APPENDIX D

AUTOMORPHISMS OF THE COMPLEX NUMBERS

This appendix discusses an issue that arose in Section VI.3. It is written at a level somewhat higher than the notes, but not as high as the level of material in Appendix B. The necessary background can be found in the graduate algebra text by T. Hungerford and the introductory graduate level topology text by J. Munkres that are listed in the bibliography.

The Fundamental Theorem of Projective Geometry in Chapter VI (Theorem VI.14) implies that for each positive integer n there is a group homomorphism from the group $\textsc{Coll}(\mathbb{FP}^n)$ of geometric symmetries, or *collineations*, of $\mathbb{FP}^n$ to the automorphism group $\textsc{Aut}(\mathbb{F})$ of $\mathbb{F}$, and this mapping is onto. For some fields such as the rational numbers $\mathbb{Q}$ and the real numbers $\mathbb{R}$, the only automorphism is the identity. On the other hand, in the notes we pointed out that the field $\mathbb{C}$ of complex numbers also has a second automorphism given by complex conjugation. This leads immediately to the following:

Quesion. *Are there any automorphisms of $\mathbb{C}$ other than the identity and complex conjugation?*

In fact, there are two reasonable ways of answering this question. If we restrict our attention to automorphisms that are *continuous* as mappings of $\mathbb{C} \cong \mathbb{R}^2$ to itself, then the identity and complex conjugation are the only possibilities. On the other hand, if we consider arbitrary automorphisms of $\mathbb{C}$ with no continuity requirement, then the automorphism group $\textsc{Aut}(\mathbb{C})$ of $\mathbb{C}$ is huge. One illustration of this is the formula for its cardinality given below.

Continuous automorphisms of $\mathbb{C}$

We shall first prove that there are only two continuous automorphisms.

Theorem D.1. *Let $\varphi : \mathbb{C} \to \mathbb{C}$ be an automorphism of the complex numbers that is also continuous as a function of two variables. Then φ is either equal to the identity or to complex conjugation.*

Proof. Every automorphism sends 0 and 1 to themselves, and from this it follows that every automorphism sends the rational numbers $\mathbb{Q} \subset \mathbb{C}$ to itself by the identity. Furthermore, if $a \in \mathbb{Q}$ is nonzero and $b \in \mathbb{C}$ satisfies $b^2 = a$, then we also have $\varphi(b)^2 = a$, and since $\pm\, b$ are the only two numbers such that $b^2 = a$ we must have $\varphi(b) = \pm\, b$.

Let $\mathbb{Q}[\mathbf{i}]$ be the set of all complex numbers of the form $a + b\mathbf{i}$, where $\mathbf{i}^2 = -1$ and $a,\ b \in \mathbb{Q}$. Since $\pm\, \mathbf{i}$ are the only two complex numbers whose squares are equal to -1, it follows that $\varphi(\mathbf{i}) = \pm\, \mathbf{i}$. Therefore φ agrees with either the identity or conjugation on $\mathbb{Q}[\mathbf{i}]$.

Just as the rationals are dense in $\mathbb{R}$, so also the set $\mathbb{Q}[\mathbf{i}]$ is dense in $\mathbb{C}$.[1] Since two continuous functions from $\mathbb{C}$ to itself are equal if they agree on a dense subset,[2] it follows that φ is equal to the identity or complex conjugation, depending upon whether $\varphi(\mathbf{i}) = \mathbf{i}$ or $\varphi[\mathbf{i}] = -\mathbf{i}$.■

Arbitrary automorphisms of $\mathbb{C}$

This discussion will rely heavily on the existence of *transcendence bases* for the $\mathbb{C}$ with respect to its subfield $\mathbb{Q}$; more generally, this notion is defined for any pair of fields $\mathbb{F}$ and $\mathbb{E}$ such that $\mathbb{F}$ is a subfield of $\mathbb{E}$ (equivalently, $\mathbb{E}$ is an extension field of $\mathbb{F}$), at least if we have a field of characteristic zero which contains an isomorphic copy of $\mathbb{Q}$. Formal definitions and the basic properties of such subsets are contained in Section VI.1 of Hungerford's book. A brief summary of some important points is given in the Wikipedia reference:[3]

`http://en.wikipedia.org/wiki/Transcendence_degree`

For our purposes the main thing to know is that if $\mathbb{E}$ is an extension field of $\mathbb{F}$, then different transcendence bases for $\mathbb{E}$ with respect to $\mathbb{F}$ have the same cardinality, and in fact one has the following basic result:

Theorem D.2. *Let $\mathbb{E}$ and $\mathbb{F}$ be as above, assume that $\mathbb{E}$ is algebraically closed, let B and B' be transcendence bases for $\mathbb{E}$ with respect to $\mathbb{F}$, and let $h : B \to B'$ be a $1-1$ correspondence. Then there is an automorphism φ of $\mathbb{E}$ such that φ maps itself to the identity and $\varphi(b) = h(b)$ for all $b \in B$.*■

EXAMPLE. In particular, if B is nonempty, then one can take B' to be the set of all negatives of elements in B and define $h(b) = -b$. Similarly, if we split B into two nonempty disjoint subsets $B_0 \cup B_1$, take B_1' to be the set of all negatives of elements in B_1, write $B' = B_0 \cup B_1'$, and take $h : B \to B'$ to be the identity on B_0 and multiplication by (-1) on B_1, then we obtain an automorphism that is different from the preceding one. In particular, if the cardinality of B is β, this yields a family of 2^β automorphisms of $\mathbb{E}$.

In order to apply the preceding theorem to the complex numbers, we need the following additional facts.

Theorem D.3. *Let $\mathbb{E}$ and $\mathbb{F}$ be as above, let B be a transcendence base for $\mathbb{E}$ over $\mathbb{F}$, let $\mathbb{L} \subset \mathbb{E}$ be the smallest subfield containing $\mathbb{F}$ and B, and suppose that $\mathbb{F}$ is a countably infinite set. Denote the cardinality of B by β. Then the cardinality of $\mathbb{L}$ is also equal to β.*■

Theorem D.4. *Let $\mathbb{L}$ be a field of infinite cardinality λ, and let $\mathbb{E}$ be the algebraic closure of $\mathbb{L}$. Then the cardinality of $\mathbb{E}$ is also equal to λ.*■

The applications to the complex numbers are now immediate.

---

[1] See Munkres, Exercise 10, p. 194.

[2] Munkres, Exercise 5, p. 199, plus (*i*) the definition of dense subset on p. 191, (*ii*) the proof that metric spaces are Hausdorff on p. 129.

[3] Previous comments about Wikipedia articles also apply here.

Theorem D.5. *If B is a transcendence base for the complex numbers with respect to the rationals, then the cardinality of B is equal to $\mathfrak{c} = 2^{\aleph_0}$.*

Proof. Let $\mathbb{L}$ again be the smallest subfield containing both the rationals and B. By definition of transcendence bases, it follows that every element of $\mathbb{C}$ is algebraic over $\mathbb{L}$. Since $\mathbb{C}$ is algebraically closed, it contains an isomorphic copy of the algebraic closure $\mathbb{K}$ of $\mathbb{L}$. We claim that $\mathbb{K} = \mathbb{C}$; this is true because the elements of $\mathbb{C}$ are all algebraic over $\mathbb{L}$.

Applying the previous results, we see that the cardinalities of $\mathbb{C}$ and $\mathbb{L}$ must be the same, so the latter has cardinality $\mathfrak{c}$. By another of the theorems stated above, this in turn implies that the cardinality of the transcendence base B is also equal to $\mathfrak{c}$.■

The existence of infinitely many distinct automorphisms of the complex numbers (in fact, $2^{\mathfrak{c}}$ of them) follows immediately, and hence the identity and complex conjugation are far from being the only ones. In fact, we can evaluate the cardinality of $\textsc{Aut}(\mathbb{C})$ precisely:

Theorem D.6. *The cardinality of* $\textsc{Aut}(\mathbb{C})$ *is equal to* $2^{\mathfrak{c}}$.

Proof. The cardinality γ of $\textsc{Aut}(\mathbb{C})$ is certainly no greater than $\mathfrak{c}^{\mathfrak{c}}$, which is the cardinality of the set of (purely set-theoretic) functions from $\mathbb{C}$ to itself. On the other hand, we also have

$$2^{\mathfrak{c}} \ \leq \ \mathfrak{c}^{\mathfrak{c}} \ = \ \left(2^{\aleph_0}\right)^{\mathfrak{c}} \ = \ 2^{\aleph_0 \cdot \mathfrak{c}} \ = \ 2^{\mathfrak{c}}$$

(since $\mathfrak{c} \ \leq \ \aleph_0 \cdot \mathfrak{c} \ \leq \ \mathfrak{c} \cdot \mathfrak{c} \ = \ \mathfrak{c}$) so that

$$\mathfrak{c}^{\mathfrak{c}} \ = \ 2^{\mathfrak{c}}$$

and hence $\gamma \leq 2^{\mathfrak{c}}$. We had already established the reverse inequality earlier, and thus it follows that the equation in the theorem is correct.■

FURTHER RESULTS. We should also mention one additional consequence of the preceding ideas which is mentioned in the Wikipedia article. Namely, there exist field homomorphisms from $\mathbb{C}$ to itself whose images are proper subfields of $\mathbb{C}$; in other words, $\mathbb{C}$ is algebraically isomorphic to proper subfields of itself.■