Lecture 27: Some properties of finite fields

Friday, June 8, 2018 10:38 AM

<u>Theorem</u> For any prime p and $d \in \mathbb{Z}^+$, there is a unique, up to an isomorphism, field of order p^d. (It is often denoted by $\mathbb{F}_{p^d}$.)

<u>Pf.</u> We have proved the existence. Suppose E_1 and E_2 are two fields of order p^d. Then char E_i = the additive order of 1 divides $|E_i|$; and char E_i is prime as E_i is an integral domain. Hence char $E_i = p$ as p is the only prime factor of $|E_i| = p^d$. Hence $\mathbb{Z}_p$ is a subring of E_i. We have seen that $x^{p^d} - x = \prod_{\alpha \in E_i} (x - \alpha)$ in $E_i[x]$. Hence E_i is a splitting field of $x^{p^d} - x$ over $\mathbb{Z}_p$. Therefore by the uniqueness of splitting fields, $E_1 \simeq E_2$. ■

<u>Proposition.</u> Suppose p is prime, $m | n$ are positive integers. Then there is a unique subfield of $\mathbb{F}_{p^n}$ that has order p^m.

<u>Pf.</u> <u>Existence.</u> Suppose $n = mk$. Then $p^n - 1 = (p^m)^k - 1$. Let $q = p^m$. Then $p^n - 1 = q^k - 1 = \underbrace{(q-1)}_{p^m-1}(q^{k-1} + q^{k-2} + \cdots + 1)$. And so $p^m - 1 \mid p^n - 1$.

Hence similarly $x^{p^m-1} - 1$ divides $x^{p^n-1} - 1$. Therefore

Lecture 27: Some properties of finite fields

Friday, June 8, 2018 10:51 AM

$x^{p^m}-x$ divides $x^{p^n}-x=\prod_{\alpha\in\mathbb{F}_{p^n}}(x-\alpha)$. Hence all the zeros of $x^{p^m}-x$ are in $\mathbb{F}_{p^n}$; and so a splitting field of $x^{p^m}-x$ is a subfield of $\mathbb{F}_{p^n}$. Thus $\mathbb{F}_{p^n}$ has a subfield of order p^m.

Uniqueness. Suppose E_1 and E_2 are two subfields of $\mathbb{F}_{p^n}$ that have p^m elements. Suppose to the contrary that $E_1\neq E_2$. Hence $|E_1\cup E_2|\geq p^m+1$. On the other hand,

$\forall \alpha\in E_1\cup E_2$, $\alpha^{p^m}-\alpha=0$; and $x^{p^m}-x$ has at least p^m+1 zeros in $\mathbb{F}_{p^n}$. This is a contradiction as a poly. of degree d has at most d zeros in a field. $\blacksquare$

Remark. If $\mathbb{F}_{p^n}$ has a subfield of order p^m, then $m|n$. Hence there is a bijection between subfields of $\mathbb{F}_{p^n}$ and positive divisors of n.

An important tool for classifying objects is the study of their symmetries. In some sense mathematics is about finding patterns in order to simplify complex objects. One way of discribing patterns is

Lecture 27: Group of Automorphisms

Friday, June 8, 2018 10:30 PM

via maps that preserve the given pattern. Galois theory uses the same philosopy in order to study structure of a field.

<u>Def</u>. $Aut(\mathbb{F}_{p^n}) = \{\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \mid \sigma \text{ is a ring isomorphism}\}$

<u>Remark</u> $(Aut(\mathbb{F}_{p^n}), \circ)$ is a group.

(Identity) $I_{\mathbb{F}_{p^n}} \in Aut(\mathbb{F}_{p^n})$

(Inverse) $\sigma \in Aut(\mathbb{F}_{p^n}) \Rightarrow \sigma^{-1} \in Aut(\mathbb{F}_{p^n})$

(Operation) $\sigma_1, \sigma_2 \in Aut(\mathbb{F}_{p^n}) \Rightarrow \sigma_1 \circ \sigma_2 \in Aut(\mathbb{F}_{p^n})$.

- We have seen $Fr : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $Fr(\alpha) = \alpha^p$ is an isomorphism (it is called the Frobinus map.).

$$Fr^2(\alpha) = Fr(Fr(\alpha)) = Fr(\alpha^p) = (\alpha^p)^p = \alpha^{p^2}$$

and by induction $Fr^k(\alpha) = \alpha^{p^k}$. And so $Fr^n(\alpha) = \alpha^{p^n} = \alpha$

Hence $Fr^n = I$. For $m < n$, $|\{\alpha \in \mathbb{F}_{p^n} \mid Fr^m(\alpha) = \alpha\}|$

$$= |\{\alpha \in \mathbb{F}_{p^n} \mid \alpha^{p^m} - \alpha = 0\}| \leq p^m$$

And so $Fr^m \neq I$ if $1 \leq m < n$. Therefore the order of Fr is n.

Thus $\{I, Fr, Fr^2, \ldots, Fr^{n-1}\} \subseteq Aut(\mathbb{F}_{p^n})$. In fact one can

Lecture 27: Group of Automorphisms

Friday, June 8, 2018 10:51 PM

Show that $Aut(\mathbb{F}_{p^n}) = \{I, Fr, Fr^2, \ldots, Fr^{n-1}\} \simeq \mathbb{Z}_n$.

Recall that all the subgroups of $\mathbb{Z}_n$ are cyclic, and for any $m|n$ there is a unique cyclic subgp of order m. And so

$$\{\text{Subgroups of } \mathbb{Z}_n\} \rightleftarrows \{m \text{ s.t. } m|n\} \rightleftarrows \{\text{Subfields of } \mathbb{F}_{p^n}\}$$

This is a very special case of Galois theory. This type of bijec. between subfields and subgroups of auto. is part of the main theorem of Galois theory.