freshman's dream

Canonical name	FreshmansDream
Date of creation	2013-03-22 15:51:17
Last modified on	2013-03-22 15:51:17
Owner	Algeboy (12884)
Last modified by	Algeboy (12884)
Numerical id	18
Author	Algeboy (12884)
Entry type	Theorem
Classification	msc 11T23
Classification	msc 11T30
Synonym	Frobenius Automorphism
Related topic	PolynomialCongruence

Theorem 1 (Freshman's dream)**.** *If k if a field of* `http://planetmath.org/Characteristic`*chara*
$p > 0$ (so p is prime) then for all $x, y \in k$ we have

$$(x+y)^{p^i} = x^{p^i} + y^{p^i}.$$

Therefore $x \mapsto x^{p^i}$ is a field monomorphism (called a Frobenius monomorphism.)

When k is finite then it is indeed an automorphism. A field k is called a perfect field when the map is surjective.

The theorem is so named because it is a common mistake for freshman math students to make over the real numbers. However, as the characteristic of the real numbers is 0, this does not apply in any interesting way to that setting.

It should also be noted that the result applies only to powers of the characteristic, and not all exponents.

Proof. The proof is an application of the binomial theorem. We prove it for p first.

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}.$$

Now observe

$$\binom{p}{i} = \frac{p!}{(p-i)!i!} = p \cdot \frac{(p-1)!}{(p-i)!i!}.$$

As p is prime and $1 \leq i \leq p-1$ it follows $i!$ and $(p-i)!$ do not divide p. As the field k has characteristic p, $\frac{(p-1)!}{(p-i)!i!}$ is an integer m where

$$\binom{p}{i} = pm \equiv 0.$$

Thus $(x+y)^p = x^p + y^p$.

Now for p^i simply use induction:

$$(x+y)^{p^i} = ((x+y)^p)^{p^{i-1}} = (x^p + y^p)^{p^{i-1}} = x^{p^i} + y^{p^i}.$$

$\square$