Finite Fields Section 33

Main Goal: Thm

Existence For every prime p and any $n > 0$ there exists a finite field of order p^n

Uniqueness If E and E' are fields of order p^n then $E \cong E'$

Structure of finite fields

A finite field F must have characteristic a prime p.

ie. $p \cdot 1 = 1 + \dots + 1 = 0$ in F

Thm 33.1 If E is a degree n extension over a finite field F with $|F| = q$, then $|E| = q^n$.

Proof. Recall E is a vector space of dim n over F. ie. $E = \{ b_1 \alpha_1 + \dots + b_n \alpha_n \mid b_i \in F \}$.

$|E| = |F|^n$. $\square$

Example $E = \mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ is a field of size $2^2 = 4$ $E = \{ a_0 + a_1\alpha \mid a_0, a_1 \in \mathbb{Z}_2 \}$

where $\alpha^2 + \alpha + 1 = 0 \Rightarrow \alpha^2 = \alpha + 1$ . . . .

Corollary 33.2 If E is a finite field with $\operatorname{char} E = p$ then E has order p^n for some $n > 0$.

Proof Every field of characteristic p contains $\mathbb{Z}_p = \{ a\cdot 1 \mid 0 \le a < p \} \subseteq E$. Hence E is a finite extension of $\mathbb{Z}_p$. Now apply 33.1 $\square$

Thm 33.3 Let E be a field with $|E| = p^n$. The elements of E are precisely the zeros in $\overline{\mathbb{Z}_p}$ of the polynomial $x^{p^n} - x$ in $\mathbb{Z}_p[x]$.

Proof $0 \in E$ is a zero of $x^{p^n} - x$.

Let E^* denote the non-zero elts. Then E^* is a group of order $p^n - 1$ under multiplication.

Recall: $g^{|G|} = 1$ for all $g \in G$.

$\Rightarrow$ $\alpha \in E^*$ satisfies $\alpha^{p^n - 1} = 1 \Rightarrow \alpha^{p^n} = \alpha \Rightarrow$ α is a zero of $x^{p^n} - x$. There are at most

p^n roots and $|E| = p^n$. Hence the elements of E are precisely the zeros of $X^{p^n} - X$. $\square$

Example $E = \dfrac{\mathbb{Z}_2[x]}{\langle x^2+x+1 \rangle}$ $[E:F] = 2$ $|E| = 4$.

let $\alpha = x + \langle x^2+x+1 \rangle$ $E = \{ a_0 + a_1\alpha \mid a_0, a_1 \in \mathbb{Z}_2 \}$

$a_0 = a_1 = 1$ $(1+\alpha)^4 + (1+\alpha) = 1 + \alpha + 1 + \alpha = 0$.

Notice also $E^* = \{1, \alpha, 1+\alpha\}$ has 3 elts. Hence cyclic!

Thm 33.5 The group $\langle F^*, \cdot \rangle$ of non-zero elements of a finite field under multiplication is cyclic.

Proof (see 23.6) $\langle F^*, \cdot \rangle$ is a finite abelian gp; hence isomorphic to $\mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_k}$ for some d_i's with $|F^*| = d_1 \cdots d_k$.

If $m = \operatorname{lcm}(d_1, \dots, d_k)$ then $\alpha^m = 1$ for all $\alpha \in F^*$. However, $x^m - 1$ has at most m distinct roots so $m = |F^*| = d_1 \cdots d_k$. Hence $\langle F^*, \cdot \rangle = \mathbb{Z}_{|F^*|}$ and it is cyclic.

Def 33.4 An element α of a field is an **n^{th} root of unity** if $\alpha^n = 1$. It is a **primitive n^{th} root of unity** if $\alpha^n = 1$ and $\alpha^m \neq 1$ $m<n$.

Previous two theorems state:

1) every $\alpha \in F^*$ $|F| = p^n$ is a $(p^n - 1)$th root of unity

2) the primitive (p^n-1)th roots of unity are the generators of $\langle F^*, \cdot \rangle$

Example $E = \mathbb{Z}_{11}$ $|E^*| = 10$ and is cyclic. Who are the generators (primitive 10^{th} roots of unity)?

Recall the order of elts must divide 10, $(1, 2, 5, 10)$

Try: 2^2 2^5 hence 2 has order 10

All other primitive 10^{th} roots of unity in E are:

$2^1 = 2$, $2^3 = 8$, $2^7 = 7$ $2^9 = 6$.

Corollary 33.6 A finite extension E of a finite field F is a simple extension $E = F(\alpha)$

Proof Let α be a generator of E^*.

Then $F(\alpha)$ contains all powers of α. (hence $p^n - 1$ elts) in addition it is a subfield of E. Hence $F(\alpha) = E$. $\square$.

Existence & Uniqueness of finite fields

Plan: Use existence of algebraic closure $\overline{\mathbb{Z}_p}$ and show zeros of $x^{p^n}-x$ form a subfield of size p^n.

Lemma 33.8 If F is a field with $\operatorname{char}(F)=p$ and alg. closure $\overline{F}$ then $x^{p^n}-x$ has p^n distinct zeros in $\overline{F}$.

Proof First 0 is a zero of $x^{p^n}-x$ with mult. 1.

Take $\alpha \neq 0$ a zero of $x^{p^n}-x$, Then $(x-\alpha)$ divides $f(x) = x^{p^n}-x$

$$\frac{X^{p^n} - X}{X - \alpha} = g(X) = X^{p^n-2} + \alpha X^{p^n-3} + \dots + \alpha^{p^n-3} X + \alpha^{p^n-2}$$

$$g(\alpha) = \alpha^{p^n-2} + \dots + \alpha^{p^n-2} = (p^n - 1)\frac{1}{\alpha} = -\frac{1}{\alpha} \neq 0$$

Hence α is a zero of multiplicity 1 of $X^{p^n} - X$.

all zeros are distinct! $\square$

Thm 83.10 A finite field $GF(p^n)$ of p^n elts exists for every prime power p^n.

Proof Let $\overline{\mathbb{Z}_p}$ be alg. closure of $\mathbb{Z}_p$. Let

$$GF(p^n) = \{ \alpha \mid \alpha^{p^n} = \alpha \quad \alpha \in \overline{\mathbb{Z}_p} \}.$$

Claim $GF(p^n)$ is a field.

1) $\alpha, \beta \in GF(p^n)$

$$(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta.$$

$\Rightarrow \quad \alpha + \beta \in GF(p^n)$

2) $\alpha, \beta \in GF(p^n)$ then $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$

$\Rightarrow \alpha\beta \in GF(p^n)$

3) $\alpha \in GF(p^n)$ then $(-\alpha)^{p^n} = (-1)^{p^n}\alpha^{p^n} = -\alpha$ if p odd.

since $(-1) = 1$ when $p = 2$ $\Rightarrow (-\alpha)^{p^n} = -\alpha$.

$\Rightarrow -\alpha \in GF(p^n)$

4) $0, 1 \in GF(p^n)$

5) $\alpha \in GF(p^n)$ then $\left(\frac{1}{\alpha}\right)^{p^n} = \left(\frac{1}{\alpha}\right) \Rightarrow \frac{1}{\alpha} \in GF(p^n)$.

Therefore $GF(p^n)$ is a field $\square$.

Corollary 33.11 If F is any finite field, then there exists an irreducible polynomial of degree n in $F[x]$ for all $n > 0$.

Proof $|F| = p^r = q$ elements. By Thm 33.10 $\exists$ a field K with q^n and $\mathbb{Z}_p \leq K \leq \overline{F}$ s.t.

$$K = \{\alpha \in \overline{F} \mid \alpha^{q^n} = \alpha\}$$

$$F = \{\beta \in \overline{F} \mid \beta^q = \beta\}$$

$\beta \in F \Rightarrow$

$$\beta^{q^n} = (\beta^q)^{q \cdots q} = \beta$$

$\Rightarrow \beta \in K$

$F \leq K$. Moreover $[K : F] = n$ and since K is simple over F of degree n. $K = F(\alpha)$ for some $\alpha \in K$ and $\mathrm{irr}(\alpha, F)$ has degree n.

D.

Thm 33.12 If E, E' are finite fields of the same order then $E \cong E'$.

Proof Suppose $|E| = |E'| = p^n$ so that $\mathbb{Z}_p \leq E, E'$ (up to isomorphism) then $E, E' \leq \overline{\mathbb{Z}_p}$ both consisting of zeros of $x^{p^n} - x$.

Notice E, E' are both simple extensions. The irreducible $f(x)$ of both extensions divides $x^{p^n} - x$.

$\square$

Example $\mathbb{Z}_3$ and $f(x) = x^2 + x + 2$, $g(x) = x^2 + 1$.

Both are irreducible / $\mathbb{Z}_3$. check!

$$E = \mathbb{Z}_3[x] / \langle f(x) \rangle = \{ a_1 \alpha + a_0 \mid a_i \in \mathbb{Z}_3 \}.$$

$$E' = \mathbb{Z}_3[x] / \langle g(x) \rangle = \{ b_1 \beta + b_0 \mid b_i \in \mathbb{Z}_3 \}.$$

$\psi(a_1 \alpha + a_0) = a_1 \beta + b_0$ is <u>not</u> an isomorphism.

$$E \longrightarrow E'$$

$$
\begin{aligned}
0 &\mapsto 0,\\
1 &\mapsto 1,\\
2 &\mapsto 2,\\
x &\mapsto x+1,\\
x+1 &\mapsto x+2,\\
x+2 &\mapsto x,\\
2x &\mapsto 2x+2,\\
2x+1 &\mapsto 2x,\\
2x+2 &\mapsto 2x+1\,.
\end{aligned}
$$