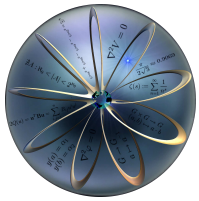

planetmath.org

Math for the people, by the people.

primitive element theorem

Canonical name	PrimitiveElementTheorem
Date of creation	2013-03-22 11:45:48
Last modified on	2013-03-22 11:45:48
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	18
Author	alozano (2414)
Entry type	Theorem
Classification	msc 12F05
Classification	msc 65-01
Related topic	SimpleFieldExtension
Related topic	PrimitiveElementOfBiquadraticField2
Related topic	PrimitiveElementOfBiquadraticField

Theorem 1. *Let F and K be arbitrary fields, and let K be an extension of F of finite degree. Then there exists an element $\alpha \in K$ such that $K = F(\alpha)$ if and only if there are finitely many fields L with $F \subseteq L \subseteq K$.*

Note that this implies that every finite separable extension is not only finitely generated, it is generated by a single element.

Let X be an indeterminate. Then $\mathbb{Q}(X, i)$ is not generated over $\mathbb{Q}$ by a single element (and there are infinitely many intermediate fields $\mathbb{Q}(X, i)/L/\mathbb{Q}$). To see this, suppose it is generated by an element α. Then clearly α must be transcendental, or it would generate an extension of finite degree. But if α is transcendental, we know it is isomorphic to $\mathbb{Q}(X)$, and this field is not isomorphic to $\mathbb{Q}(X, i)$: for example, the polynomial $Y^2 + 1$ has no roots in the first but it has two roots in the second. It is also clear that it is not sufficient for every element of K to be algebraic over F: we know that the algebraic closure of $\mathbb{Q}$ has infinite degree over $\mathbb{Q}$, but if α is algebraic over $\mathbb{Q}$ then $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ will be finite.

This theorem has the corollary:

Corollary 1. *Let F be a field, and let $[F(\beta, \gamma) : F]$ be finite and separable. Then there exists $\alpha \in F(\beta, \gamma)$ such that $F(\beta, \gamma) = F(\alpha)$. In fact, we can always take α to be an F-http://planetmath.org/LinearCombinationlinear combination of β and γ.*

To see this (in the case of characteristic 0), we need only show that there are finitely many intermediate fields. But any intermediate field is contained in the splitting field of the minimal polynomials of β and γ, which is Galois with finite Galois group. The explicit form of α comes from the proof of the theorem.

For more detail on this theorem and its proof see, for example, *Field and Galois Theory*, by Patrick Morandi (Springer Graduate Texts in Mathematics 167, 1996).