theorem on constructible numbers

Canonical name	TheoremOnConstructibleNumbers
Date of creation	2013-03-22 17:16:28
Last modified on	2013-03-22 17:16:28
Owner	Wkbj79 (1863)
Last modified by	Wkbj79 (1863)
Numerical id	10
Author	Wkbj79 (1863)
Entry type	Theorem
Classification	msc 12D15
Related topic	ConstructibleNumbers
Related topic	ClassicalProblemsOfConstructibility
Defines	immediately constructible from

Theorem 1. *Let $\mathbb{F}$ be the field of constructible numbers and $\alpha \in \mathbb{F}$. Then there exists a nonnegative integer k such that $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2^k$.*

Before proving this theorem, some preliminaries must be addressed.

First of all, within this entry, the following nonconventional definition will be used:

Let S be a subset of $\mathbb{C}$ that contains a nonzero complex number and $\alpha \in \mathbb{C}$. Then α is *immediately constructible from S* if any of the following hold:

- $\alpha = a + b$ for some $a, b \in S$;
- $\alpha = a - b$ for some $a, b \in S$;
- $\alpha = ab$ for some $a, b \in S$;
- $\alpha = a/b$ for some $a, b \in S$ with $b \neq 0$;
- $\alpha = \sqrt{|z|}e^{\frac{i\theta}{2}}$ for some $z \in S$ with $z \neq 0$ and $\theta = \arg(z)$ with $0 \leq \theta < 2\pi$.

The following lemmas are clear from this definition:

Lemma 1. *Let S be a subset of $\mathbb{C}$ that contains a nonzero complex number and $\alpha \in \mathbb{C}$. Then α is constructible from S if and only if there exists a finite sequence $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ such that α_1 is immediately constructible from S, α_2 is immediately constructible from $S \cup \{\alpha_1\}$, $\dots$, and α is immediately constructible from $S \cup \{\alpha_1, \dots, \alpha_n\}$.*

Lemma 2. *Let F be a subfield of $\mathbb{C}$ and $\alpha \in \mathbb{C}$. If α is immediately constructible from F, then either $[F(\alpha):F] = 1$ or $[F(\alpha):F] = 2$.*

Now to prove the theorem.

Proof. By the first lemma, there exists a finite sequence $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ such that α_1 is immediately constructible from $\mathbb{Q}$, α_2 is immediately constructible from $\mathbb{Q} \cup \{\alpha_1\}$, $\dots$, and α is immediately constructible from $\mathbb{Q} \cup \{\alpha_1, \dots, \alpha_n\}$. Thus, α_2 is immediately constructible from $\mathbb{Q}(\alpha_1)$, $\dots$, and α is immediately constructible from $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$. By the second lemma, $[\mathbb{Q}(\alpha_1):\mathbb{Q}]$ is equal to either 1 or 2, $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)]$ is equal to either 1 or 2, $\dots$, and $[\mathbb{Q}(\alpha_1, \dots, \alpha_n, \alpha):\mathbb{Q}(\alpha_1, \dots, \alpha_n)]$ is equal to either 1 or 2. Therefore, there exists a nonnegative integer m such that $[\mathbb{Q}(\alpha_1, \dots, \alpha_n, \alpha):\mathbb{Q}] = 2^m$. Since $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha_1, \dots, \alpha_n, \alpha)$, it follows that there exists a nonnegative integer k such that $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2^k$. $\square$