- F končno polje. $\forall n \in \mathbb{N}. \exists p(x) \in F[x]. st(p(x)) = n$
- $p \nmid a_n$. $p(x)$ neraz nad $\mathbb{Z}_p \Rightarrow p(x)$ neraz. nad $\mathbb{Q}$
- Eisensteinov test:

  $p \mid a_{n-1}, \dots a_n \quad p \nmid a_n \quad p^2 \nmid a_0$

  $\Rightarrow f(x)$ ni razcepen nad $\mathbb{Q}$
- $st(p(x)) = 2 \vee 3 \Rightarrow (p(x)$ nerazc. $\Leftrightarrow \forall x \in F. p(x) \neq 0$
- Primitivni polinom: $a_n \dots a_0$ so tuja
- produkt primitivnih polinomov je primitiven
- $p(x)$ je minimalni polinom $\Longleftrightarrow p(x)$ je nerazcepen nad $F \Leftrightarrow p(x)$ deli vsak polinom z ničlo v

K/F K je vektorski prostor nad F
$[K:F] = \dim_F K$

- L/F, K/L končni razširitvi $\Rightarrow$ K/F končna razširitev
  velja: $[K:F] = [K:L] \cdot [L:F]$

- končna razširitev $\Rightarrow$ algebraična razširitev
- primitivna razširitev: $\exists a \in K.\ K = F(a)$
  " enostavna
- $a \in K$ algebraičen stopnje n $\Rightarrow$ $F(a) = F[a]$
  $[F(a):F] = n$

- K/F: $\{a \in K ; a \text{ je alg. nad } F\}$ je podpolje v K

- a, b alg: razširitvi sta tuji $\Rightarrow [F(a,b):F] = [F(a):F] \cdot [F(b):F]$

- $F(a^k, a^l) = F(a^{D(k,l)})$

- $[F:F(b)] = m \Rightarrow \exists p(x) \in F[x]$ nerazc. $p(b) = 0$
  $st(p(x)) = m$
- $F(a,b) \leq F(a) \cdot F(b)$

- $p(x)$ nerazc. $\Rightarrow st(p(x)) \mid [E:F] \wedge [E:F] \leq st(p(x))!$

- končna separabilna razširitev je enostavna
- polje je perfektno, če je vsaka končna razširitev separabilna

- $\operatorname{char} F = 0 \Rightarrow F$ je perfektno
- $|F| < \infty \Rightarrow F$ je perfektno

- Razpadno polje $p(x)$... najmanjše polje, ki vsebuje vse ničle $p(x)$ $E = F(a_1, \dots, a_n)$

- Galoisova razširitev - normalna, separabilna
- $p(x)$ je seperabilen če so njegove ničle v poljubni razširitvi polja enostavne (stopnje 1)

- K/F algebraična razširitev je separabilna če za $\forall a \in K$ je minimalni polinom a-ja nad F je seperabilen
- K/F je normalna, če za $\forall p(x)$ nerazcepen velja da ima vse ničle v K ali pa nobene

- K/F končna razširitev $\Rightarrow$ (K/F normalna $\Leftrightarrow$ K razpadno polje)

- $F \subseteq L \subseteq K$. L/F algebraična. $a \in K$ algebraičen nad K $\Rightarrow$ a algebraičen nad F

- Algebraično zaprtje $\overline{F}$. $F \subseteq \overline{F}$ in $\overline{F}/F$ algebraična ($\Leftrightarrow$ najmanjše alg. zaprto polje, ki vsebuje F)
$F \subseteq A$; A alg. zaprto polje. $\overline{F} = \{a \in A; a \text{ alg. nad } F\}$

- Karakteristika polja n: $n \cdot 1 = 0$
  ($\operatorname{char} F = 0$ če $\nexists n,\ n \cdot 1 = 0$)

- K končno polje $\Rightarrow \operatorname{char} K = p;\ p \in \mathbb{P}$ $(\underset{\text{podpolje}}{\mathbb{Z}_p} \subseteq K)$
  $|K| = p^n$
- $|K| = p^n \Leftrightarrow K$ razpadno polje za $x^{p^n} - x \in \mathbb{Z}_p[x]$
- $\forall p \in \mathbb{P}.\ n \in \mathbb{N}.\ \exists! K$ polje. $|K| = p^n$
- $x^{p^n} - x = \prod_{a \in GF(p^n)} (x-a) = (x-a_1) \cdots\cdots (x-a_{p^n})$

- Končen obseg je polje (Wedderburnov izrek)
- Multiplikativna grupa konč. polja je ciklična

- $\operatorname{char} F = 0$, $p(x)$ nerazc. poljubna ničla je enostavna v vsaki razširitvi

- $\operatorname{char} F = 0$, K raz. polje $f(x) \in F[x] \Rightarrow K/F$ Galoisova
- $\forall K \supseteq \mathbb{Z}_p.\ K/\mathbb{Z}_p$ galoisova

- $F \subseteq L \subseteq K$:

  K/F končna/normalna/seperabilna $\Rightarrow$
  1) K/L končna/normalna/seperabilna
  2) L/F končna/~~normalna~~/seperabilna

- $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + \beta c)$

  $c \in \mathbb{Q} \quad c \neq \dfrac{\alpha_i - \alpha_1}{\beta_j - \beta_1} \quad j \neq 1$

  $\beta_1, \dots, \beta_n$ ničle min. polinoma za β
  $\alpha_1, \dots, \alpha_m$ ničle min. polinoma za

- $\mathrm{Gal}(K/F) = \{\sigma : \sigma|_F = id_F\} \leq \mathrm{Aut}(K)$

  ↖ F-automorfizem

- G/F končna, galoisova $\Rightarrow |\mathrm{Gal}(K/F)| = [K:F]$

- $\mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Aut}(F)$, ker automorfizmi pustijo $\mathbb{Q}$ nemi...
- $\mathrm{Gal}(F/K) \leq S_n$; n stopnja minimalnega polinoma