Algebra I Lecture: Splitting fields, finite fields [redacted]

13.4 - 13.5, 14.3 (13.4-13.5 next time too).

: Splitting field.

K field. $g(x) \in K[x]$ non-zero-poly.

we know: $\exists$ ext^n L/K where g has a root. [redacted]

Def^n: A splitting field for $g(x)/K$ is an ext^n L/K s.t.:

1). $g(x)$ factors completely into linear factors in $L[x]$

2). $g(x)$ doesn't factor into linear factors over any proper subfield of L.

Th^m: Splitting fields exist, are unique up to $\cong$.

Pf of existence: Induct on $n = \deg(g)$.

$n=1$: Take $L = K$.

For $n \geq 2$, we show $\exists$ ext^n E/K where g splits.

Let E_1/K be an ext^n where g has a root α

$\Rightarrow g$ factors as $(x-\alpha)g'(x)$ in E_1, $\deg(g') = n-1$

$\Rightarrow$ induction g' splits over some ext^n E of E_1 $\Rightarrow g$ splits completely / E.

For minimality, let L = intersection of all subfields of E containing K & all roots of $g(x)$.

Skip uniqueness pf. (See book!)

Th: $\varphi: F \to F'$ isom. $f \in F[x]$, E spl. field of f, E' for φf in F': $\exists E \to E'$, $F \to F'$.

Idea: $F \to F'$, $F(\alpha) \to F'(\beta)$, α root of f, β root of $\varphi(f)$, repeat $\forall$ roots.

Example of splitting field:

- $x^2-2 / \mathbb{Q}$: $\mathbb{Q}(\sqrt{2})$ deg 2
- $(x^2-2)(x^2-3)/\mathbb{Q}$: $\mathbb{Q}(\sqrt{2},\sqrt{3})$ deg 4. (bi-quad. ratio)
- $x^3-2/\mathbb{Q}$: $\mathbb{Q}(\sqrt[3]{2}, \omega)$ deg 6.

ω root of x^2+x+1

$x^3-2 = (x-\sqrt[3]{2})(x-\omega\sqrt[3]{2})(x-\omega^2\sqrt[3]{2})$

- $x^4+4/\mathbb{Q}$

$x^4+4 = (x^2+2x+2)(x^2-2x+2)$

roots: $\pm 1, \pm i$.

so $\mathbb{Q}(i)$ is a splitting field of deg 2

- $x^p-1/\mathbb{Q}$: $\mathbb{Q}(e^{2\pi i/p})$ deg $p-1$

cyclotomic

$\frac{x^{p-1}}{x-1}$ irred.

- $x^p-2/\mathbb{Q}$: $\mathbb{Q}(\sqrt[p]{2}, e^{2\pi i/p})$ deg. $p\cdot(p-1)$

Rmk: deg(splitting field) $\leq n!$ ← most common (with stats: ★★)

Indeed, adjoining one root gives deg $\leq n$, next gives deg $\leq n-1$, ... Now use multiplicativity of degrees. (I have read for Artin ext'n)

Finite fields: Finite fields have finite char $\Rightarrow$ char p $\Rightarrow$ are n-dim vector spaces over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ $\Rightarrow$ have size p^n.

We'll show: $\exists!$ field ω p^n elts.

Construction: splitting field $\mathbb{F}_p$ of $x^{p^n} - x$ / $\mathbb{F}_p$.

Differential calculus in $K[x]$: (Supposed?!)

$$F(x) = \sum_{i=0}^{n} c_i x^i \in K[x] \quad (K \text{ Field}), \quad F'(x) := \sum_{j=1}^{n} j c_j x^{j-1}.$$

Lemma: $(GH)' = G'H + GH'$

Pf: Enough to prove for monomials.

$G(x) = x^m$, $H(x) = x^n$. Check that it works!

$$(x^m x^n)' = (m+n)x^{m+n-1} \stackrel{?}{=} m x^{m-1+n} + n x^{m+n-1}$$

Cor: $\frac{d}{dx}(x-r)^n = n(x-r)^{n-1}$

Cor: $(x-r)^2$ divides $F[x]$ $\iff$ double root.

$F(r) = F'(r) = 0$.

Pf: If $F(r) = F'(r) = 0$, then

$$(x-r) \mid F(x) \Rightarrow F(x) = (x-r)G(x)$$

$$\Rightarrow F'(x) = (x-r)G(x) + (x-r)G'(x)$$

$$\Rightarrow G(r) = 0 \Rightarrow (x-r) \mid G(x) \Rightarrow (x-r)^2 \mid F(x).$$

Conversely, suppose $F(x) = (x-r)^2 G(x)$.

Then $F'(r) = 0$. Differentiate:

$$F'(x) = 2(x-r)G(x) + (x-r)^2 G'(x)$$

$$\Rightarrow F'(r) = 0 \quad \text{Pf}$$

Frobenius map:

Lemma: If K is a field of char p, the map $\varphi(x) = x^p$ is an injective hom. from K to itself.

Pf: $(ab)^p = a^p b^p$, $(a+b)^p = a^p + b^p$, injective automatic from $\varphi(1) = 1$.
(last $\neq$ b/w fields, not $=0$) ■

Cor: If F is a finite field, of char p, $\varphi(x) = x^p$ is an automorphism of F (perfect field = φ is surjective)
Pf: injective from a finite set to itself!

Existence of finite field of order p^n.

Let $q = p^n$. $n \geq 1$. p prime.

Let K = splitting field of $x^{p^n} - x$ / $\mathbb{F}_p$.

Since $\frac{d}{dx}(x^{p^n} - x) = -1 \neq 0$, $x^{p^n} - x$ factors into distinct linear factors / K.

Thus, $x^{p^n} - x$ has p^n distinct roots in K.

Claim: The roots of $x^{p^n} - x$ in K form a subfield F of K.

Indeed, if α, β are any two roots, $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$
$\Rightarrow (\alpha\beta)^{p^n} = \alpha\beta$, $(\alpha+\beta)^{p^n} = \alpha+\beta$, $(\alpha^{-1})^{p^n} = \alpha^{-1}$.
Clearly, $|F| = p^n$. By minimality of splitting field $F = K$.
(4)

Uniqueness: F finite field of order p^n (char p)

$\Rightarrow |F^\times| = p^n - 1 \Rightarrow \alpha^{p^n - 1} = 1 \quad \forall \alpha \neq 0$ in F

(it's a gp!)

$\Rightarrow \alpha^{p^n} = \alpha \quad \forall \alpha \in F \Rightarrow \alpha$ is a root of $x^{p^n} - x \Rightarrow$

$F \subseteq$ splitting field of $x^{p^n} - x$, which has a set of p^n (we showed)

Follows by uniqueness of splitting fields. ☐

Call this field $\mathbb{F}_{p^n}$.

Remarks:

1). Every finite field $\mathbb{F}$ with $|\mathbb{F}| = p^n$ is $\cong$ to $\mathbb{F}_p[x]/(g(x))$ for some irred. poly $g \in \mathbb{F}_p[x]$ of deg. n, and conversely.

pf: Show $\mathbb{F}/\mathbb{F}_p$ is a simple ext^n.

$\mathbb{F}^\times$ cyclic $\rightsquigarrow$ let $\mathbb{F}^\times = \langle \pi \rangle$, $|\pi| = p^n - 1$.

$\mathbb{F}$
|
$\mathbb{F}' = \mathbb{F}_p(\pi)$
|
$\mathbb{F}_p$

If $d < n$, $|(\mathbb{F}')^\times| = p^d - 1$
$\Rightarrow \pi^{p^d - 1} = 1$ *.

2). $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ iff. $m \mid n$. (see HW)

Pf. uses (can) R comm. ring w/ 1, $a \in R$, $m, n \geq 1$,
(we'll skip) then $(a^m - 1, a^n - 1) = (a^d - 1)$
where $d = \gcd(m, n)$.

Cyclotomic : field.

$x^n - 1$ / $\mathbb{Q}$.

Splitting field: $\mathbb{Q}(e^{2\pi i/n})$.

Sol^{n} / $\mathbb{C}$: ζ_n^k $k \in \mathbb{Z}$.

orsrdln roots of unity

$\zeta_n = e^{2\pi i/n}$.

A generator of the n^{th} order roots of unity is a primitive n^{th} order r.o.u.

they are ζ_n^a, a rel. prime to n.

prim. $\varphi(n)$. (Euler φ)

$n = p$: $x^p - 1 = (x+1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$

ζ_p root of $\frac{x^p - 1}{x+1} = \Phi_p(x)$., irred. $\Rightarrow$

$\Phi_p(x)$ is the min poly of ζ_p / $\mathbb{Q}$ $\Rightarrow [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$

More generally, it's true that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

n^{th} cyclotomic poly

$\Phi_n(x) = \prod_{\substack{1 \le a \le n \\ (a,n)=1}} (x - \zeta_n^a)$

Roots are the primitive n^{th} order roots of unity, so degree $= \varphi(n)$.

A priori, $\Phi_n(x) \in \mathbb{C}[x]$.

Lemma: $\Phi_n \in \mathbb{Z}[x]$.

Pf: Strong induction on n; $n = 1$ ✓.

Assume true $\forall\, m < n$. $x^n - 1 = \prod_{1 \le a \le n} (x - \zeta_n^a) = \prod_{d \mid n} \Phi_d(x)$

$= \Phi_n(x) \cdot \prod_{\substack{d \mid n \\ d < n}} \Phi_d(x) = \Phi_n(x) \cdot h(x)$ By induction, $h \in \mathbb{Z}[x]$

By long division, $\Phi_n(x) \in \mathbb{Q}[x]$

By Gauss' Lemma, $\Phi_n \in \mathbb{Z}[x]$