

**algebarski element** Neka je  $F$  polje i  $E$  neko proširenje tog polja. Za element  $\alpha \in E$  kažemo da je algebarski nad  $F$  ako postoji nenul polinom  $f \in F[X]$  takav da je  $f(\alpha) = 0$ . Proširenje polja  $E/F$  je algebarsko ako je svaki element od  $E$  algebarski nad  $F$ .

**algebarski zatvarač** Polje  $\Omega$  je algebarski zatvarač potpolja  $F$  ako je algebarski zatvoreno (vidi definiciju) i algebarsko nad  $F$ .

**algebarski zatvoreno polje** Polje  $\Omega$  je algebarski zatvoreno ako zadovoljava sljedeće ekvivalentne uvjete:

- 1) svaki nekonstantan polinom iz  $\Omega[X]$  se cijepa u  $\Omega[X]$  (vidi definiciju),
- 2) svaki nekonstantni polinom u  $\Omega[X]$  ima barem jedan korijen u  $\Omega$ ,
- 3) ireducibilni polinomi u  $\Omega[X]$  su polinomi stupnja jedan,
- 4) svako polje konačnog stupnja nad  $\Omega$  (vidi definiciju) je jednako  $\Omega$ .

*Primjer:* Polje kompleksnih brojeva  $\mathbb{C}$  je algebarski zatvoreno, vidi "fundamentalni teorem algebre".

### algoritam

**za dijeljenje polinoma** Algoritmom za djeljenje polinoma nazivamo sljedeću tvrdnju: ako su dani  $f(X)$  i  $g(X) \in F[X]$  t.d.  $g \neq 0$ , onda postoje  $q(X), r(X) \in F[X]$  t.d. je stupanj od  $r$  manji od stupnja od  $q$  i vrijedi

$$f = gq + r.$$

Nadalje,  $q$  i  $r$  su jedinstveno određeni sa  $f$  i  $g$ .

**Euklidov** Neka su  $f$  i  $g$  elementi od  $F(X)$  i neka je njihov najveći zajednički djelitelj polinom  $d(X) \in F[X]$ . Euklidov algoritam konstruira polinome  $a(X)$  i  $b(X)$  takve da

$$a(X) \cdot f(X) + b(X) \cdot g(X) = d(X), \quad st(a) < st(g) \quad \text{ i } \quad st(b) < st(f)$$

koristeći algoritam za djeljenje polinoma.

**za faktORIZACIJU polinoma** Polinom  $f \in \mathbb{Q}[X]$  možemo faktorizirati na sljedeći način: prvo ga množimo sa odgovarajućim cijelim brojem  $c$  da dobijemo normirani polinom, tj. tako da je  $cf$  oblika

$$cf(X) = X^m + a_1 X^{m-1} + \dots + a_m, \quad a_i \in \mathbb{Z}.$$

Fundamentalni teorem algebre (vidi pod "fundamentalni teorem algebre") kaže da se  $cf$  potpuno cijepa u  $\mathbb{C}[X]$ :

$$cf(X) = \prod_{i=1}^m (X - \alpha_i), \quad \alpha_i \in \mathbb{C}.$$

Iz jednakosti

$$0 = f(\alpha_i) = \alpha_i^m + a_1 \alpha_i^{m-1} + \dots + a_m$$

slijedi da je  $|\alpha_i|$  manje od neke ograde koja ovisi samo o stupnju i koeficijentima polinoma  $cf$ . Ako je sada  $g(X)$  normirani faktor od  $cf(X)$ , onda su njegovi korjeni neki od  $\alpha_i$ -ova, a koeficijenti tog polinoma  $g$  su simetrični polinomi u njegovim korjenima. Stoga su koeficijenti od  $g(X)$  ograničeni s obzirom na stupanj i koeficijente od  $cf(X)$ , dakle, za  $g$  ima samo konačno mnogo kombinacija. Ispitujemo te kombinacije jednu po jednu i dobivamo faktORIZACIJU. Ovaj postupak može se primjeniti i ako je  $f(X) \in \mathbb{F}_p[x] = (\mathbb{Z}/p\mathbb{Z})[X]$ .

**Artinova propozicija** Neka je  $G$  konačna grupa automorfizama polja  $E$  i neka je  $F$  fiksno potpolje od  $G$  u  $E$ ,  $F = E^G$  (vidi definicije). Onda je stupanj od  $E$  nad  $F$  manji ili jednak redu grupe  $G$ , tj.  $[E : F] \leq (G : 1)$  (vidi definicije).

**automorfizam** Neka su dana polja  $E \supset F$ ,  $E' \supset F$ .  $F$ -izomorfizam je izomorfizam  $\varphi : E \longrightarrow E'$  takav da  $\varphi(\alpha) = \alpha$  za svako  $\alpha \in F$ .  $F$ -izomorfizam sa  $E \longrightarrow E$  još nazivamo i  $F$ -automorfizam od  $E$ .  $F$ -automorfizmi od  $E$  čine grupu (s obzirom na kompoziciju funkcija kao operaciju) koju označavamo sa  $\text{Aut}(E/F)$ .

**biracionalan** Grupu  $\text{Aut}(\mathbb{C})/\mathbb{C}$  nazivamo grupom biracionalnih automorfizama  $n$ -dimenzionalne Riemannove sfere  $\mathbb{P}_{\mathbb{C}}^n$ . Ta se grupa još zove i Cremona-grupa.

**cijepanje** Neka je  $F$  neko polje. Polinom  $f$  se cijepa u  $F[X]$  ako je  $f$  produkt polinom stupnja jedan u  $F[X]$  (vidi "algebarski zatvoreno polje" za opis polja polinoma u kojima se svaki polinom iz tog polja cijepa).

**ciklotomski polinomi** Polinom  $X^n - 1$  ima neke očite faktore u  $\mathbb{Q}$ , naime, polinome oblika  $X^d - 1$  za svako  $d|n$ . Iz rastava od  $X^n - 1$  sada izbacimo one linearne faktore koji su linearni faktori od  $X^d - 1$  za  $d|n$  za sve  $d < n$ . Na primjer, za  $X^4 - 1$  imamo rastav  $X^4 - 1 = (X - 1)(X + 1)(X^2 + 1)$  i tu izbacujemo faktore  $(X - 1)$  (dijeli  $X - 1$ , a 1 dijeli 4) i  $(X + 1)$  (dijeli  $X^2 - 1$ , a 2 dijeli 4). Dobiveni polinom zove se  $n$ -ti ciklotomski polinom  $\Phi_n$ . U slučaju  $X^4 - 1$  to je očito  $X^2 + 1$ . Stoga je

$$\Phi_n(X) = \prod (X - \zeta), \quad \text{produkt po svim primitivnim } n\text{-tim korjenima jedinice.}$$

Lako se pokaže da vrijedi:

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Na primjer,  $\Phi_1(X) = X - 1$ ,  $\Phi_2(X) = X + 1$ ,  $\Phi_3(X) = X^2 - X + 1$  itd.

**diskriminanta** Neka je zadan polinom

$$f(X) = X^n + a_1 X^{n-1} + \dots + a_n$$

i neka  $f(X) = \prod_{i=1}^n (X - \alpha_j)$  u nekom polju cijepanja od  $f$  (vidi definiciju). Definiramo

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j), \quad D(f) = \Delta(f)^2 = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Broj  $D(f)$  zovemo diskriminanta polinoma  $f$ . Primjetimo da je  $D(f) \neq 0$  ako i samo ako  $f$  ima samo proste korjene, tj. ako je  $f$  separabilan bez višestrukih faktora. Diskriminanta od  $f$  može se izraziti kao univerzalni polinom u koeficijentima od  $f$ . Na primjer:

$$\begin{aligned} D(aX^2 + bX + c) &= b^2 - 4ac, \\ D(X^3 + bX + c) &= -4b^3 - 27c^2. \end{aligned}$$

**fiksno polje** Neka je  $G$  grupa homomorfizama polja  $E$ . Definiramo podskup od  $E$ :

$$E^G = \text{Inv}(G) = \{\alpha \in E \mid \sigma\alpha = \alpha \text{ za sve } \sigma \in G\}.$$

Taj podskup je potpolje od  $E$  koje nazivamo potpoljem  $G$ -invarijantata od  $E$  ili fiksnim poljem od  $G$ .

**Frobeniusov**

**endomorfizam** Neka je polje  $F$  karakteristike  $p$  (vidi definiciju). U tom slučaju vrijedi:

$$(a + b)^p = a^p + b^p.$$

Stoga je preslikavanje  $a \mapsto a^p$  homomorfizam  $F \longrightarrow F$  koji nazivamo Frobeniusov endomorfizam.

**automorfizam** Ako je polje  $F$  konačno, onda je Frobeniusov endomorfizam (vidi gore) izomorfizam kojeg nazivamo Frobeniusov automorfizam.

### fundamentalni teorem

**algebre** Fundamentalni teorem algebre prvi je rigorozno dokazao Gauss oko 1816. Teorem glasi: polje  $\mathbb{C}$  kompleksnih brojeva je algebarski zatvoreno (vidi definiciju), tj. svaki nekonstantni polinom iz  $\mathbb{C}[X]$  ima barem jednu nultočku u  $\mathbb{C}$ .

**Galoisove teorije** Neka je  $E$  Galoisovo proširenje od  $F$  i  $G = \text{Gal}(E/F)$  njegova Galoisova grupa (vidi definiciju). Preslikavanja  $H \mapsto E^H$  (koje podgrupe  $H$  od  $G$  pridružuje njeno fiksno potpolje u  $E$  (vidi definiciju)) i  $M \mapsto \text{Gal}(E/M)$  (koje potpolju od  $E$  pridružuje njegovu Galoisovu grupu) su inverzne bijekcije između skupa svih podgrupa od  $G$  i skupa svih međupolja od  $F$  i  $E$ :

$$\{ \text{podgrupe od } G \} \longleftrightarrow \{ \text{međupolja } F \subset M \subset E \}.$$

Nadalje,

- (a) ta bijekcija okreće inkluzije, tj.  $H_1 \supset H_2 \iff E^{H_1} \subset E^{H_2}$ ;
- (b) indeksi su jednaki stupnjevima:  $(H_1 : H_2) = [E^{H_2} : E^{H_1}]$ ;
- (c)  $\sigma H \sigma^{-1} \leftrightarrow \sigma M$ , tj.  $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$ ;  $\text{Gal}(E/\sigma M) = \sigma \text{Gal}(E/M) \sigma^{-1}$ ;
- (d)  $H$  je normalna u  $G \iff E^H$  je normalno (stoga i Galoisovo) nad  $F$ , i u tom slučaju

$$\text{Gal}(E^H/F) = G/H.$$

**Galoisova grupa** Neka je  $F$  polje. Konačno proširenje  $E$  od  $F$  je Galoisovo ako je  $F$  fiksno polje (vidi definiciju) grupe  $F$ -automorfizama od  $E$ . Ta grupa se onda zove Galoisova grupa od  $E$  nad  $F$  i označava sa  $\text{Gal}(E/F)$ . Za proširenje  $E/F$  ekvivalentno je:

- (a)  $E$  je polje cijepanja separabilnog polinoma  $f \in F[X]$ ;
- (b)  $F = E^G$  za neku konačnu grupu  $G$  automorfizama od  $E$ ;
- (c)  $E$  je normalno, separabilno i konačnog stupnja nad  $F$ ;
- (d)  $E$  je Galoisovo nad  $F$ .

**polinoma** Ako je polinom  $f \in F[X]$  separabilan (vidi definiciju), onda je njegovo polje cijepanja (vidi definiciju)  $F_f$  Galoisovo nad  $F$  (vidi gore). U tom slučaju Galoisovu grupu  $\text{Gal}(F_f/F)$  zovemo Galoisova grupa  $G_f$  od  $f$ .

**Galoisovo polje** Konačna polja (vidi definiciju) su se nekad zvala Galoisova polja.

**Galoisov zatvarač** Neka je  $E$  Galoisovo proširenje od  $F$  i neka je  $G$  pripadna Galoisova grupa (vidi definiciju). Neka je, nadalje,  $H$  podgrupa od  $G$  i neka je  $M = E^H$  fiksno polje od  $H$  (vidi definiciju). Može se pokazati da je najveća normalna podgrupa sadržana u  $H$  oblika  $N = \cap_{\sigma \in G} \sigma H \sigma^{-1}$  i stoga je  $E^N$  najmanje normalno proširenje (vidi definiciju) od  $F$  koje sadrži  $M$ . Zovemo ga normalni ili Galoisov zatvarač od  $M$  u  $E$ .

**Gaussovi brojevi** Gaussovim brojevima nazivamo elemente polja

$$\mathbb{Q}(i) = \{ a + bi \in \mathbb{C} \mid a, b \in \mathbb{Q} \}.$$

Polje Gaussovih brojeva je stupnja dva nad  $\mathbb{Q}$  (vidi definiciju) sa bazom  $\{1, i\}$ .

**$G$ -modul** Neka je  $G$  (konačna) grupa.  $G$ -modul je abelova grupa  $M$  zajedno sa djelovanjem od  $G$  na  $M$ , tj. sa zajedno sa preslikavanjem  $G \times M \longrightarrow M$  takvim da

- (a)  $\sigma(m + m') = \sigma(m) + \sigma(m')$  za sve  $\sigma \in G, m, m' \in M$ ;
- (b)  $(\sigma\tau)(m) = \sigma(\tau(m))$  za sve  $\sigma, \tau \in G, m \in M$ ;
- (c)  $1_G m = m$  za sve  $m \in M$ .

Stoga je zadavanje djelovanja od  $G$  na  $M$  ekvivalentno zadavanju homomorfizma  $G \longrightarrow \text{Aut}(M)$  (homomorfizma kao homomorfizma grupa).

**grupa kohomologije** Zbroj i razlika dva ukrižena homomorfizma (vidi definiciju) je opet ukriženi homomorfizam, a zbroj i razlika dvaju glavnih ukriženih homomorfizama (vidi definiciju) je opet glavni ukriženi homomorfizam. Stoga možemo govoriti o abelovoj grupi ukriženih homomorfizama i abelovoj grupi glavnih ukriženih homomorfizama, te u skladu s tim definirati kvocijentnu abelovu grupu

$$H^1(G, M) = \frac{\{\text{ukriženi homomorfizmi}\}}{\{\text{glavni ukriženi homomorfizmi}\}} = \frac{\text{kociklusi}}{\text{korubovi}}.$$

To je prva grupa kohomologije, a slično se definiraju i  $n$ -te grupe kohomologije,  $H^n(G, M)$ .

## homomorfizam

**polja** Homomorfizam polja  $\alpha : F \longrightarrow F'$  je jednostavno homomorfizam prstenova (vidi dolje) sa svojstvom da  $1_F \mapsto 1_{F'}$ . Homomorfizam polja je uvijek injektivan jer je jezgra homomorfizma pravi ideal (vidi definiciju) u polju  $F$  pa stoga mora biti nula.

**prstenova** Homomorfizam prstenova  $\alpha : R \longrightarrow R'$  je preslikavanje sa  $R$  u  $R'$  takvo da vrijedi:

$$\alpha(a + b) = \alpha(a) + \alpha(b), \quad \alpha(ab) = \alpha(a)\alpha(b), \quad \text{za sve } a, b \in R.$$

**ideal** Ideal  $I$  u komutativnom prstenu  $R$  je podgrupa abelove grupe  $(R, +)$  zatvorena s obzirom na množenje sa elementima iz  $R$ :

$$r \in R, a \in I \implies ra \in I.$$

Na primjer, u prstenu cijelih brojeva  $\mathbb{Z}$  svi brojevi djeljivi s nekim zadanim prirodnim brojem  $n$  čine ideal koji označavamo sa  $(n)$ . Dalje, trivijalno se provjeri da su jezgra i slika homomorfizma prstenova (vidi definiciju) također ideali.

**integralna domena** Komutativan prsten  $R$  je integralna domena ako  $1_R \neq 0$  i ako vrijedi zakon kraćenja, tj. ako

$$ab = ac \text{ i } a \neq 0 \implies b = c \text{ u } R.$$

Posljednji uvjet ekvivalentan je uvjetu da u  $R$  nema djelitelja nule tj. da iz jednakosti  $ab = 0$  za  $a, b \in R$  nužno slijedi  $a = 0$  ili  $b = 0$ .

**invarijante** Vidi pod "fiksno polje".

**karakteristika polja** Neka je dano polje  $F$ . Promatramo homomorfizam prstenova  $\mathbb{Z} \longrightarrow F$

$$n \mapsto 1_F + 1_F + \dots + 1_F, \quad (n \text{ puta } 1_F)$$

Jezgra tog homomorfizma je ideal u  $\mathbb{Z}$ . Razlikujemo dva slučaja:

- (1) ako je jezgra trivijalna, nenul elementi iz  $\mathbb{Z}$  se preslikaju u invertibilne elemente u polju  $F$  koje onda sadrži kopiju od  $\mathbb{Q}$ . U tom slučaju kažemo da je  $F$  karakterisitke nula.

- (2) ako jezgra nije trivijalna, onda  $n \cdot 1_F = 0$  za neko  $n \neq 0 \in \mathbb{Z}$ . Najmanji pozitivan takav  $n$  bit će prost broj  $p$  takav da  $p$  generira jezgru. Stoga preslikavanje  $n \mapsto n \cdot 1_F : \mathbb{Z} \longrightarrow F$  definira izomorfizam sa  $\mathbb{Z}/p\mathbb{Z}$  u potprsten

$$\{ m \cdot 1_F \mid m \in \mathbb{Z} \}$$

od  $F$ . U tom slučaju  $F$  sadrži kopiju od  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  i kažemo da je  $F$  karakteristike  $p$ .

**kompozit polja** Neka su  $F$  i  $F'$  potpolja polja  $E$ . Presjek potpolja od  $E$  koja sadrže  $F$  i  $F'$  je najmanje potpolje od  $E$  koje sadrži i  $F$  i  $F'$ . Zovemo ga kompozit od  $F$  i  $F'$  u  $E$  i označavamo sa  $F \cdot F'$ . Možemo ga također opisati kao potpolje od  $E$  generirano sa  $F$  i  $F'$ , ili potpolje od  $E$  generirano nad  $F'$  sa  $F$ :

$$F(F') = F \cdot F' = F'(F).$$

**komutativan prsten** Prsten  $R$  je komutativan ako je množenje u tom prstenu komutativno, tj. ako je

$$ab = ba \quad \text{za sve } a, b \in R.$$

**konačno proširenje** Kažemo da je proširenje  $E$  polja  $F$  konačno ako je njegov stupanj (vidi definiciju) nad  $F$ ,  $[E : F]$ , konačan. Na primjer, polje  $\mathbb{C}$  je konačno proširenje polja  $\mathbb{R}$  jer je stupanj od  $\mathbb{C}$  nad  $\mathbb{R}$  jednak dva,  $[\mathbb{C} : \mathbb{R}] = 2$  (baza  $\{1, i\}$ )

**konstruktibilan** Broj (ili dužina) je konstruktibilan ako se u konačno mnogo koraka može konstruirati iz jedinice pomoću uzastopnih presjeka

- pravaca povučenih kroz dvije već konstruirane točke
- kružnica sa centrom u već konstruiranoj točki i radijusa već konstruirane dužine.

To je ekvivalentno s tim da je taj broj element polja  $K$  nad  $\mathbb{Q}$  koje se dobije iz  $\mathbb{Q}$  pomoću konačno mnogo kvadratnih proširenja (vidi "konstruktibilni brojevi").

**konjugati** Neka je  $E$  Galoisovo nad  $F$  sa Galoisovom grupom  $G$  (vidi definicije). Elementi  $\alpha_1 = \alpha, \alpha_2, \alpha_3, \dots, \alpha_m$  orbite od  $\alpha$  s obzirom na djelovanje od  $G$  zovu se konjugati od  $\alpha$ . Može se pokazati da je minimalni polinom (vidi definiciju) od  $\alpha$  oblika

$$f(X) = \prod_{i=1}^m (X - \alpha_i).$$

**korijen**

**višestruki** Vidi pod "kratnost".

**prosti** Vidi pod "kratnost".

**kratnost** Neka je zadano polje  $F$  i polinom  $f \in F[X]$ . Neka je, nadalje,

$$f(X) = a \prod_{i=1}^r (X - \alpha_i)^{m_i}, \quad \alpha_i \text{ međusobno različiti, } m_i \geq 1, \quad \sum_{i=1}^r m_i = \text{st}(f), \quad a \neq 0$$

rastav od  $f$  u nekom polju cijepanja od  $f$ . Kažemo da je  $\alpha_i$  korijen kratnosti  $m_i$ . Ako je  $m_i \geq 2$ ,  $\alpha_i$  se naziva višestrukim korijenom od  $f$ . Ako  $m_i = 1$ , kažemo da je  $\alpha_i$  prosti korijen od  $f$ .

**Kummerova teorija** Kummerova teorija koristi se rezultatima klasifikacije cikličkih proširenja reda  $n$  polja  $F$  u slučaju kada  $F$  sadrži primitivni  $n$ -ti korijen jedinice (vidi definiciju). Uz iste pretpostavke na  $F$ , moguće je proširiti te rezultate na klasifikaciju Galoisovih proširenja od  $F$  čija je Galoisova grupa abelova i eksponenta  $n$  (tj. na ona proširenja čija Galoisova grupa je kvocijent grupe  $(\mathbb{Z}/n\mathbb{Z})^r$  za neko  $r$ ).

**Maple** Maple je programski paket koji se koristi za rješavanje različitih matematičkih problema.

**norma i trag** Neka je polje  $E$  konačno proširenje polja  $F$  stupnja  $n$  (vidi definicije). Element  $\alpha$  iz  $F$  definira  $F$ -linearno preslikavanje

$$\alpha_L : E \longrightarrow E, \quad x \mapsto \alpha x.$$

$E$  je vektorski prostor nad  $F$  pa za gornje linearno preslikavanje sa  $E$  u  $E$  možemo gledati standardni trag i determinantu. Funkcije traga i norme sada definiramo kao:

$$Tr_{E/F}(\alpha) = Tr(\alpha_L), \quad Nm_{E/F}(\alpha) = \det(\alpha_L).$$

Iz svojstva traga i norme sada izlazi da je  $Tr_{E/F}$  homomorfizam  $(E, +) \longrightarrow (F, +)$ , a  $Nm_{E/F}$  je homomorfizam  $(E^\times, \cdot) \longrightarrow (F^\times, \cdot)$ .

Pogledajmo, na primjer, proširenje  $\mathbb{C} \supset \mathbb{R}$ . Za  $\alpha = a + bi$ , matrica od  $\alpha_L$  u bazi  $\{1, i\}$  je  $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ . Stoga je

$$Tr_{\mathbb{C}/\mathbb{R}}(\alpha) = 2Re(\alpha), \quad Nm_{\mathbb{C}/\mathbb{R}}(\alpha) = |\alpha|^2.$$

**normalna baza** Neka je  $E$  konačno Galoisovo proširenje od  $F$  sa Galoisovom grupom  $G$  (vidi definicije). Normalna baza za  $E$  je  $F$ -baza oblika  $\{\sigma\alpha \mid \sigma \in G\}$ , tj.  $F$ -baza koja se sastoji od konjugata elementa  $\alpha$  u  $E$  (vidi definiciju). Može se pokazati da svako Galoisovo proširenje ima normalnu bazu.

**normalni zatvarač** Vidi Galoisov zatvarač.

**opći polinom** Kada promatamo polinome drugog stupnja,

$$g(X) = aX^2 + bX + c,$$

znamo da su rješenja jednadžbe  $g(X) = 0$  dana formulom

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

gdje  $a, b, c$  promatramo kao varijable. Takav rezultat ne može se dobiti za polinome bilo kojeg stupnja. Protuprimjer su tzv. opći polinomi.

Neka je  $F$  neko polje. Opći polinom stupnja  $n$  je polinom oblika

$$f(X) = X^n - t_1X^{n-1} + \dots + (-1)^nt_n \in F[t_1, \dots, t_n][X]$$

gdje su  $t_1, \dots, t_n$  varijable. Može se pokazati da je Galoisova grupa polinoma  $f$  (vidi definiciju), ako ga gledamo kao polinom u  $X$  sa koeficijentima u polju  $F(t_1, \dots, t_n)$ , grupa permutacija  $S_n$ . Iz toga slijedi da (barem za polja karakteristike nula) nema formule za rješenja jednadžbe  $f(X) = 0$  rješive u radikalima (vidi definiciju) od  $f$  ako je  $f$  opći polinom stupnja  $\geq 5$ .

**polinom**

**minimalni** Neka je  $E/F$  proširenje polja  $F$  i neka je  $\alpha \in E$  algebarski nad  $F$  (vidi definiciju). Polinomi  $g \in F[X]$  takvi da  $g(\alpha) = 0$  čine ideal u  $F[X]$  koji je generiran normiranim polinomom  $f$  najmanjeg stupnja sa svojstvom da  $f(\alpha) = 0$ . Polinom  $f$  zovemo minimalni polinom od  $\alpha$  nad  $F$ . On je ireducibilan jer bi inače mogli naći dva nenul elementa u  $E$  čiji je umnožak nula. Minimalni polinom je karakteriziran kao element iz  $F[X]$  svakim od sljedećih skupova uvjeta:

- $f$  je normiran;  $f(\alpha) = 0$  i  $f$  dijeli svaki drugi polinom  $g$  iz  $F[X]$  sa svojstvom  $g(\alpha) = 0$ ,
- $f$  je normirani polinom najmanjeg stupnja takav da je  $f(\alpha) = 0$ ,
- $f$  je normiran, ireducibilan i  $f(\alpha) = 0$ .

**separabilan** Polinom  $f \in F[X]$  je separabilan ako niti jedan od njegovih ireducibilnih faktora nema višestruke korjene (u bilo kojem polju cijepanja). Može se pokazati da je  $f$  separabilan uvijek osim u slučaju kada je

- (a) karakteristika od  $F$   $p \neq 0$  i
- (b) barem jedan od ireducibilnih faktora od  $f$  polinom u  $X^p$ .

**polje** Polje je skup  $F$  sa dvije binarne operacije  $+$  i  $\cdot$  takve da je:

- (a)  $(F, +)$  komutativna grupa,
- (b)  $(F^\times, \cdot)$  (gdje  $F^\times = F \setminus \{0\}$ ), također komutativna grupa,
- (c) vrijedi zakon distributivnosti.

Iz definicije slijedi da polje sadrži barem dva različita elementa, 0 i  $1_F$ . Primjeri polja su  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  (gdje je  $p$  prost broj).

**cijepanja** Neka je  $f$  polinom s koeficijentima u polju  $F$  i neka je  $E \supset F$  neko proširenje od  $F$ . Kažemo da polje  $E$  cijepa  $f$  ako se  $f$  cijepa u  $E[X]$  tj. ako  $f(X) = \prod_{i=1}^m (X - \alpha_i)$ ,  $\alpha_i \in E$  u  $E[X]$ . Ako je, nadalje,  $E$  generirano s korjenima od  $f$ ,

$$E = F[\alpha_1, \dots, \alpha_m],$$

onda  $E$  zovemo polje cijepanja od  $f$ . Jasno je da polinomi  $\prod f_i(X)^{m_i}$  ( $m_i \geq 1$ ) i  $\prod f_i(X)$  imaju isto polje cijepanja.

*Primjer:* Neka je  $f(X) = aX^2 + bX + c \in \mathbb{Q}[X]$ , i neka je  $\alpha = \sqrt{b^2 - 4ac}$ . Potpolje  $\mathbb{Q}[\alpha]$  od  $\mathbb{C}$  je polje cijepanja za  $f$ .

**potpolje** Potpolje  $S$  polja  $F$  je potprsten zatvoren s obzirom na invertiranje, tj.  $a \in S$  i  $a \neq 0 \implies a^{-1} \in S$ . U tom slučaju  $S$  nasljeđuje strukturu polja od  $F$ . Na primjer,  $\mathbb{R}$  i  $\mathbb{Q}$  su potpolja u  $\mathbb{C}$ .

**generirano podskupom** Lagano se pokaže da je presjek polja sadržanih u nekom polju ponovo polje. Neka je  $E$  neko polje i  $S \subset E$  podskup od  $E$ . Presjek svih potpolja od  $E$  koja sadrže  $S$  je najmanje potpolje od  $E$  koje sadrži  $S$ . Kažemo da je to potpolje generirano skupom  $S$ .

*Primjer:* Polje  $\mathbb{Q}[\pi]$  koje se sastoji od svih kompleksnih brojeva oblika

$$\frac{g(\pi)}{h(\pi)}, \quad g(X), h(X) \in \mathbb{Q}[X], \quad h(\pi) \neq 0,$$

je potpolje u  $\mathbb{C}$  generirano skupom  $\mathbb{Q} \cup \pi$ .

**potprsten** Potprsten  $S$  prstena  $R$  je podskup zatvoren je s obzirom na zbrajanje, invertiranje s obzirom na zbrajanje te na množenje. Drugim riječima,  $S$  je podgrupa od  $(R, +)$  i vrijedi

$$a, b \in S \implies a \cdot b \in S$$

za svako  $a, b \in S$ .

Presjek prstena je ponovno prsten. Kao i kod polja, možemo uzeti neki podskup prstena  $S \subset R$  i promatrati sve potprstene od  $R$  koji sadrže  $S$ . Njihov presjek je najmanji potprsten od  $R$  koji sadrži  $S$  i kažemo da je to prsten generiran sa  $S$ . Ako imamo polje  $F$  i proširenje tog polja  $E$ ,  $E \supset F$ , te podskup  $S \subset E$ , možemo promatrati sve potprstene od  $E$  koji sadrže  $F$  i  $S$ . Njihov presjek je onda ponovno najmanji potprsten od  $E$  koji sadrži  $F$  i  $S$ , a označavamo ga sa  $F[S]$  i zovemo potprsten od  $E$  generiran sa  $F$  i  $S$  (ili generiran nad  $F$  sa  $S$ ). Na primjer,  $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$ .

**pravilni  $n$ -terokut** Pravilni poligon sa  $n$ -stranica ili pravilni  $n$ -terokut je konstruktibilan (vidi definiciju) ako i samo ako  $n = 2^k p_1 \dots p_s$  gdje su  $p_i$ -ovi različiti Fermatovi prosti brojevi.

**proširenje polja** Polje  $E$  koje sadrži polje  $F$  naziva se proširenje polja  $F$ . Takvo polje može se na očit način gledati kao vektorsko polje nad  $F$ . Sa  $[E : F]$  označavamo dimenziju, konačnu ili beskonačnu, od  $E$  kao vektorskog prostora nad  $F$ . Broj  $[E : F]$  zovemo stupanj od  $E$  nad  $F$ . Imamo različite vrste proširenja:

**abelovo** Konačno proširenje  $E \supset F$  zove se abelovo proširenje ako je  $E$  Galoisovo proširenje čija je Galoisova grupa (vidi definicije) abelova.

**cikličko** Konačno proširenje  $E \supset F$  zove se cikličko proširenje ako je  $E$  Galoisovo proširenje čija je Galoisova grupa (vidi definicije) ciklička.

**Galoisovo** Vidi pod Galoisova grupa.

**normalno** Algebarsko proširenje  $E/F$  je normalno ako se minimalni polinom svakog elementa iz  $E$  cijepa u  $E[X]$  (vidi definiciju). Dakle, algebarsko proširenje je normalno ako se svaki ireducibilni polinom  $f \in F[X]$  koji ima korijen u  $E$  cijepa u  $E$ .

**prosto (jednostavno)** Proširenje  $E$  od  $F$  je prosto (jednostavno) ako je  $E = F(\alpha)$  za neko  $\alpha \in E$  ( $F(\alpha)$  je, po definiciji, najmanje polje koje sadrži polje  $F$  i element  $\alpha$ ; kažemo da je to polje generirano sa  $F$  i  $\alpha$ ).

**rješivo** Konačno proširenje  $E \supset F$  zove se rješivo proširenje ako je  $E$  Galoisovo proširenje čija je Galoisova grupa (vidi definicije) rješiva.

**separabilno** Algebarsko proširenje  $E/F$  je separabilno ako je minimalni polinom svakog elementa iz  $E$  separabilan (vidi definiciju). U suprotnom, proširenje zovemo neseparabilnim.

**primitivni element** Konačno proširenje  $E/F$  je prosto (jednostavno) ako postoji element  $\alpha \in E$  takav da je  $E = F[\alpha]$  (vidi definiciju). Takav  $\alpha$  nazivamo primitivnim elementom. Poznato je da sva separabilna proširenja (vidi definiciju) imaju primitivni element. Čak i više, vrijedi

*Teorem* Neka je  $E = F[\alpha_1, \dots, \alpha_r]$  konačno proširenje od  $F$  i pretpostavimo da su  $\alpha_2, \dots, \alpha_r$  separabilni nad  $F$  (ali ne nužno i  $\alpha_1$ ). Onda postoji  $\gamma \in E$  takav da  $E = F[\gamma]$ .

**primitivni korijen jedinice** Primitivni  $n$ -ti korijen jedinice u polju  $F$  je element reda  $n$  u  $F$ . Takav element može postojati jedino ako je  $F$  karakteristike nula ili karakteristike  $p$  gdje  $p$  ne dijeli  $n$ .

**prsten** Prsten je skup  $R$  sa dvije binarne operacije  $+$  i  $\cdot$  takve da

(a)  $(R, +)$  je komutativna grupa;

(b)  $\cdot$  je asocijativna operacija;

(c) vrijedi zakon distributivnosti: za sve  $a, b, c \in R$  je

$$\begin{aligned}(a + b) \cdot c &= a \cdot c + b \cdot c \\ a \cdot (b + c) &= a \cdot b + a \cdot c.\end{aligned}$$



Ponekad se traži i uvjet postojanja jedinice tj. elementa  $1_R \in R$  sa svojstvom da  $a \cdot 1_R = 1_R \cdot a = a$  za sve  $a \in R$ . Prsteni sa takvim elementom nazivaju se onda prsteni sa jedinicom.

**polinoma** Prsten polinoma  $F[X]$  je komutativan prsten čiji su elementi polinomi s koeficijentima u polju  $F$  u jednoj varijabli  $X$ . Dakle, elementi tog prstena se mogu na jedinstven način zapisati kao

$$a_m X^m + a_{m-1} X^{m-1} + \dots + a_0, \quad a_i \in F, \quad m \in \mathbb{N}, \quad a_m \neq 0.$$

Njihovo zbrajanje i množenje definirano je na standardni način.

**rješiva u radikalima** Za polinom  $f \in F[X]$  kažemo da je jednačba  $f(X) = 0$  rješiva u radikalima ako se njena rješenja mogu dobiti algebarskim operacijama zbrajanja, oduzimanja, množenja, dijeljenja i korjenovanja, ili, preciznije, ako postoji toranj polja

$$F = F_0 \subset F_1 \subset F_2 \subset \dots \subset F_m$$

takav da je

- (a)  $F_i = F_{i-1}[\alpha_i], \quad \alpha_i^{m_i} \in F_{i-1};$
- (b)  $F_m$  sadrži polje cijepanja (vidi definiciju) za  $f$ .

Može se pokazati da vrijedi sljedeće: neka je  $F$  karakteristike nula. Jednačba  $f = 0$  je rješiva u radikalima ako i samo ako je Galoisova grupa od  $f$  rješiva (vidi definiciju).

**savršeno polje** Polje  $F$  je savršeno ako su svi polinomi u  $F[X]$  separabilni (ili, ekvivalentno, ako su svi ireducibilni polinomi u  $F[X]$  separabilni). Može se pokazati da je svako polje karakteristike nula (vidi definiciju) savršeno te da je polje karakteristike  $p \neq 0$  savršeno ako i samo ako je  $F = F^p$ , tj. ako je svaki element od  $F$   $p$ -ta potencija. Algebarski zatvorena polja su također savršena.

**separabilan** Kažemo da je algebarski element  $\alpha$  nad  $F$  (vidi definiciju) separabilan nad  $F$  ako njegov minimalni polinom nad  $F$  nema višestrukih korjena (vidi definicije).

**separabilni element** Neka je  $E/F$  konačno proširenje polja  $F$  (vidi definiciju). Element  $\alpha \in E$  nazivamo separabilnim elementom nad  $F$  ako je njegov minimalni polinom nad  $F$  separabilan (vidi definiciju).

**simetrični polinomi** Neka je  $R$  komutativni prsten s jedinicom  $1_R$ . Polinom  $P(X_1, \dots, X_n) \in R[X_1, \dots, X_n]$  je simetričan ako je invarijantan na permutacije varijabli, tj. ako

$$P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n) \quad \text{za sve } \sigma \in S_n.$$

**elementarni** Polinomi oblika

$$\begin{aligned} p_1 &= \sum_i X_i = X_1 + \dots + X_n, \\ p_2 &= \sum_{i < j} X_i X_j = X_1 X_2 + X_1 X_3 + \dots + X_{n-1} X_n, \\ p_3 &= \sum_{i < j < k} X_i X_j X_k = X_1 X_2 X_3 + \dots, \\ &\dots \\ p_r &= \sum_{i_1 < \dots < i_r} X_{i_1} \dots X_{i_r}, \\ &\dots \\ p_n &= X_1 X_2 \dots X_n \end{aligned}$$

su očito simetrični jer su  $p_r$  sume svih monoma stupnja  $r$  sastavljenih od različitih  $X_i$ -ova. Te polinome zovemo elementarni simetrični polinomi. Jasno je da su sve njihove linearne kombinacije također simetrični polinomi.

**stupanj** Neka je  $E/F$  neko proširenje polja  $F$ .  $E$  se na prirodan način može gledati kao vektorski prostor nad  $F$ . Dimenzija od  $E$  nad  $F$  kao vektorskog prostora nad  $F$ , zove se stupanj od  $E$  nad  $F$  i označava sa  $[E : F]$ . Taj broj može biti i beskonačan.

## teorem

### binomni u karakteristici $p$ Binomni teorem

$$(a + b)^m = a^m + \binom{m}{1} a^{m-1} b + \binom{m}{2} a^{m-2} b^2 + \dots + b^m$$

vrijedi u svakom komutativnom prstenu. Ako je  $p$  prost, onda  $p \mid \binom{p}{r}$  za svako  $r$ ,  $1 \leq r \leq p-1$ . Stoga, ako je polje  $F$  karakteristike  $p$ , vrijedi jednakost

$$(a + b)^p = a^p + b^p.$$

(vidi "Frobeniusov automorfizam")

**ciklotomski polinomi** Taj teorem dokazao je još Dedekind, a glasi:

*Teorem*  $N$ -ti ciklotomski polinom (vidi definiciju),  $\Phi_n$ , je ireducibilan u  $\mathbb{Q}[X]$ .

**Dedekindov** Neka je  $f(X) \in \mathbb{Z}[X]$  normirani polinom stupnja  $m$  i neka je  $p$  prost broj takav da  $f \bmod p$  ima proste korjene (ili, ekvivalentno, takav da diskriminanta  $D(f)$  nije djeljiva s  $p$ ). Pretpostavimo da je slika od  $f$  u  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  s obzirom na standardnu projekciju oblika  $\bar{f} = \prod f_i$  gdje su  $f_i$  ireducibilni polinomi stupnja  $m_i$  u  $\mathbb{F}_p[X]$ . Onda Galoisova grupa polinoma  $f$ ,  $G_f$  (vidi definiciju), sadrži element čija je ciklička dekompozicija oblika

$$m = m_1 + \dots + m_r.$$

Ovaj teorem daje strategiju za računanje Galoisove grupe ireducibilnog polinoma  $f \in \mathbb{Q}[X]$ .

**Galoisov iz 1832.** Neka je  $F$  polje karakteristike nula (vidi definiciju). Jednadžba  $f = 0$  je rješiva u radikalima ako i samo ako je Galoisova grupa od  $f$  rješiva (vidi "rješiva u radikalima").

**Galoisova proširenja** Za proširenje  $E/F$  sljedeće tvrdnje su ekvivalentne:

- (a)  $E$  je polje cijepanja separabilnog polinoma  $f \in F[X]$ ;
- (b)  $F$  je fiksno polje neke konačne grupe  $G$  automorfizama od  $F$ ,  $F = E^G$ ;
- (c)  $E$  je normalno i separabilno, te konačnog stupnja nad  $F$ ;
- (d)  $E$  je Galoisovo nad  $F$

(vidi pripadne definicije). Neke od važnih posljedica ovog teorema jesu:

- svako konačno separabilno proširenje  $E$  od  $F$  je sadržano u nekom konačnom Galoisovom proširenju od  $F$ ,
- neka  $E \supset M \supset F$ ; ako je  $E$  Galoisovo nad  $F$ , onda je  $E$  Galoisovo i nad  $M$ .

**konstruktibilnosti  $n$ -terokuta** Vidi pod pravilni  $n$ -terokut.

**konstruktibilni brojevi** Imamo dva važna teorema o konstruktibilnosti brojeva (vidi definiciju):

*Teorem 1*

- (a) skup konstruibilnih brojeva čini polje,

(b) broj  $\alpha$  je konstruibilan ako i samo ako  $\alpha$  leži u polju oblika

$$\mathbb{Q}[\sqrt{a_1}, \dots, \sqrt{a_r}], \quad a_i \in \mathbb{Q}[\sqrt{a_1}, \dots, \sqrt{a_{i-1}}].$$

Posljedice ovog teorema su rješenja poznatih problema iz povijesti:

- nemoguće je udvostručiti kocku pomoću ravnala i šestara,
- nemoguće je konstruirati trisekciju proizvoljnog kuta,
- nemoguće je konstruirati kvadrat iste površine kao i zadani krug, tj. nemoguća je kvadratura kruga.

Drugi teorem glasi:

**Teorem 1** Ako je  $\alpha$  sadržan u Galoisovom proširenju stupnja  $2^r$ ,  $r \in \mathbb{N}$  od  $\mathbb{Q}$  (vidi definicije), onda je  $\alpha$  konstruktibilan.

Iz ovog teorema slijedi da, ako je  $p$  prost broj oblika  $2^k + 1$ , onda je  $\cos \frac{2\pi}{p}$  konstruktibilan. Krajnja posljedica je ta da je pravilni  $p$ -terokut ( $p$  prost broj), konstruktibilan ako i samo ako je  $p$  Fermatov broj, tj. oblika  $2^{2^r} + 1$ .

**Liouvilleov** 1884. god. matematičar Liouville je prvi pokazao da postoje brojevi koji nisu algebarski, odnosno našao je neke transcendentale brojeve koje danas zovemo Liouvilleovi brojevi. Jedan takav broj navodi sljedeći teorem:

**Teorem** Broj  $\alpha = \sum \frac{1}{2^{n!}}$  je transcendentalan.

**nezavisnost karaktera** Neka je  $F$  polje i neka je  $G$  grupa (može i slabiji zahtjev,  $G$  monoid). Onda je svaki konačni skup  $\chi_1, \dots, \chi_m$  homomorfizama  $G \longrightarrow F^\times$  linearно nezavisan nad  $F$ , tj.

$$\sum a_i \chi_i = 0 \quad (\text{kao funkcija } G \longrightarrow F) \implies a_1 = 0, \dots, a_m = 0.$$

Neke od važnih posljedica tog teorema jesu:

- neka su  $F_1$  i  $F_2$  polja i neka su  $\sigma_1, \dots, \sigma_m$  različiti homomorfizmi  $F_1 \longrightarrow F_2$ . Onda su  $\sigma_1, \dots, \sigma_m$  linearно nezavisni nad  $F_2$ ;
- neka je  $E$  konačno separabilno proširenje od  $F$  stupnja  $m$ . Neka je  $\alpha_1, \dots, \alpha_m$  baza od  $E$  nad  $F$  i neka su  $\sigma_1, \dots, \sigma_m$  različiti  $F$ -homomorfizmi sa  $E$  u polje  $\Omega$ . Onda je matrica  $(\sigma_i \alpha_j)$  invertibilna.

**normalna baza** Svako Galoisovo proširenje ima normalnu bazu (vidi definicije).

**trag** Vidi pod norma i trag.

**transcendentalan** Neka je  $F$  polje i  $E$  neko proširenje tog polja. Za element  $\alpha \in E$  kažemo da je transcendentalan nad  $F$  ako homomorfizam

$$f(X) \mapsto f(\alpha) : F[X] \longrightarrow E$$

ima trivijalnu jezgru, tj. ako ne postoji polinom  $f \in F[X]$  takav da je  $f(\alpha) = 0$ . Ako takav element postoji u  $E$ ,  $E$  nazivamo transcendentálnim proširenjem od  $F$ . Najpoznatije transcendentálno proširenje je  $\mathbb{R}$  nad  $\mathbb{Q}$ , već 1884. god. Liouville je našao prve transcendentálne brojeve u  $\mathbb{R}$  (vidi pod Liouville). 1873. god. Hermite je pokazao da je broj  $e$  transcendentalan, a 1882. god. Lindemann dokazuje isto za  $\pi$ . U vezi transcendentálnih brojeva postoji puno otvorenih pitanja, npr. još se ne zna je li Eulerova konstanta

$$\gamma = \lim_{n \rightarrow \infty} \left( \sum_{k=1}^n \frac{1}{k} - \log n \right)$$

transcendentalna ili ne.

**ukriženi homomorfizam (kociklus)** Neka je  $M$   $G$ -modul (vidi definiciju). Ukriženi homomorfizam (kociklus) je preslikavanje  $f : G \longrightarrow M$  takvo da

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau) \quad \text{za sve } \sigma, \tau \in G.$$

Iz definicije odmah slijedi da  $f(1) = f(1 \cdot 1) = f(1) + f(1)$  pa  $f(1) = 0$ .

**glavni (korub)** Za bilo koje  $x \in M$  možemo dobiti ukriženi homomorfizam ako definiramo

$$f(\sigma) = \sigma x - x, \quad \text{za sve } \sigma \in G.$$

Takav ukriženi homomorfizam nazivamo glavnim ukriženim homomorfizmom (korubom).