Groups & Rings: Lecture #24

Finite fields (§22.1)

- Separability
- Characteristic p
- Derivatives
- Finite fields
- Properties of finite fields

Separability

Def: • A polynomial $p(x) \in F[x]$ is separable if its roots in a splitting field are all distinct. Otherwise inseparable.

• If E/F is a field extension, then an element $\alpha \in E$ is separable if its minimal polynomial is separable. Otherwise inseparable.

• A field extension E/F is separable if every $\alpha \in E$ is separable. Otherwise inseparable. The extension E/F is purely inseparable if every $\alpha \in E \setminus F$ is inseparable.

Ex: $E = \mathbb{Q}(\sqrt{D})$ (D sq-free integer).

• $\alpha = \sqrt{D}$ separable element because minimal polynomial $p(x) = x^2 - D = (x-\sqrt{D})(x+\sqrt{D})$ has two distinct roots $\pm\sqrt{D}$.

• $E/\mathbb{Q}$ is separable field extension because if $\alpha = a + b\sqrt{D}$ then

$$\begin{aligned} p(x) = (x-\alpha)(x-\bar{\alpha}) &= \left(x-(a+b\sqrt{D})\right)\left(x-(a-b\sqrt{D})\right) \\ &= (x-a)^2 - b^2 D = x^2 - 2ax + a^2 - b^2 D \\ &= x^2 - tr(\alpha)x + N(\alpha) \in \mathbb{Q}[x] \end{aligned}$$

is a polynomial vanishing at α. Moreover

- $p(x)$ inseparable (repeated roots) $\iff \alpha = \bar{\alpha} \iff b = 0$
  $\Rightarrow p_{min}(x) = x - a$ separable
- $p(x)$ separable $\iff b \neq 0 \Rightarrow p_{min}(x) = p(x)$ separable

So α is separable $\forall \alpha \in E$.

Fact: (not in book) If $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$, then

E/F separable $\iff \alpha_1, \dots, \alpha_n$ separable.

Characteristic p

Lem 22.3: (Freshman's dream) If R ring with $p=0$ (p prime) then
(i) $(a+b)^p = a^p + b^p \quad \forall a,b \in R$
(ii) $(a+b)^q = a^q + b^q \quad \forall a,b \in R,\ q = p^n\ \forall n$

pf: (i) $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} \overset{\uparrow}{=} a^0 b^p + a^p b^0 = a^p + b^p$

$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \begin{cases} p(\cdots) & k=1,2,\dots,p-1 \\ 1 & k=0 \text{ or } k=p \end{cases}$

(ii) Use (i) repeatedly. $\square$

Consequence: When $p=0$ in R, we have a ring homomorphism, the Frobenius: $\mathrm{Frob}: R \to R,\ a \mapsto a^p$

Rmk: If F field of char p, then $F^p = \{x^p : x \in F\}$ is a subfield, and $\mathrm{Frob}: F \to F^p$. Often $F^p = F$.

$F^p \subset F \xrightarrow[(\text{inj})]{} F^p$ (composition usually not identity)

Ex: Let F be a field of char p. Then $x^p - a \in F[x]$ is inseparable b/c if α root in splitting field E, then $\alpha^p = a$ so $(x-\alpha)^p = x^p - \alpha^p = x^p - a$.

Ex: $F = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Then $x^2 - 1 = (x - \sqrt{1})(x + \sqrt{1})$
but $-1 = +1$ in $\mathbb{F}_2 \Rightarrow x^2 - 1 = (x - \sqrt{1})^2 = (x-1)^2$

Ex: $F = \mathbb{F}_p(t) = \{\frac{f(t)}{g(t)} : f, g \in \mathbb{F}_p[t], g \neq 0\}$ rational functions
$p(x) = x^p - t$ irreducible and inseparable: $p(x) = (x - t^{1/p})^p$.
$\mathbb{F}_p(t) \subset \mathbb{F}_p(t^{1/p})$ purely inseparable extension.

Derivatives

Def: Let $p(x) = \sum_{d=0}^{n} a_d x^d \in F[x]$. Then the derivative of $p(x)$ is

$$p'(x) := \sum_{d=1}^{n} d a_d x^{d-1} \in F[x]$$

Exc:
- $D: F[x] \longrightarrow F[x]$ is a group homomorphism (not a ring homo.)
  $p(x) \longmapsto p'(x)$
- Leibniz rule: $D(pq) = p'q + pq'$
- $\ker D = \{\sum_{d=0}^{n} a_d x^d : d a_d = 0 \ \forall d\}$
  (char $F=0$) $= \{\text{constant polynomials}\} = F$ $\qquad$ ($d>0$, $d a_d = 0 \Rightarrow a_d = 0$)
  (char $F = p$) $= \{\sum_{d=0}^{n} a_d x^d : a_d = 0 \text{ if } p \nmid d\} = F[x^p]$

Ex: $(x^9 - 2x^3)' = 0$ in char 3.

Lem 22.5: $f \in F[x]$ is separable $\iff$ f, f' are relatively prime

Lemma (missing in the book): Let E/F field ext., $f, g \in F[x]$. Then

f, g are relatively prime in $F[x]$
$\iff$ f, g are relatively prime in $E[x]$.

pf: $\Leftarrow$ If $d \mid f$, $d \mid g$, $d \in F[x]$ then $f = dp$, $g = dq$ in $F[x]$ and $E[x]$.
$\Rightarrow$ If f, g are rel. prime in $F[x]$, then $1 = af + bg$ (Euclid's algo) with $a, b \in F[x]$. This relation also holds in $E[x]$ so f, g are also rel. prime in $E[x]$. $\square$

pf of Lem 22.5: By Lemma, can replace F by splitting field of f. Thus, $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ $\alpha_i \in F$.

f and f' have a common factor $\iff$ f and f' have a common root

$\iff f'(\alpha_i) = 0$ for some i

$$f'(x) = \sum_{i=1}^{n} \frac{f(x)}{x-\alpha_i} \qquad \iff \alpha_i \text{ repeated root for some } i$$

Leibniz rule

$$f'(\alpha_i) = \left(\frac{f(x)}{x-\alpha_i}\right)\Big|_{x=\alpha_i} + 0 = 0 \iff \alpha_i \text{ is a repeated root.}$$

□

Prop 23.11: Let $f(x) \in F[x]$ be irreducible.

(i) If char $F = 0$, then $f(x)$ is separable.

(ii) If char $F = p$, then $f(x)$ inseparable $\iff f(x) = g(x^p)$

pf: We have that f separable $\underset{\text{Lem 22.5}}{\iff}$ f, f' relatively prime

Since f is irreducible and $\deg f' \leq \deg f - 1$, this is equivalent to $f' \neq 0$. This implies that (see prev. page)

(char $F = 0$) f constant $\Rightarrow$ contradicts f irreducible

(char $F = p$) $f(x) = g(x^p)$ □

Finite fields

Recall (Prop 22.1 – 22.2): Suppose F is a finite field.

(i) $n = 1+1+\cdots+1 \in F$ zero for some $n \Rightarrow \operatorname{char} F \neq 0$

$\Rightarrow \operatorname{char} F = p$ for some prime p.

(ii) $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \longrightarrow F$. $\quad \underline{\mathbb{F}_p} \subset F$ field ext.
$\quad\quad 1 \longmapsto 1$

prime field

(iii) $|F| = |\mathbb{F}_p|^{[F:\mathbb{F}_p]} = p^n = q$.

Thm 22.6: Let p be a prime number and $n \in \mathbb{Z}_+$.

- There exists a unique field of order p^n. (unique up to non-unique isom.)
- This field is a splitting field of $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.

Def: $\mathbb{F}_{p^n} = \mathbb{F}_q$ is "the" field of $q = p^n$ elements.

(also called $GF(q)$, the Galois field w/ q elements)

pf: **Existence**: Let F be the splitting field of $f(x)$.
Need to prove that $|F| = p^n$.

- f is separable, b/c $f'(x) = D(x^{p^n} - x) = p^n x^{p^n - 1} - 1 = -1$
  so roots of f are distinct.
- Let $S = \{\alpha \in F : f(\alpha) = 0\} = \{\alpha \in F : \alpha^q = \alpha\}$ (a subset of F)
  Then $|S| = \deg f = p^n$.
- Recall $F = \mathbb{F}_p(S)$ smallest field containing S.
  Need to prove that S is a field ($\Rightarrow S = F$)

• S is a field:

– $0^q = 0 \Rightarrow 0 \in S$

$1^q = 1 \Rightarrow 1 \in S$

– $\alpha, \beta \in S \Rightarrow \boxed{\alpha^q = \alpha,\ \beta^q = \beta}$

Freshman's dream

$\Rightarrow (\alpha+\beta)^q = \alpha^q + \beta^q = \alpha + \beta \quad \Rightarrow \alpha+\beta \in S$

$\Rightarrow (\alpha\beta)^q = \alpha^q \beta^q = \alpha\beta \quad \Rightarrow \alpha\beta \in S$

$\Rightarrow (-\alpha)^q = (-1)^q \alpha^q = (-1)\alpha = -\alpha \quad \Rightarrow -\alpha \in S$

(if $\alpha \neq 0$) $\Rightarrow (1/\alpha)^q = 1/\alpha^q = 1/\alpha \quad \Rightarrow \alpha^{-1} \in S$

Uniqueness: Suppose E is a field with p^n elements.

Note that $E^\times = E \setminus \{0\}$ is a group (under mult.) of order $p^n - 1$.

$\Rightarrow |a| \mid p^n - 1 \quad \forall a \in E^\times$, that is, $a^{p^n - 1} = 1 \quad \forall a \in E^\times$

Lagrange's thm

~ Euler's thm

$\Rightarrow a^{p^n} = a \quad \forall a \in E$

Fermat's little thm

Thus, every element of E is a root of $f(x) = x^{p^n} - x$.

$\Rightarrow E$ is a splitting field of $f(x)$

$\Rightarrow E \cong F$ $\square$

Thm 21.33 (splitting fields are unique)

Ex: $n=1$, $f(x) = x^p - x = x(x-1)(x-2)\cdots(x-(p-1))$

$S = \{0, 1, 2, \ldots, p-1\} = \mathbb{F}_p$.

Ex: $f(x) = x^3 + x + 1$ in $\mathbb{F}_2[x]$, deg 3, no roots $\Rightarrow$ irreducible

$F = \mathbb{F}_2[x]/(x^3+x+1)$ field with 2^3 elts so $F \cong \mathbb{F}_8 \cong \text{split}(x^8 - x)$.

Properties of finite fields

Thm 22.10: If G is a finite subgroup of $F^\times$ for any field F, then G is cyclic.

pf: Let $N = \operatorname{lcm}\{|a| : a \in G\}$ (the "exponent" of G). Then $N \mid |G|$ and $a^N = 1$ $\forall a \in G$. Thus every $a \in G$ is a root of $f(x) = x^N - 1$ $\Rightarrow$ $N = |G|$.

Since G is finite abelian, $G \cong \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_r^{e_r}$ and $|G| = p_1^{e_1} \cdots p_r^{e_r}$ and $N = \operatorname{lcm}(p_1^{e_1}, \ldots, p_r^{e_r})$.

Now $N = |G| \iff$ the p_i are distinct $\iff$ G cyclic. $\square$

Cor 22.11: $\mathbb{F}_q^\times$ is cyclic. $\left(\iff \exists \alpha \in \mathbb{F}_q^\times \text{ s.th. } \mathbb{F}_q^\times = \langle \alpha \rangle \text{ that is: } \forall \beta \in \mathbb{F}_q^\times\ \exists n : \beta = \alpha^n \right)$

α is called a primitive element — not so easy to find!

Best case: $\mathbb{F}_q = \mathbb{F}_p[x]/(p(x))$ — $p(x)$ irreducible and $\alpha = \bar{x} = x + (p(x))$ is primitive.

Such $p(x)$ called primitive polynomial and always exist.
(The minimal polynomial of a primitive element is a primitive polynomial.)

Thm 22.7: If $E \subseteq \mathbb{F}_{p^n}$ subfield, then $|E| = p^m$ and $m \mid n$.
Conversely, if $m \mid n$, then $\exists$ unique subfield $E \subseteq \mathbb{F}_{p^n}$ with p^m elts

$$\begin{tikzcd}
 & \mathbb{F}_{p^2} \arrow[r, phantom, "\subset"] \arrow[d, phantom, "\cap"] & \mathbb{F}_{p^4} \arrow[r, phantom, "\subset"] & \mathbb{F}_{p^8} & \subset \\
\mathbb{F}_p \arrow[ur, phantom, "\subset"] \arrow[r, phantom, "\subset"] \arrow[d, phantom, "\cap"] & \mathbb{F}_{p^3} \arrow[r, phantom, "\subset"] & \mathbb{F}_{p^6} & & \overline{\mathbb{F}_p} \\
\mathbb{F}_{p^5} & & & & \subset
\end{tikzcd}$$

$\overline{\mathbb{F}_p}$ alg. closure of $\mathbb{F}_p$ (infinite)