a polynomial of degree n over a field has at most n roots

Canonical name	APolynomialOfDegreeNOverAFieldHasAtMostNRoots
Date of creation	2013-03-22 15:09:01
Last modified on	2013-03-22 15:09:01
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	5
Author	alozano (2414)
Entry type	Theorem
Classification	msc 13P05
Classification	msc 11C08
Classification	msc 12E05
Related topic	Root
Related topic	FactorTheorem
Related topic	PolynomialCongruence
Related topic	EveryPrimeHasAPrimitiveRoot
Related topic	CongruenceOfArbitraryDegree

Lemma (cf. factor theorem)**.** *Let R be a commutative ring with identity and let $p(x) \in R[x]$ be a polynomial with coefficients in R. The element $a \in R$ is a root of $p(x)$ if and only if $(x - a)$ divides $p(x)$.*

Proof. See proof of factor theorem using division. $\square$

Theorem. *Let F be a field and let $p(x)$ be a non-zero polynomial in $F[x]$ of degree $n \geq 0$. Then $p(x)$ has at most n roots in F (counted with multiplicity).*

Proof. We proceed by induction. The case $n = 0$ is trivial since $p(x)$ is a non-zero constant, thus $p(x)$ cannot have any roots.

Suppose that any polynomial in $F[x]$ of degree n has at most n roots and let $p(x) \in F[x]$ be a polynomial of degree $n + 1$. If $p(x)$ has no roots then the result is trivial, so let us assume that $p(x)$ has at least one root $a \in F$. Then, by the lemma above, there exist a polynomial $q(x)$ such that:

$$p(x) = (x - a) \cdot q(x).$$

Hence, $q(x) \in F[x]$ is a polynomial of degree n. By the induction hypothesis, the polynomial $q(x)$ has at most n roots. It is clear that any root of $q(x)$ is a root of $p(x)$ and if $b \neq a$ is a root of $p(x)$ then b is also a root of $q(x)$. Thus, $p(x)$ has at most $n + 1$ roots, which concludes the proof of the theorem. $\square$

Note: The fundamental theorem of algebra states that if F is algebraically closed then any polynomial of degree n has exactly n roots (counted with multiplicity).