CARDINALITY OF AUTOMORPHISM GROUPS OF FIELD EXTENSIONS

Andrew Barlow

College of William and Mary

Abstract. In this paper, we will consider the cardinalities of different groups related to both finite and infinite groups, specifically, the cardinality of automorphism groups. While the behavior for finite groups is quite predictable, an examination of the cardinalities of automorphism groups of infinite groups leads to an interesting result. By considering certain infinite groups as field extensions of the field of rationals $\mathbb{Q}$, we can show that for such groups, the cardinality of the isomorphism group is dependent on the degree of extension. This concept can be further generalized to apply to any field of characteristic 0.

1. Introduction. Comparing cardinalities of finite sets is relatively easy. At the very least, we can find relations to bound these cardinalities. For example, for a finite set T with cardinality $n > 3$, it is clear that $|P(T)| < |S_T| < |\mathcal{F}_T|$ where $P(T)$ is the power set of T, S_T is the symmetry group of T, and $\mathcal{F}_T$ is the set of all functions from T to T. However, such relations become less clear when dealing with infinite sets. In [2], it is shown that when T is an infinite set, $|P(T)| = |S_T| = |\mathcal{F}_T|$. We seek to find a similar result by studying the cardinality of the automorphism groups of infinite sets.

Consider a group G and let $|G|$ denote the cardinality of G. If G is finite, that is $|G| = n$ and $n > 1$, it is clear that there is a strict relation: $|Aut(G)| < |Hom(G)| < |\mathcal{F}_G|$, where $\mathcal{F}_G$ denotes the set of all functions on G, $Hom(G)$ denotes the set of all homomorphisms on G, and $Aut(G)$ denotes the set of all automorphisms on G. This is because for any such set, the mapping $\phi(x) = 0$ for all x in G is a homomorphism, but not an automorphism, because it is not bijective. Similarly, the mapping $\phi(x) = n$ for all x in G where n is a constant is a mapping in $\mathcal{F}_G$ that is not a homomorphism. But what if G is an infinite group? Then, G could be countable, that is $|G| = \aleph_0$, or G could be uncountable, that is $|G| \geq 2^{\aleph_0}$. We consider the cardinality of the group of automorphisms of G, $|Aut(G)|$. The group of automorphisms on G, $Aut(G)$ is defined as the set of all isomorphisms $\phi : G \to G$, or in other words all bijections $\phi : G \to G$ such that for any $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$ [1]. We will consider how $|Aut(G)|$ compares to the cardinality of other related sets: the symmetry group of G, S_G, the power set of G, $P(G)$, and the set of all functions on G, $\mathcal{F}_G$. In this investigation of $|Aut(G)|$ it will be useful to know that for an infinite set G, $|P(G)| = |S_G| = |\mathcal{F}_G|$ from [2].

We will prove that given a field E that is an extension field of $\mathbb{Q}$, if the degree of extension α of E over $\mathbb{Q}$, $\alpha = [E : \mathbb{Q}]$ is finite, that is $\alpha < \aleph_0$, then $|Aut(E, +)| = |Q|$. Otherwise, if the degree of extension is infinite, that is $\alpha \geq \aleph_0$, then $|Aut(E, +)| = 2^{|E|} = |\mathcal{F}_E|$. This result can be further generalized to show that the above is true for a general field of characteristic 0, or in other words, a field in which the multiplicative identity can be added to itself infinite times without ever reaching the additive identity.

2. Examples. We will begin by studying several infinite groups of differing cardinality and structure as examples. These groups will include the integers $\mathbb{Z}$ under addition, the rationals $\mathbb{Q}$ under addition, and the reals $\mathbb{R}$ under addition.

2.1 The group of integers under addition. To find the cardinality of $Aut(\mathbb{Z}, +)$, we must find all automorphisms on $\mathbb{Z}$. In order for a bijection $\phi : \mathbb{Z} \to \mathbb{Z}$ to be an automorphism, it must preserve the operation, or in other words, for some $a, b \in \mathbb{Z}$, $\phi(a + b) = \phi(a) + \phi(b)$. Since $\mathbb{Z}$ is cyclic, it follows that all automorphisms on $\mathbb{Z}$ must map generators of $\mathbb{Z}$ to other generators of $\mathbb{Z}$ in order to preserve the operation. The generations of $\mathbb{Z}$ are 1 and -1. Hence, we have two automorphisms on $\mathbb{Z}$ determined by $\phi(1) = 1$ and $\phi(1) = -1$, and $|Aut(\mathbb{Z}, +)| = 2$.

2.2 The group of rational numbers under addition. To find the cardinality of $Aut(\mathbb{Q}, +)$ we will show that every automorphism on $\mathbb{Q}$ is of the form $\phi(x) = x\phi(1)$ for every $x \in \mathbb{Q}$. Let ϕ be an automorphism on $\mathbb{Q}$. Then for some n, $\phi(n) = \phi(1+1+\cdots+1) = \phi(1)+\phi(1)+\cdots+\phi(1) = n\phi(1)$. Similarly, $\phi(1) = \phi(\frac{n}{n}) = \phi(\frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n}) = \phi(\frac{1}{n}) + \phi(\frac{1}{n}) + \cdots + \phi(\frac{1}{n}) = n\phi(\frac{1}{n})$. Since $\phi(1) = n\phi(\frac{1}{n})$, it follows that $\phi(\frac{1}{n}) = \frac{1}{n}\phi(1)$. Using these facts, consider $\phi(\frac{m}{n})$. $\phi(\frac{m}{n}) = \phi(\frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n}) = \phi(\frac{1}{n}) + \phi(\frac{1}{n}) + \cdots + \phi(\frac{1}{n}) = m\phi(\frac{1}{n})$. Then,

since $\phi(\frac{1}{n}) = \frac{1}{n}\phi(1)$, $\phi(\frac{m}{n}) = m\frac{1}{n}\phi(1) = \frac{m}{n}\phi(1)$. Therefore, for any $x \in \mathbb{Q}$ where ϕ is an automorphism, $\phi(x) = x\phi(1)$. Since we can define an automorphism for each $q \in \mathbb{Q}$ by setting $\phi(1) = q$, it follows that $|Aut(\mathbb{Q}, +)| = |\mathbb{Q}| = \aleph_0$.

2.3 The group of real numbers under addition. The cardinality of $Aut(\mathbb{R}, +)$ can be found by considering the real numbers as a vector space over the rational numbers. From [3], the Axiom of Choice guarantees that there exists a basis for $\mathbb{R}$ over $\mathbb{Q}$, $B = \{q_i : i \in I\}$. But what is the size of this basis $|B|$? This can be found using the method from [4]. It is clear that $B \subseteq \mathbb{R}$, so $|B| \leq |\mathbb{R}|$. Then, for each $x \in \mathbb{R}$, there exists a finite set $B_x = \{b_1, b_2, \ldots, b_n\} \subset B$ such that $x = q_1b_1 + q_2b_2 + \cdots + q_nb_n$ where $q_i \in \mathbb{Q}$ for each $i \in \mathbb{N}$ with $1 \leq i \leq n$. Now, let H denote the set of all finite subsets of B. Clearly, $|H| = |B|$. Then, for each $h = \{b_1, b_2, \ldots, b_n\} \in H$ there are $|\mathbb{Q}|^n = \aleph_0^n = \aleph_0$ linear combinations $q_1b_1 + q_2b_2 + \cdots + q_nb_n$, again with each $q_i \in \mathbb{Q}$. So, $|\mathbb{R}| = 2^{\aleph_0} = |span(B)|$. The cardinality of the span of B must be less than or equal to the number of all linear combinations formed with each $h \in H$. So, $|\mathbb{R}| = |span(B)| \leq |H| * \aleph_0 = |B| * \aleph_0 = |B|$. Now, since $|B| \leq |\mathbb{R}|$ and $|B| \geq |\mathbb{R}|$, it follows that $|B| = |\mathbb{R}| = \aleph_0$.

Now, any bijection ϕ such that $\phi(B) = B'$ is a basis for $\mathbb{R}$ over $\mathbb{Q}$ is an automorphism on the group of reals under addition from [5]. Therefore, any bijection that permutes the elements of B is an automorphism, or in other words, if $a \in B$, then $\phi(a) \in B$. Since S_B is the group of all one to one functions from $B \to B$, it follows that $|Aut(\mathbb{R}, +)| \geq |S_B| = |S_{\mathbb{R}}|$, since $|B| = |\mathbb{R}|$. Since every automorphism on $\mathbb{R}$ is a function on $\mathbb{R}$, it also follows that $|Aut(\mathbb{R}, +)| \leq |\mathcal{F}_{\mathbb{R}}|$. Since $|S_{\mathbb{R}}| \leq |Aut(\mathbb{R}, +)| \leq |\mathcal{F}_{\mathbb{R}}| = |S_{\mathbb{R}}|$, $|Aut(\mathbb{R}, +)| = |S_{\mathbb{R}}| = |\mathcal{F}_{\mathbb{Q}}| = |P(\mathbb{R})|$.

3. Result. We will now prove that for a field extension E of $\mathbb{Q}$ with $[E : \mathbb{Q}] = \alpha$, if $\alpha < \aleph_0$ then $|Aut(E)| = |\mathbb{Q}| = \aleph_0$, and if $\alpha \geq \aleph_0$ then $|Aut(E)| = |\mathcal{F}_E|$. After that, we will consider the general case of any field of characteristic 0. There are two cases:

3.1 Finite extension fields of $\mathbb{Q}$ under addition. In this case $\alpha < \aleph_0$. The proof of this case relies on the fact that $|Aut(\mathbb{Q}, +)| = \aleph_0$, which is shown above. Let E be a finite extension field of $\mathbb{Q}$, $E = \mathbb{Q}(x_1, x_2, \ldots, x_n)$ with $[E : \mathbb{Q}] = \alpha$. Then, consider the automorphism group $Aut(E, +)$. Let $x, y \in E$. Then by definition, if ϕ is an automorphism on E, $\phi(x+y) = \phi(x)+\phi(y)$. Given an integer m, it is clear that $\phi(mx) = \phi(x+x+\cdots+x) = m\phi(x)$. Since $\phi(x) = \phi(\frac{x}{m}+\frac{x}{m}+\cdots+\frac{x}{m}) = \phi(\frac{x}{m})+\phi(\frac{x}{m})+\cdots+\phi(\frac{x}{m}) = m\phi(\frac{x}{m})$, it follows that $\phi(\frac{x}{m}) = \frac{1}{m}\phi(x)$. Therefore, for any rational $\lambda \in \mathbb{Q}$, $\phi(\lambda x) = \lambda\phi(x)$. Now, let $B = \{b_1, b_2, \ldots, b_\alpha\}$ be the basis of E over $\mathbb{Q}$. Then any element $x \in E$ can be expressed as a linear combination of the form $x = b_1q_1 + b_2q_2 + \cdots + b_\alpha q_\alpha$ where $q_i \in \mathbb{Q}$. Knowing that $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(\lambda x) = \lambda\phi(x)$, it follows that $\phi(x) = q_1\phi(b_1) + q_2\phi(b_2) + \cdots + q_\alpha\phi(b_\alpha)$. Then, any group isomorphism between vector spaces A and B can be represented as an invertible α by β matrix where α is the dimension of A and β is the dimension of B where each element of the matrix is in E. It is clear that $|E| = \aleph_0$, so there are $\aleph_0$ possibilities for each element of the matrix. Therefore, there are $\aleph_0^{\alpha^2} = \aleph_0$ possible α by α matrices, so $|Aut(E, +)| \leq \aleph_0$. However, we can find $\aleph_0$ automorphisms by mapping $\phi(B) = B$, since there are $\aleph_0$ mappings on $\mathbb{Q}$. Therefore, $\aleph_0 \leq |Aut(E, +)| \leq \aleph_0$, so $|Aut(E, +)| = \aleph_0$.

3.2 Infinite extension fields of $\mathbb{Q}$ under addition. In this case $\alpha \geq \aleph_0$. The proof of this case is similar to the proof for $\mathbb{R}$ as a vector space over $\mathbb{Q}$. The axiom of choice guarantees the existence of a basis B for E over $\mathbb{Q}$. To find the cardinality of B, we use the fact that $|B|$ is clearly less than or equal to $|E|$ since B spans E, and show that $|B| \geq |E|$. By definition, each element $x \in E$ can be written as a linear combination on a finite subset of B, such that $x = q_1b_1 + q_2b_2 + \cdots + q_nb_n$ where $q_i \in \mathbb{Q}$ and $b_i \in B$. Let H denote the set of all finite subsets of B. Clearly $|H| = |B|$. Then, for each $h \in H$ where $|h| = n$, there are $|\mathbb{Q}|^n = |\mathbb{Q}| = \aleph_0$ possible linear combinations on h. We know that $|E| = |span(B)|$. Then, the cardinality of $span(B)$ must be less than or equal to the number of all possible linear combinations formed by each $h \in H$. So, $|E| = |span(B)| \leq |H| * \aleph_0 = |B| * \aleph_0 = |B|$, since $|B| \geq \aleph_0$. Since $|B| \leq |E|$ and $|B| \geq |E|$ it follows that $|B| = |E|$.

Now, we can find $|S_B|$ automorphisms on E, as each permutation of the basis over $\mathbb{Q}$ will give an automorphism. So, $|Aut(E, +)| \geq |S_B|$. Since $|B| = |E|$, $|S_B| = |S_E| = |\mathcal{F}_E|$ from [2]. Since $\mathcal{F}_E$ is the set of

all functions on E, $|Aut(E,+)| \leq |\mathcal{F}_E|$. Since $|\mathcal{F}_\mathcal{E}| \leq |Aut(E,+)| \leq |\mathcal{F}_E|$, it follows that $|Aut(E,+)| = |\mathcal{F}_E|$.

3.3 A general field of characteristic 0. Let F be a field with characteristic 0. Then, we can construct an integral sub domain $D = \{1 * n : n \in \mathbb{Z}\}$ where 1 is the multiplicative identity of F. From this construction, it is clear that D is isomorphic to $\mathbb{Z}$, and it follows that the quotient field of D which we will denote as $\mathcal{D}$ is isomorphic to the quotient field of $\mathbb{Z}$, $\mathbb{Q}$. So, we have a subfield of F isomorphic to $\mathbb{Q}$. Then, the result from above can be directly applied, such that when the index of F over $\mathcal{D}$ is finite, $|Aut(F,+)| = \aleph_0$ and when the index of F over $\mathcal{D}$ is infinite, $|Aut(F,+)| = |\mathcal{F}_F|$.

4. Conclusion We have shown that for any infinite group G that is also a field of characteristic 0, we can construct a subfield $\mathcal{D}$ isomorphic to $\mathbb{Q}$ and determine the number of group automorphisms on G by finding the degree of extension of G over this subfield. If $[G : \mathcal{D}]$ is finite, then $|Aut(G)| = \aleph_0$ and if $[G : \mathcal{D}]$ is infinite, then $|Aut(G)| = |\mathcal{F}_G|$. Further research could be done by studying the behavior of different infinite groups without this field structure, to determine whether a more general statement can be made about the automorphism groups of these infinite groups.

References

[1] Gallian, Joseph. *Contemporary Abstract Algebra 8th Edition*, Brooks/Cole, 2013. 127-138.

[2] O'Brien, Erin. *Cardinality of Permutation Groups.* 2015.

[3] Schechter, Eric. "Axiom of Choice",
URL = <http://www.math.vanderbilt.edu/ schectex/ccc/choice.html>.

[4] Youcis, Alex. "The Dimension of R over Q",
URL = <https://drexel28.wordpress.com/2010/10/22/the-dimension-of-r-over-q/>.

[5] "What is $Aut(\mathbb{R},+)$?,
URL = <http://math.stackexchange.com/questions/115486/what-is-operatornameaut-mathbbr>