, \ell_2 - 2\}$ so that $f(a) = c^r$ and $g(b) = d^s$. By Proposition 9, we must have that $m_1 \cdot (\ell_1, r) \mid \ell_1 \mid m_1 f$ and $m_2 \cdot (\ell_2, s) \mid \ell_2 \mid m_2 s$.

We need to construct the homomorphism $\psi : C_{\ell_2} \to \operatorname{Aut}(C_{\ell_1})$. Note that ψ is determined entirely by $\psi_d(c)$: Suppose $\phi_d(c) = c^e$ for some $e \in 1, 2 \ldots, \ell_1 - 1$. If $j, k \in \mathbb{Z}$, then

$$\psi_d(c^j) = (\psi_d(c))^j = (c^e)^j = c^{je}$$

$$\psi_{d^k}(c) = \psi_d \cdots \psi_d \psi_d \psi_d(c) = \psi_d \cdots \psi_d \psi_d (c^e) = \psi_d \cdots \psi_d \left(c^{e^2}\right) = \cdots = c^{e^k},$$

and so

$$\psi_{d^k}(c^j) = (\psi_{d^k}(c))^j = \left(c^{e^k}\right)^j = c^{je^k}.$$

So in order to determine ψ we need to choose e. In order for the funtion $c \to c^e$ to be an automorphism, we must have that $(e, \ell_1) = 1$. In order for the function ψ to be a homomorphism, we need $\psi_{d^{\ell_2}} = id_{C_{\ell_1}}$. Therefore we need

$$c^{e^{\ell_2}} = \psi_{d^{\ell_2}}(c) = id_{C_{\ell_1}}(c) = c,$$

that is, we need $e^{\ell_2} \equiv 1 (\operatorname{mod} \ell_1)$.

Similarly, if we let $h \in \{1, 2 \ldots, m_1 - 1\}$ so that $\phi_b(a) = a^h$, through an identical computation we find that $\phi_{b^k}(a^j) = a^{jh^k}$, $(h, m_1) = 1$, and $h^{m_2} \equiv 1 (\operatorname{mod} m_1)$.

Proposition 18 tells us that we need $\psi_{g(y)}\big(f(x)\big) = f\big(\phi_y(x)\big)$ for all $x \in C_{m_1}$, $y \in C_{m_2}$. Because all our functions are homomorphisms and our groups are cyclic, we need only confirm this in the case of generators, i.e. we need $\psi_{g(b)}\big(f(a)\big) = f\big(\phi_b(a)\big)$. But since we have formulae for these functions, we can be more explicit:

$$\psi_{g(b)}\big(f(a)\big) = \psi_{d^s}\left(c^r\right) = c^{re^s}$$

$$f\big(\phi_b(a)\big) = f\left(a^h\right) = c^{rh}.$$

So this condition reduces to the congruence $rh \equiv re^s (\mathrm{mod}\ \ell_1)$.

Now we consider the problem of n-divisibility. Let $(a^j, b^k) \in C_{m_1} \rtimes_\phi C_{m_2}$. Then

$$(f,g)(a^j, b^k) = (c^{rj}, d^{sk}).$$

By Corollary 20, this is equal to $(x,y)^n$ for some $(x,y) \in C_{\ell_1} \rtimes_\psi C_{\ell_2}$ if and only if $y^n = d^{sk}$ and $\Lambda_n(x,y) = c^{rj}$. The first condition is clearly satisfied if and only if the equation $y^n = d^s$ is solvable. By Proposition 7, this occurs exactly when $(\ell_2, n) \mid s$.

Assuming we have such a condition, i.e. $y^n = d^{ks}$ is solvable for any $k \in \mathbb{Z}$, let us turn to solving the equation $\Lambda_n(x,y) = c^{rj}$. We must have that $y = d^q$ for some $q \in \{0, 1, \ldots, \ell_2 - 1\}$. Therefore for any $z \in C_{\ell_1}$,

$$\lambda_{x,y}(z) = x\psi_y(z) = x\psi_{d^q}(z) = xz^{e^q}.$$

Hence,

$$\begin{array}{rcl}
\Lambda_1(x,y) & = & \lambda_{x,y}(1) = x, \\
\Lambda_2(x,y) & = & \lambda_{(}x,y)(x) = xx^{e^q} = x^{e^q+1}, \\
\Lambda_3(x,y) & = & \lambda_{(}x,y)\left(x^{e^q+1}\right) = xx^{e^{2q}+e^q} = x^{e^{2q}+e^q+1}, \\
\vdots & \vdots & \vdots \\
\Lambda_n(x,y) & = & x^{e^{(n-1)q}+e^{(n-2)q}+\cdots e^q+1}.
\end{array}$$

For the sake of notation, let

$$Q_n(z) = \sum_{i=0}^{n-1} z^i = \begin{cases} n; & z = 1 \\ (z^n - 1)/(z-1); & z \neq 1 \end{cases}.$$

Then $\Lambda_n(x,y) = x^{Q_n(e^q)}$. We wish for this expression to be equal to c^{rj}. Since $x \in C_{\ell_1}$, $x = c^t$ for some $t \in \{0, 1 \ldots, \ell_1 - 1\}$. So we want to find t such that $c^{tQ_n(e^q)} = c^{rj}$, that is, $tQ_n(e^q) \equiv rj (\text{mod } \ell_1)$. This is solvable exactly when $(Q_n(e^q), \ell_1) \mid rj$. So we want $(Q_n(e^q), \ell_1) \mid rj$ for all $j \in \{0, 1, \ldots, m_1\}$. Clearly this is equivalent to simply $(Q_n(e^q), \ell_1) \mid r$.

Hence, what we need is for every $k \in \{0, 1, \ldots, m_2 - 1\}$, there to exist some $q \in \{0, 1, \ldots, \ell_2 - 1\}$ with $qn \equiv sk (\text{mod } \ell_2)$ (so that $(d^q)^n = d^{sk}$), such that $(Q_n(e^q), \ell_1) \mid r$ (so that for some t, $\Lambda_n(c^t, d^q) = c^{rj}$).

All the previous discussion leads us to the following theorem:

Theorem 21. Suppose we are given positive integers m_1, m_2, h and n with $(h, m_1) = 1$ and $h^{m_2} \equiv 1 (\text{mod } m_1)$ and a homomorphism $\phi : C_{m_2} \longrightarrow \text{Aut}(C_{m_1})$ given by $\phi_b(a) = a^h$. If we choose positive integers ℓ_1, ℓ_2, construct functions $f : C_{m_1}a \longrightarrow C_{\ell_1}c$ and $g : C_{m_2}b \longrightarrow C_{\ell_2}d$ by $f(a) = c^r$ and $g(b) = d^s$, where r and s are positive integers, and construct a function $\psi : C_{\ell_2} \longrightarrow \text{Aut}(C_{\ell_1})$ by $\psi_d(c) = c^e$, then $(f, g) : C_{m_1} \rtimes_\phi C_{m_2} \hookrightarrow_n C_{\ell_1} \rtimes_\psi C_{\ell_2}$ if and only if

1. $m_1 \cdot (\ell_1, r) \mid \ell_1 \mid m_1 r$

2. $m_2 \cdot (\ell_2, s) \mid \ell_2 \mid m_2 s$

3. $(e, \ell_1) = 1$

4. $e^{\ell_2} \equiv 1 (\text{mod } \ell_1)$

5. $rh \equiv re^s (\text{mod } \ell_1)$

6. $(\ell_2, n) \mid s$

7. For all $k \in \{0,1,\dots,m_2-1\}$, there exists $q \in \{0,1,\dots,\ell_2-1\}$ such that $qn \equiv sk (\operatorname{mod} \ell_2)$ and $(Q_n(e^q),\ell_1) \mid r$.

Proof. The only if part of the theorem comes directly from the argument above.

Now suppose that we are given positive integers m_1, m_2, h, and n with $(h,m_1)=1$ and $h^{m_2} \equiv 1 (\operatorname{mod} m_1)$ and a homomorphism $\phi : C_{m_2}b \longrightarrow \operatorname{Aut}(C_{m_1}a)$ given by $\phi_b(a) = a^h$, and that we can find ℓ_1, ℓ_2, e, r, s satisfying conditions 1-7. If $f : C_{m_1}a \longrightarrow C_{\ell_1}c$ and $g : C_{m_2}b \longrightarrow C_{\ell_2}d$ are given by $f(a) = c^r$ and $g(b) = d^s$ and $\psi : C_{\ell_2}d \longrightarrow \operatorname{Aut}(C_{\ell_2}c)$ is given by $\psi_d(c) = c^e$, then $(f,g) : C_{m_1} \rtimes_\phi C_{m_2} \hookrightarrow_n C_{\ell_1} \rtimes_\psi C_{\ell_2}$: Conditions 1 and 2 ensure that f and g are monomorphisms. That, combined with condition 5, shows that (f,g) is a monomorphism. Condition 3 implies that ψ does actually map into $\operatorname{Aut}(C_{\ell_1})$, while condition 4 shows ψ is a homomorphism. Condition 6 shows that the equation $(d^q)^n = g(b^k) = d^{sk}$ can always be solved in C_{ℓ_2}, while condition 7 says that for any $a^j \in C_{m_1}$, $b^k \in C_{m_2}$, we can always find some q and t such that $(d^q)^n = g(b^k)$ and $c^{tQ_n(e^q)} = f(a^j) = a^{jr}$. But this exactly means that $(c^t, d^q)^n = \big(f(a^j), g(b^k)\big)$. So $(f,g) : C_{m_1} \rtimes_\phi C_{m_2} \hookrightarrow_n C_{\ell_1} \rtimes_\psi C_{\ell_2}$. □

The conditions in Theorem 21 can be simplified somewhat to allow for easier computation. The first two conditions imply that $m_1 \mid \ell_1$ and $m_2 \mid \ell_2$. Choose μ_1, μ_2 such that $\ell_1 = m_1\mu_1$ and $\ell_2 = m_2\mu_2$. Then the first condtion becomes $m_1 \cdot (m_1\mu_1, r) \mid m_1\mu_1 \mid m_1 r$, which can now be simplified to $(m_1\mu_1, r) \mid \mu_1 \mid r$. Since $\mu_1 \mid r$, let $r = \mu_1\eta_1$. Then the second division in the condition is clear, so we are left with the first division, which now says $(m_1\mu_1, \mu_1\eta_1) \mid \mu_1$. But since $\mu_1 \mid (m_1\mu_1, \mu_1\eta_1)$, we have $(m_1\mu_1, \mu_1\eta_1) = \mu_1$. This is true exacly when $(m_1, \eta_1) = 1$. Similarly, if we let $s = \mu_2\eta_2$. we can reduce the second condition to $(m_2, \eta_2) = 1$.

The third condition can now be rewritten as $(e, m_1\mu_1) = 1$. This is clearly equivalent to the two separate conditions $(e, m_1) = 1$ and $(e, \mu_1) = 1$.

The fourth condition does not simplify: we merely rewrite it as $e^{m_2\mu_2} \equiv 1 (\operatorname{mod} m_1\mu_1)$.

The fifth condition becomes $\mu_1\eta_1 h \equiv \mu_1\eta_1 e^{\mu_2\eta_2} (\operatorname{mod} m_1\mu_1)$. Reducing the μ_1 yields

$\eta_1 h \equiv \eta_1 e^{\mu_2\eta_2} (\bmod m_1)$. From the reduced first condition we know $(m_1, \eta_1) = 1$, so cancelling the η_1s gives $h \equiv e^{\mu_2\eta_2} (\bmod m_1)$.

The sixth condition we rewrite as $(m_2\mu_2, n) \mid \mu_2\eta_2$.

The seventh condition we rewrite as follows: For all $k \in \{0, 1, \ldots, m_2 - 1\}$, there exists $q \in \{0, 1, \ldots, m_2\mu_2 - 1\}$ such that $qn \equiv \mu_2\eta_2 k (\bmod m_2\mu_2)$ and $(Q_n(e^q), m_1\mu_1) \mid \mu_1\eta_1$.

Notice that because of the way that we have defined μ_1 and μ_2, if we can find positive integers satisfying these conditions, then we find a factorable n-power extension of order $\mu_1 \cdot \mu_2$. Summarizing, we have

Corollary 22. A group $C_{m_1}a \rtimes_\phi C_{m_2}b$, with $\phi_b(a) = a^h$, has a factorable n-power extension if and only if there exist positive integers $\mu_1, \mu_2, \eta_1\eta_2, e$ such that

1. $(m_1, \eta_1) = 1$
2. $(m_2, \eta_2) = 1$
3. $(e, m_1) = 1$
4. $(e, \mu_1) = 1$
5. $e^{m_2\mu_2} \equiv 1 (\bmod m_1\mu_1)$
6. $h \equiv e^{\mu_2\eta_2} (\bmod m_1)$
7. $(m_2\mu_2, n) \mid \mu_2\eta_2$
8. For all $k \in \{0, 1, \ldots, m_2 - 1\}$, there exists $q \in \{0, 1, \ldots, m_2\mu_2 - 1\}$ such that $qn \equiv \mu_2\eta_2 k (\bmod m_2\mu_2)$ and $(Q_n(e^q), m_1\mu_1) \mid \mu_1\eta_1$.

These conditions can be used to find factorable n-power extensions of this type of semidirect product or to prove that none exist.

6.1 Eliminating Possibilities

Suppose we wish show that for a particular 4-tuple (m_1, m_2, h, n) a factorable n-power extension of $C_{m_1}a \rtimes_\phi C_{m_2}b$, with $\phi_b(a) = a^h$, does not exist. Note that then we need $h \neq 1$, for if $h = 1$, then we have a direct product, and as was shown in the previous section, direct products always have factorable n-power extensions.

Consider the most commonly encountered semidirect product in elementary abstract algebra: the dihedral group D_m on m vertices. Recall that $D_m \cong C_m a \rtimes_\phi C_2 b$, where $\phi_b(a) = a^{-1}$. For example, consider $D_4 = C_4 a \rtimes_\phi C_2 b$, and suppose $n = 2$. There exists a factorable n-extension of D_m if and only if we can find numbers $\mu_1, \mu_2, \eta_1, \eta_2, e$ such that the above 8 conditions hold, with $(m_1, m_2, h, n) = (4, 2, -1, 2)$.

From condition 2 we have that $(2, \eta_2) = 1$, implying η_2 is odd. However, condition 7 implies that $(2\mu_2, 2) = 2 \mid \mu_2\eta_2$. Then we must have $2 \mid \mu_2$. So then condition 6 gives that

$$-1 \equiv e^{\mu_2\eta_2} = \left(e^{\frac{\mu_2\eta_2}{2}}\right)^2 \pmod{4}.$$

So we have that -1 is a square modulo 4, a contradiction. Therefore there exist no $\mu_1, \mu_2, \eta_1, \eta_2, e$ making conditions 1-8 hold. Therefore D_4 has no factorable n-power extension.

This argument is generalized to all semidirect products in the following proposition.

Proposition 23. Let $k = (m_2, n)$. If there exists a factorable n-power extension of $C_{m_1}a \rtimes_\phi C_{m_2}b$ with $\phi_b(a) = a^h$, then h has a kth root modulo m_1.

Proof. Note that $k = (m_2, n) \mid (m_2\mu_2, n) \mid \mu_2\eta_2$ by condition 7, so by condition 6, $h \equiv \left(e^{\frac{\mu_2\eta_2}{(m_2,n)}}\right)^{(m_2,n)} \pmod{m_1}$. So h has a kth root modulo m_1, namely $e^{\frac{\mu_2\eta_2}{(m_2,n)}}$. □

6.2 Finding Factorable n-power Extensions

The fact that Theorem 21 is an if and only if statement allows us to use its conditions to find factorable n-power extensions of semidirect products. Furthermore, the simple nature of the conditions allows them to be programmed into a computer. The relationship between the simplified variables μ_1, μ_2, η_1, η_2, e and the "natural" variables ℓ_1, ℓ_2, r, s, e are given here for reference (note that m_1 and m_2 are as before):

- $\ell_1 = m_1\mu_1$
- $\ell_2 = m_2\mu_2$
- $r = \mu_1\eta_1$
- $s = \mu_2\eta_2$

We note some relationships between the elements $\mu_1, \mu_2, \eta_1, \eta_2, e$ that can assist when writing an algorithm for finding factorable n-power extensions. Notice that since $b^r = b^{\mu_1\eta_1}$is the image of the generator of $C_{m_1}a$ in $C_{\ell_1}c$ under the function f, we can require that $\mu_1\eta_1 < \ell_1 = m_1\mu_1$. Therefore $1 \le \eta_1 < m_1$. Similarly, $1 \le \eta_2 < m_2$. Futhermore, since $\psi_d(c) = c^e \in C_{\ell_1}$, we can require that $1 \le e < \ell_1 = m_1\mu_1$. So for a fixed μ_1, μ_2, there are only a finite number of possible triples (η_1, η_2, e) that might give rise to distinct extensions of $C_{m_1} \rtimes_\phi C_{m_2}$. To be precise, given μ_1, μ_2, there are at most $(m_1 - 1)(m_2 - 1)(m_1\mu_1 - 1)$ triples to check. Note that this number does not depend on μ_2.

Furthermore, note that the order of the extension represented by the 5-tuple $(\mu_1, \mu_2, \eta_1, \eta_2, e)$ is $\mu_1\mu_2$. This now gives us a way of algorithmically finding $\mu_n^F\left(C_{m_1} \rtimes_\phi C_{m_2}\right)$, assuming it exists. First, find one 5-tuple $(\mu_1^*, \mu_2^*, \eta_1^*, \eta_2^*, e^*)$ satisfying the conditions of Corollary 22. Now there are a finite number of pairs (μ_1, μ_2) such that $\mu_1\mu_2 < \mu_1^*\mu_2^*$. If any of these pairs (μ_1, μ_2) have a triple (η_2, η_2, e) such that the five variable together satisfy the conditions in Theorem 22, then they correspond to an n-extension of

$C_{m_1} \rtimes_\phi C_{m_2}$ of smaller oder. We can repeat the process until we find a pair (μ_1,μ_2) that is minimal. Summarizing, we give the outline of an algorithm that could be used by a computer to find these extensions. At this time, we do not have a convenient limit on the sizes of μ_1 and μ_2 as a function of m_1, m_2, h, and n. However, it seems likely that one exists.

The Cyclic Semidirect *n*-power Extension Algorithm

1. Begin with positive integers m_1, m_2, h, and n. Choose a limit M for the value of $\mu_1\mu_2$. Set $\mu_1 = \mu_2 = 1$ and $M^* = M$.

2. Check the $(m_1-1)(m_2-1)(m_1\mu_1-1)$ triples (η_1,η_2,e) with $1 \leq \eta_1 < m_1$, $1 \leq \eta_2 < m_2$, and $1 \leq e < m_1\mu_1$ to see if any of the 5-tuples $(\mu_1,\mu_2,\eta_1,\eta_2,e)$ satisfy the conditions of Theorem 22. If so, set $M^* = \mu_1\mu_2$.

3. Check the next potential value of $\mu_1\mu_2$ to see what to check next.

   If $(\mu_1+1)\mu_2 < M^*$, increase μ_1 by 1 and go to step 1

   Otherwise, if $\mu_2+1 < M^*$, set $\mu_1 = 1$, increase μ_2 by 1, and go to step 1

   If $\mu_2+1 \geq M^*$, we're done. We've either found a minimal n-power extension of $C_{m_1} \rtimes_\phi C_{m_2}$ or we've determined that no factorable extension with order less than M exists.

6.3 The Dihedral Groups

We now attempt to give an complete a description as we can of $\mu_n^F(D_m)$ for D_m the dihedral group of order $2m$. Note that $D_m = C_m a \rtimes_\phi C_2 b$, where $\phi(b) = a^{-1}$. So we wish to know for what values of m and n can a 5-tuple $(\mu_1,\mu_2,\eta_1,\eta_2,e)$ be found such that these values satisfy the eight conditions with $(m_1,m_2,h,n) = (m,2,-1,n)$. Substituting these values into the eight conditions of Theorem 22, we have

1. $(m,\eta_1) = 1$

2. $(2, \eta_2) = 1$

3. $(e, m) = 1$

4. $(e, \mu_1) = 1$

5. $e^{2\mu_2} \equiv 1 (\bmod m\mu_1)$

6. $-1 \equiv e^{\mu_2 \eta_2} (\bmod m)$

7. $(2\mu_2, n) \mid \mu_2 \eta_2$

8. For all $k \in \{0, 1\}$, there exists $q \in \{0, 1, \ldots, 2\mu_2 - 1\}$ such that $qn \equiv \mu_2 \eta_2 k (\bmod 2\mu_2)$ and $(Q_n(e^q), m\mu_1) \mid \mu_1 \eta_1$.

Further, notice that from the discussion above we have the conditions

- $1 \leq \eta_1 < m$
- $1 \leq \eta_2 < 2$
- $1 \leq e < m\mu_1$

The second condition above implies that $\eta_2 = 1$, allowing us to eliminate condition 2 (since it is automatically satisfied) and simplify conditions 6, 7, and 8. The simplified conditions are now

- I) $(m, \eta_1) = 1$
- II) $(e, m) = 1$
- III) $(e, \mu_1) = 1$
- IV) $e^{2\mu_2} \equiv 1 (\bmod m\mu_1)$
- V) $-1 \equiv e^{\mu_2} (\bmod m)$

- VI) $(2\mu_2, n) \mid \mu_2$
- VII) For all $k \in \{0,1\}$, there exists $q \in \{0,1,\ldots,2\mu_2 - 1\}$ such that $qn \equiv \mu_2 k (\bmod 2\mu_2)$ and $(Q_n(e^q), m\mu_1) \mid \mu_1\eta_1$.

Proposition 24. If n is odd, then a factorable n-power extension of D_m exists and $\mu_n^F(D_m) \leq K(m,n)$.

Proof. Let $\mu_1 = K(m,n)$, $\mu_2 = \eta_1 = \eta_2 = 1$ and let $e = m\mu_1 - 1 = m \cdot K(m,n) - 1$. Then condition I is satisfied automatically. Conditions II and V are satisfied since $e \equiv -1(\bmod m)$. Condition III is satisfied since $e \equiv -1(\bmod \mu_1)$, and condition IV is satisfied since $e \equiv -1(\bmod m\mu_1)$ and so $e^2 \equiv 1(\bmod m\mu_1)$. Condition VI is satisfied since n is odd and so $(2 \cdot K(m,n), n) = (K(m,n), n) \mid K(m,n)$. For condition VII, if $k = 0$, then setting $q = 0$ satisfies the first requirement of condition VII, and $Q_n(e^0) = Q_n(1) = n$. Then $(n, m \cdot K(m,n)) = K(m,n) = \mu_1\eta_1$. So the second requirement is satisfied. If $k = 1$, then setting $q = 1$, we require $n \equiv K(m,n)(\bmod 2)$, which is true since n and $K(m,n)$ are both odd. Furthermore,

$$Q_n(e^1) \equiv Q_n(-1) \equiv (-1)^{n-1} + (-1)^{n-2} + \cdots + (-1) + (-1)^0$$

$$\equiv 1 - 1 + \cdots - 1 + 1 \equiv 1(\bmod m\mu_1).$$

So $Q_n(e^1)$ is coprime to $m\mu_1$. Therefore all the conditions are satisfied, and so a factorable n-power extension of D_m exists. Notice that the order of this extension is $\mu_1\mu_2 = K(m,n) \cdot 1$, and $h : D_m \hookrightarrow_n D_{m \cdot K(m,n)}$, where $h : C_m a \rtimes_\phi C_2 b \to C_{m \cdot K(m,n)} c \rtimes_\psi C_2 d$ is given by $h(a,1) = (c^{K(m,n)}, 1)$ and $h(1,b) = (1,b)$. □

Now we consider what happens when n is even. This is a more difficult situation to handle because of the C_2 factor in D_m. When n was odd, then raising anything in C_2 to the nth power didn't do anything, and so every element of C_2 was its own nth root. Such is not the case when n is even, since anything in C_2 raised to an even power is the identity.

Corollary 25. If n is even and -1 is not a square modulo m, then there exists no factorable n-power extension of D_m. More generally, if $n = 2^k(2r-1)$ for some $k, r \in \mathbb{N}$, then if -1 is not a 2^kth power modulo m, then there exists no factorable n-power extension of D_m.

Proof. If we apply the 2-adic valuation to condition VI, we get that

$$\min(v_2(2) + v_2(\mu_2), v_2(n)) \leq v_2(\mu_2).$$

But this implies that $v_2(\mu_2) \geq v_2(n) = k$. Let $\mu_2 = 2^k t$. Then condition V implies that

$$-1 \equiv e^{\mu_2} = \left(e^t\right)^{2^k} (\operatorname{mod} m),$$

so -1 is a 2^kth power modulo m. Hence, if -1 is not a 2^kth power, then no such factorable n-power extension exists. □

Conjecture 26. If n is even, $v_2(n) = k > 0$, and -1 is a 2^kth power modulo m, then there exists an n-power extension of $D_m = C_m \rtimes_\phi C_2$.

The simplest way to accomplish a proof of Conjecture 26 is to show that under the hypotheses, we can find integers satisfying conditions I-VII. In particular, if $a \in \{1, \ldots, m-1\}$ such that $(a, m) = 1$ and $a^{2^k} \equiv -1 (\operatorname{mod} m)$, then taking $\mu_1 = K(m, n)$, $\mu_2 = 2^k$, $\eta_1 = 1$, $\eta_2 = 1$ and $e = a$ looks promising as a possible n-power extension of D_m. Note that conditions I, II, V, and VI are already satisfied by this choice of integers. If we can then show that such an a always exists and that these integers satisfy conditions III, IV, and VII, we will have proved the conjecture.

7 Total Divisibility

A natural question that arises in the discussion of divisibility is that of total divisibility, i.e. given a group G, what kinds of groups H can G be embedded into such that G is divisible in H. We will begin by proving an analogue to Proposition 2. We will be using some of the terminology from Definition 1 on page 2.

Proposition 27. Let G be a group. There exists a power extension H of G.

Proof. Let $G = \langle S : R \rangle$ be a presentation of G. Let $A = \left\{a_{g,n} \mid g \in G,\, n \in \mathbb{N}\right\}$ be a set indexed by the elements of G and the natural numbers. Form the group $H = \langle S, A : R, P \rangle$, where $P = \left\{a_{g,n}^{n} g^{-1} \mid g \in G,\, n \in \mathbb{N}\right\}$. Then G naturally embeds into H and by construction, every element of G has an nth root in H for all $n \in \mathbb{N}$, namely $a_{g,n}$. Therefore H is a power extension of G. □

In a manner unlike that of n-divisibility, most of the time a power extension of a group G must be of infinite order. In particular, we show that if G is not already divisble, then it must have infinite index in a power extension H.

Proposition 28. Suppose $f : G \to H$ such that $f : G \hookrightarrow_n H$ for all $n \in \mathbb{N}$. If G is not divisible, then $[H : f(G)] = \infty$.

Proof. Choose $g \in G$ and $n \in \mathbb{N}$ such that g does not have an nth root in G. Let $k \in \mathbb{N}$. Choose $h \in H$ such that $h^{n \cdot k!} = g$. Consider the cosets $h^i f(G)$ for $i = 1, \ldots, k$. Suppose $h^i f(G) = h^j f(G)$ for some $1 \leq j < i \leq k$. Then $h^i h^{-j} = h^{i-j} \in f(G)$. So there exists $x \in G$ such that $f(x) = h^{i-j}$. Let $\hat{x} = x^{k!/(i-j)}$. Then

$$f(\hat{x}^n) = f(\hat{x})^n = f(x)^{n \cdot k!/(i-j)} = \left(h^{i-j}\right)^{n \cdot k!/(i-j)} = h^{n \cdot k!} = f(g).$$

Since f is injective, this implies $\hat{x}^n = g$, a contradiction to our assumption. Therefore the cosets $h^i f(G)$ for $i = 1, , \ldots, k$ are all distinct, so $[H : f(G)] > k$. Since $k \in \mathbb{N}$ was arbitrary, it follows that $[H : f(G)] = \infty$. □

7.1 Cyclic Groups

In this section we will, for ease of computation, write our cyclic groups additively, as $\mathbb{Z}$ instead of C_∞ and $\mathbb{Z}_m$ instead of C_m. We will write the generator of the group as 1 and the identity as 0. In this case, divisibility becomes the problem of being able to solve the equation $n \cdot x = g$ for some element g of the cyclic group. Let us first consider a well-known example: the infinite cyclic group $\mathbb{Z}$. In order to solve the equation $n \cdot x = 1 \in \mathbb{Z}$, we need essentially the element $\frac{1}{n}$ for all n. Thus, we find that

Proposition 29. A power extension of $\mathbb{Z}$ is the additive group $\mathbb{Q}$.

Let us consider the problem of finding a power extension for a finite cyclic group $\mathbb{Z}_m$.

Definition 8. Let $p_1, p_2, \ldots, p_k$ be primes. Let $\mathbb{Z}(p_1, p_2, \ldots, p_k)$ be the set of all fractions whose denominators' prime factors are contained in $\{p_1, p_2, \ldots, p_k\}$ (including those fractions with denominator 1). If $m \in \mathbb{N}$, let $\mathbb{Z}_m(p_1, p_2, \ldots, p_k) = \mathbb{Z}(p_1, p_2, \ldots, p_k)/m\mathbb{Z}$ be this set of fractions modulo m.

Proposition 30. Let $m \in \mathbb{N}$ have prime factors $p_1, p_2, \ldots, p_k$. Then a power extension of $\mathbb{Z}_m$ is $\mathbb{Z}_m(p_1, \ldots, p_k)$.

Proof. Let $H = \mathbb{Z}_m(p_1, \ldots, p_k)$. Note that $\mathbb{Z}(p_1, \ldots, p_m)$ is a subgroup of $\mathbb{Q}$ because adding two fractions does not introduce any new prime factors to the denominator. Let $f : Z_m \to H$ be given by the composition of the inclusion map with the quotient map, i.e. $f(x) = x + N$ for all $x \in \mathbb{Z}_m$. First we must ensure that f is well-defined. This follows from the fact that two elements in H are identified precisely when they differ by a multiple of m. The fact that f is a homomorphism follows from the fact that the inclusion map and the quotient map are both homomorphisms. Suppose $f(x_1) = f(x_2)$. Then $x_1 - x_2 \in N$, and so $x_1 \equiv x_2 (\text{mod } m)$. But this means exactly that $x_1 = x_2$ in $\mathbb{Z}_m$, so f is injective.

By Proposition 7, the group $\mathbb{Z}_m$ is n-divisible for any n coprime to m. Let $n \in \mathbb{N}$ such that $(m,n) > 1$. We wish to show that there exists $z \in H$ such that $n \cdot z = f(1) = 1$. Let $n = n'q$, where n' is coprime to m and q has only prime factors in the set $\{p_1, p_2, \ldots, p_k\}$. Since $(n', m) = 1$, we can find $x \in \mathbb{Z}_m$ such that $n' \cdot x = 1$. By the construction of q, $\frac{1}{q} \in H$. Let $z = \frac{x}{q}$. Then

$$n \cdot z = n'q \cdot z = n'q \cdot \frac{x}{q} = n' \cdot x = 1.$$

So the equation $n \cdot z = 1$ is solvable, hence $\mathbb{Z}_m$ is divisible in H. □

7.2 Direct Products

A natural result on direct products results from essentially applying Proposition 13 with n arbitrary to get an analogous result.

Proposition 31. If f is a power embedding from A to G and g is a power embedding from B to H, then (f,g) is a power embedding from $A \times B$ to $G \times H$.

Proof. For any $n \in \mathbb{N}$, $f : A \hookrightarrow_n G$ and $g : B \hookrightarrow_n H$ since f and g are power embedding. Therefore, by Proposition 13, $(f,g) : A \times B \hookrightarrow_n G \times H$. Since n was arbitrary, (f,g) is a power embedding. □

We finish off this section with a proposition that gives a power extension for any finitely generated Abelian group.

Proposition 32. Let G be a finitely generated Abelian group, and let $G = \mathbb{Z}^r \times \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_m^{\alpha_m}}$ be the elementary divisor decomposition of G. Then the group H is a power extension of G, where

$$H = \mathbb{Q}^r \times \mathbb{Z}_{p_1^{\alpha_1}}(p_1) \times \cdots \times \mathbb{Z}_{p_m^{\alpha_m}}(p_m).$$

Proof. We apply Propositions 29, 30, and 31 a total of r, m, and $r+m-1$ times respectively. □

8 Conjectures and Questions

We end this paper with a conjecture, which we suspect to be true but have not been able to prove, and some questions which are related to the topics in this paper but we did not address.

Conjecture 33. If A and B are groups, then $\mu_n(A \times B) = \mu_n(A) \cdot \mu_n(B)$.

Question 1. We have shown ways of embedding a group G in a larger group H such that every element of G has at least one nth root. Can we say how many nth roots there are? In particular, which of these constructions allows for us to determine a unique nth root of any element of G?

Question 2. Can our techniques be expanded and applied to matrix groups? What about semidirect products of arbitrary (not necessarily finite) cyclic groups? How do they apply to $O(2)$ and $SO(2)$, groups of linear transformations in the plane?

Question 3. The homotopy groups $\pi_m(X)$ of a topological space X are somewhat special in that their elements are equivalence classes of functions into X, and so have a more concrete realization than we normally encounter when working with groups. Given a space X, is there a way to find another space Y and a map $f : X \to Y$ such that f induces an n-embedding of $\pi_m(X)$ into $\pi_m(Y)$, i.e. $f_* : \pi_m(X) \hookrightarrow_n \pi_m(Y)$?

Question 4. We have seen how the $\mu_n(G)$ function behaves with repect to direct and semidirect products. How does it interact with free products $G * H$ or amalgamated free products $G *_N H$? Can this be used to partially answer Question 3 for the fundamental groups $\pi_1(X)$ via the Seifert-van Kampen Theorem?

References

[Dum] Dummit, David S. and Foote, Richard M., *Abstract Algebra 3 ed.*, Wiley, Hoboken, NJ, 2004.

[Fin] Finkelstein, H., *Solving Equations in Groups: A survey of Frobenius' Theorem*, Periodice Mathematica Hungarica Vol 9 (3), (1978), 187-204

[Kur] Kurosh, A.G., *The Theory of Groups, Vol. 1, 2 ed.*, K.A. Hirsch, ed., Chelsea, New York, 1960

[Lyn] Lyndon, R.C., *Equations in Groups*, Bol. Soc. Bras. Mat., Vol. 11 (1) (1980), 79-102

[Jhn] Johnson, D.L., *Presentations of Groups 2 ed.*, Cambridge University Press, Cambridge, 1997