algebraic closure of a finite field

Canonical name	AlgebraicClosureOfAFiniteField
Date of creation	2013-03-22 16:40:51
Last modified on	2013-03-22 16:40:51
Owner	Algeboy (12884)
Last modified by	Algeboy (12884)
Numerical id	5
Author	Algeboy (12884)
Entry type	Derivation
Classification	msc 12F05
Related topic	FiniteField
Related topic	FiniteFieldCannotBeAlgebraicallyClosed

Fix a prime p in $\mathbb{Z}$. Then the Galois fields $GF(p^e)$ denotes the finite field of order p^e, $e \geq 1$. This can be concretely constructed as the splitting field of the polynomials $x^{p^e} - x$ over $\mathbb{Z}_p$. In so doing we have $GF(p^e) \subseteq GF(p^f)$ whenever $e|f$. In particular, we have an infinite chain:

$$GF(p^{1!}) \subseteq GF(p^{2!}) \subseteq GF(p^{3!}) \subseteq \cdots \subseteq GF(p^{n!}) \subseteq \cdots .$$

So we define $GF(p^\infty) = \bigcup_{n=1}^{\infty} GF(p^{n!})$.

Theorem 1. *$GF(p^\infty)$ is an algebraically closed field of characteristic p. Furthermore, $GF(p^e)$ is a contained in $GF(p^\infty)$ for all $e \geq 1$. Finally, $GF(p^\infty)$ is the algebraic closure of $GF(p^e)$ for any $e \geq 1$.*

Proof. Given elements $x, y \in GF(p^\infty)$ then there exists some n such that $x, y \in GF(p^{n!})$. So $x+y$ and xy are contained in $GF(p^{n!})$ and also in $GF(p^\infty)$. The properties of a field are thus inherited and we have that $GF(p^\infty)$ is a field. Furthermore, for any $e \geq 1$, $GF(p^e)$ is contained in $GF(p^{e!})$ as $e|e!$, and so $GF(p^e)$ is contained in $GF(p^\infty)$.

Now given $p(x)$ a polynomial over $GF(p^\infty)$ then there exists some n such that $p(x)$ is a polynomial over $GF(p^{n!})$. As the splitting field of $p(x)$ is a finite extension of $GF(p^{n!})$, so it is a finite field $GF(p^e)$ for some e, and hence contained in $GF(p^\infty)$. Therefore $GF(p^\infty)$ is algebraically closed. $\square$

We say $GF(p^\infty)$ is *the* algebraic closure indicating that up to field isomorphisms, there is only one algebraic closure of a field. The actual objects and constructions may vary.

Corollary 2. *The algebraic closure of a finite field is countable.*

Proof. By construction the algebraic closure is a countable union of finite sets so it is countable. $\square$

References

[1] McDonald, Bernard R., *Finite rings with identity*, Pure and Applied Mathematics, Vol. 28, Marcel Dekker Inc., New York, 1974, p. 48.