Algebarski broj

Algebarski broj je element polja algebarskih brojeva.

Algebarski element u proširenju polja

Neka je L/K proširenje polja K. Kažemo da je $u \in L$ algebarski element nad K ako je u korijen nekog ne-nul polinoma $f \in K[X]$.

Na primjer, algebarski elementi od $\mathbb{C}$ nad $\mathbb{Q}$ jesu upravo algebarski brojevi.

Algebarski zatvoreno polje

Polje F je algebarski zatvoreno ako ne postoji niti jedno algebarsko proširenje od F osim njega samog.

Na primjer, polje $\mathbb{C}$ kompleksnih brojeva je algebarski zatvoreno, kao i polje $\overline{\mathbb{Q}}$ svih algebarskih brojeva.

Algebarsko zatvorenje polja

Neka je L/K proširenje polja K. Prema rezultatu iz teorije polja, sljedeći uvjeti su ekvivalentni:

(1) L je algebarsko proširenje od K i L je algebarski zatvoreno polje

(2) L je polje razlaganja nad K skupa svih (ireducibilnih) polinoma u $K[X]$.

Ako vrijede ovi uvjeti, onda kažemo da je polje L algebarsko zatvorenje polja K.

Na primjer, polje $\mathbb{C}$ je algebarsko zatvorenje polja $\mathbb{R}$, polje $\overline{\mathbb{Q}}$ (polje svih algebarskih brojeva) je algebarsko zatvorenje od $\mathbb{Q}$.

Algebarsko proširenje polja

Proširenje L/K polja K je algebarsko ako je svaki element polja L algebarski nad K.

Algebra

Prsten B s homomorfizmom prstena $A \to B$ zovemo $A-$algebra. Najčešće se ova terminologija koristi kada je A potprsten od B. U tom slučaju za elemente $\beta_1, \beta_2, \ldots, \beta_m \in B$ s $A[\beta_1, \beta_2, \ldots, \beta_m]$ označavamo najmanji potprsten od B koji sadrži A i sve β_i. Taj se potprsten sastoji od svih polinoma u β_i s koeficijentima u A. Dalje, kažemo da je $A[\beta_1, \beta_2, \ldots, \beta_m]$ $A-$podalgebra od B generirana s β_i, a u slučaju da je $B = A[\beta_1, \beta_2, \ldots, \beta_m]$ kažemo da β_i generiraju B kao $A-$algebru.

Apsolutna vrijednost

vidi Valuacija

Arhimedska točka

vidi Teorem o točkama ("primes") u polju brojeva

Arhimedska valuacija
vidi Valuacija

Baza cijelih brojeva
Neka je K polje algebarskih brojeva, a $\mathcal{O}_K$ pripadni prsten cijelih brojeva. Bazu $\alpha_1, \ldots, \alpha_m$ za $\mathcal{O}_K$ kao $\mathbb{Z}-$modul zovemo baza cijelih brojeva za K.
Na primjer, ako je $K = \mathbb{Q}(\sqrt{d})$, gdje je d kvadratno slobodan cijeli broj različit od 0 i 1, onda je $\{1, \sqrt{d}\}$ baza za $\mathbb{Q}_K$ ako je $d \equiv 2, 3 \pmod 4$, a $\{1, \frac{1+\sqrt{d}}{2}\}$ je baza ako je $d \equiv 1 \pmod 4$.

Baza modula
Neka je A prsten i M $A-$modul. Skup elemenata $\{e_1, \ldots, e_n\}$ zovemo baza modula M ako:

(a) $\sum_{i=1}^{n} a_i e_i = 0$, $a_i \in A \Rightarrow a_i = 0$, $i = 1, \ldots, n$

(b) svaki element $x \in M$ možemo izraziti u obliku $x = \sum_{i=1}^{n} a_i e_i$, $a_i \in A$, $i = 1, \ldots, n$.

Binarna kvadratna forma
Binarna kvadratna forma je forma Q oblika $Q(X, Y) = aX^2 + bXY + cY^2$, gdje koeficijenti pripadaju danom komutativnom prstenu s jedinicom.

Blago razgranato proširenje
Proširenje konačnog stupnja L potpunog polja K obzirom na nearhimedsku valuaciju $|\ |$ je blago razgranato ako char(k) $\nmid e$, gdje je k rezidualno polje od K, a e indeks grananja od L/K.

Broj klasa ideala
Broj klasa ideala Dedekindove domene A je red grupe klasa ideala $\mathrm{Cl}(A)$ (ako je $\mathrm{Cl}(A)$ konačan). Za polje algebarskih brojeva K označavamo ga s h_K.
Na primjer, $h_k = 1$ za $K = \mathbb{Q}, \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$, a $h_K = 2$ za $K = \mathbb{Q}(\sqrt{10}), \mathbb{Q}(\sqrt{-5})$.

Cauchyjev niz
Neka je K polje s netrivijalnom valuacijom $|\ |$. Niz (a_n) elemenata u K zovemo Cauchyjev niz ako za svaki $\varepsilon > 0$ postoji prirodan broj N takav da je $|a_m - a_n| < \varepsilon$ za sve $m, n > N$.

Cijeli element
Neka je A integralna domena i L polje koje sadrži A. Element $\alpha \in L$ je cijeli element nad A ako je korijen unitarnog polinoma s koeficijentima u A, tj. ako zadovoljava jednadžbu

$$\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0 \text{ za neke } a_i \in A, i = 1 \ldots n.$$

Cijeli ideal
vidi Razlomljen ideal

Cijelo zatvoren prsten
Prsten A je cijelo zatvoren ako je jednak svom cijelom zatvorenju u vlastitom polju razlomaka K, tj. ako vrijedi

$$\alpha \in K, \alpha \text{ cio nad } A \Rightarrow \alpha \in A.$$

Cijelo zatvorenje
Neka je A integralna domena i L polje koje sadrži A. Prema rezultatu iz teorije brojeva, skup elemenata iz L koji su cijeli nad A tvori prsten. Taj prsten zovemo cijelo zatvorenje od A u L.

Dedekindova domena
Dedekindova domena je integralna domena A koja nije polje, takva da vrijedi:

(1) A je Noetherina

(2) A je cijelo zatvorena

(3) svaki nenul prost ideal je maksimalan.

Na primjer, za svako polje algebarskih brojeva K pripadni prsten cijelih brojeva $\mathcal{O}_K$ uvijek je Dedekindova domena. Dalje, prsten polinoma $F[X]$ polja F je Dedekindova domena.

Dedekindova lema
Neka je G grupa i F polje te neka su $\sigma_1, \dots, \sigma_m$ različiti homomorfizmi $G \to F^\times$. Tada su $\sigma_1, \dots, \sigma_m$ linearno nezavisni nad F, tj. ne postoje netrivijalni $c_i \in F$ takvi da je $x \mapsto \sum_{i=1}^m c_i\sigma_i(x) : G \to F$ nul-preslikavanje.

Dedekindov teorem o računanju Galoisove grupe
Neka je $f(X)$ unitaran polinom stupnja n nad poljem brojeva K takav da je $f(X) \in \mathcal{O}_K[X]$, gdje je $\mathcal{O}$ prsten cijelih brojeva od K. Neka je G Galoisova grupa od f, a $\mathfrak{p}$ prost ideal u K takav da je

$$f(X) \equiv f_1(X) \cdots f_r(X) \mod \mathfrak{p}$$

za različite ireducibilne polinome $f_i \in k[X]$, $k := \mathcal{O}_K/\mathfrak{p}$. Tada G sadrži permutaciju σ koja je produkt disjunktnih ciklusa duljina $\deg f_i$, $i = 1, \dots, r$.

Dekompozicijska grupa
isto što i Grupa cijepanja

Diskretna podgrupa
Diskretna podgrupa je aditivna podgrupa konačnodimenzionalnog realnog vektorskog prostora koja je diskretan topološki prostor u induciranoj topologiji.

Diskretna valuacija

vidi Valuacija, $\mathfrak{p}-$adska apsolutna vrijednost

Diskriminanta polja algebarskih brojeva

Neka je K polje algebarskih brojeva s pripadnim prstenom cijelih brojeva $\mathcal{O}_K$. Neka je $\{w_1, \ldots, w_n\}$ baza $\mathcal{O}_K$ kao slobodnog $\mathbb{Z}-$modula. Diskriminantu polja K, u oznaci $\triangle_K$, definiramo kao $\triangle_K := \det(\mathrm{Tr}_{K/\mathbb{Q}}(w_i w_j))$, gdje je $\mathrm{Tr}_{K/\mathbb{Q}}(w_i w_j)$ matrica forme traga proširenja polja $K/\mathbb{Q}$ u bazi $\{w_1, \ldots, w_n\}$.
Na primjer, za $K = \mathbb{Q}(\sqrt{d})$, gdje je d kvadratno slobodan cijeli broj različit od 0 i 1, imamo da je $\triangle_K = d$ ako $d \equiv 1 \pmod 4$ te $\triangle_K = 4d$ ako je $d \equiv 2, 3 \pmod 4$.

Diskriminanta proširenja polja

Neka je L/K proširenje stupnja n polja K i neka je $\{a_1, \ldots, a_n\}$ baza od L kao vektorskog prostora nad K. Diskriminanta proširenja L/K, u oznaci $D_{L/K}$, definira se kao $D_{L/K}(a_1, \ldots, a_n) := \det(\mathrm{Tr}_{L/K}(a_i a_j))$, gdje je $\mathrm{Tr}_{L/K}(a_i a_j)$ matrica forme traga proširenja polja L/K u bazi $\{a_1, \ldots, a_n\}$). Diskriminanta proširenja polja ovisi o izboru baze L/K: za neku drugu bazu $\{b_1, \ldots, b_n\}$ je $D_{L/K}(b_1, \ldots, b_n) = \det(e_{ij})^2 \cdot D_{L/K}(a_1, \ldots, a_n)$, gdje je $(e_{ij})_{i,j=1}^n$ matrica prijelaza među bazama $\{a_1, \ldots, a_n\}$ i $\{b_1, \ldots, b_n\}$.
vidi Diskriminanta polja algebarskih brojeva

Dobar algoritam

Dobar algoritam je algoritam koji završava u manje od N^c koraka za neki broj c, gdje je N broj znakova potrebnih za ispis podataka (input).

Eisensteinov kriterij

Polinom $X^m + a_1 X^{m-1} + \cdots + a_m$ takav da je $a_i \in \mathbb{Z}$ i $p | a_i$ za sve $i = 1 \ldots m$ te $p^2 \nmid a_m$, je ireducibilan u $\mathbb{Q}[X]$.

Eisensteinov polinom

Neka je $\mathfrak{p}$ prost ideal u Dedekindovoj domeni A. Polinom $X^m + a_1 X^{m-1} + \cdots + a_m$, $a_i \in A$, je Eisensteinov polinom u odnosu na $\mathfrak{p}$ ako je

$$\mathrm{ord}_{\mathfrak{p}}(a_1) > 0, \ldots, \mathrm{ord}_{\mathfrak{p}}(a_{m-1}) > 0, \mathrm{ord}_{\mathfrak{p}}(a_m) = 1.$$

Ekvivalentne valuacije

Valuacije $|\ |_1$ i $|\ |_2$ na polju K su ekvivalentne ako je $|\ |_1$ netrivijalna i vrijede sljedeće ekvivalentne tvrdnje:

(1) $|\ |_1$ i $|\ |_2$ definiraju istu topologiju na K

(2) $|\alpha|_1 < 1 \Rightarrow |\alpha|_2 < 1$

(3) $|\ |_2 = |\ |_1^a$ za neki $a > 0$.

Euklidova domena

Euklidova domena je integralna domena D na kojoj postoji funkcija ν koja nenul elementima iz D pridružuje nenegativne cijele brojeve, a ima sljedeća svojstva:

(1) za svaka dva ne-nul elementa iz D je $\nu(ab) \geq \nu(a)$

(2) za $a, b \in D$, $b \neq 0$, postoje $q, r \in D$ takvi da je $a = bq + r$ i $r = 0$ ili $\nu(r) < \nu(b)$.

Na primjer, prsten $\mathbb{Z}$ s $\nu(x) := |x|$ je Euklidova domena. Prsten $\mathbb{Z}[i]$ je Euklidova domena s $\nu(z) := |z|$. Dalje, polje F s $\nu(x) := 1$ za sve $x \in F$, $x \neq 0$, je Euklidova domena. Također, za polje F je prsten polinoma jedne varijable s $\nu(f) := \deg f$ Euklidova domena.

Faktorijalan prsten

Prsten A je faktorijalan ako je svaki ne-nul neinvertibilan element moguće na jedinstven način prikazati kao produkt ireducibilnih elemenata.
Takvi su npr. $A = \mathbb{Z}$ ili $k[X], k[X, Y]$ za k polje, potom $\mathbb{Z}[i]$, $\mathbb{Z}[\rho]$, dok je $\mathbb{Z}[\sqrt{-5}]$ primjer prstena koji nije faktorijalan.

Frobeniusov automorfizam

Neka je F konačno polje s p elemenata. Tada za svaki $a, b \in F$ vrijedi

$$(a+b)^p = a^p + b^p, \qquad (ab)^p = a^p \cdot b^p.$$

Stoga je preslikavanje $\varphi : F \to F$ dano s $a \mapsto a^p$ automorfizam $-$ zovemo ga Frobeniusov automorfizam.
vidi primjer uz Frobeniusov element

Frobeniusov element

Neka je L/K Galoisovo proširenje polja brojeva s pripadnom Galoisovom grupom G i prstenima cijelih brojeva $\mathcal{O}_K$ za K i $\mathcal{O}_L$ za L. Neka je dan prost ideal $\mathfrak{P}$ u L nerazgranat u L/K; označimo s $G(\mathfrak{P}) := \{\sigma \in G | \sigma\mathfrak{P} = \mathfrak{P}\}$ dekompozicijsku grupu ideala $\mathfrak{P}$. Frobeniusov element $\sigma_{Fr} := (\mathfrak{P}, L/K)$ je element $G(\mathfrak{P})$ koji djeluje kao Frobeniusov automorfizam na rezidualnom polju.
σ_{Fr} je jedinstveno određen sljedećim dvama uvjetima:

(1) $\sigma_{Fr} \in G(\mathfrak{P})$, tj. $\sigma\mathfrak{P} = \mathfrak{P}$

(2) za sve $\alpha \in \mathcal{O}_L$ je $\sigma\alpha \equiv \alpha^q \bmod \mathfrak{P}$, gdje je q broj elemenata rezidualnog polja $\mathcal{O}_K/\mathfrak{p}$ za $\mathfrak{p} := \mathfrak{P} \cap K$.

Napomena: zbog $1-1$ korespondencije između prostih ideala i klasa ekvivalencija diskretnih valuacija može se grupa cijepanja (kako i jest slučaj u definiciji tog pojma) označiti s G_ω, gdje je ω predstavnik klase ekvivalencije diskretnih valuacija koja odgovara idealu $\mathfrak{P}$. Vidi Grupa cijepanja.
Na primjer, neka je $K = \mathbb{Q}[\sqrt{d}]$ za kvadratno slobodan cijeli broj d i $\mathfrak{p}$ nerazgranata točka ("prime") u K. S obzirom da $\mathrm{Gal}(K/\mathbb{Q})$ možemo identificirati s $\{-1, 1\}$, to je $(\mathfrak{p}, K/\mathbb{Q}) = 1$ ili $(\mathfrak{p}, K/\mathbb{Q}) = -1$, ovisno o tome je li d kvadrat modulo $\mathfrak{p}$ ili ne. Preciznije:

(1) Ako za numeričku normu ideala $\mathfrak{p}$ vrijedi $\mathbb{N}(\mathfrak{p}) = p$ za neki prosti broj p i p se ne grana ($(p) = \mathfrak{p} \cdot \mathfrak{p}'$ gdje je $\mathfrak{p}'$ različit od $\mathfrak{p}$), onda je pripadno rezidualno

polje izomorfno polju $\mathbb{F}_p$ (konačnom polju s p elemenata). U tom slučaju je Frobeniusov automorfizam $a \mapsto a^p$ identitet, za Frobeniusov element je $(\mathfrak{p}, K/\mathbb{Q}) = 1$, a za dekompozicijsku grupu $G(\mathfrak{p}) = 1$. To je onda kada je $(\frac{p}{d}) = 1$.

(2) Ako je $\mathbb{N}(\mathfrak{p}) = p^2$ za neki prosti broj p ($(p) = \mathfrak{p}$ je prost ideal u K), onda je pripadno rezidualno polje izomorfno $\mathbb{F}_{p^2}$. Tada je Frobeniusov automorfizam $a \mapsto a^p$ netrivijalan, Frobeniusov element je $(\mathfrak{p}, K/\mathbb{Q}) = -1$, a dekompozicijska grupa $G(\mathfrak{p}) = \{-1, 1\}$. To je kada je $(\frac{p}{d}) = -1$

(3) Ako je $\mathbb{N}(\mathfrak{p}) = p$ i p se grana ($(p) = \mathfrak{p}^2$), onda za dekompozicijsku grupu imamo $G(\mathfrak{p}) = \{-1, 1\}$, a Frobeniusov element nije jednoznačno određen uvjetima (1) i (2) iz definicije ovog pojma (ta dva uvjeta vrijede i za $\sigma = -1$ i za $\sigma = 1$). To je kada p dijeli diskriminantu polja K.

Fundamentalni paralelepiped

Neka je V konačnodimenzionalni vektorski prostor dimenzije n i Λ puna rešetka u V dana s $\Lambda = \sum_{i=1}^{n} \mathbb{Z}e_i$. Za svaki $\lambda_0 \in \Lambda$ definiramo

$$D = \{\lambda_0 + \sum_{i=1}^{n} a_i e_i | 0 \leq a_i < 1\}.$$

Takav skup zovemo fundamentalni paralelepiped za rešetku Λ.

Fundamentalni sistem jedinica

Označimo s U_K grupu jedinica u polju brojeva K, a s $\mu(K)$ grupu korijena iz jedinice u K. Prema Teoremu o jedinicama U_K je konačno generirana ranga je $r + s - 1$, gdje je r broj realnih, a s broj parova kompleksno-konjugiranih ulaganja K u $\mathbb{C}$.

Za skup jedinica $\{u_1, \ldots, u_{r+s-1}\}$ kažemo da je fundamentalni sistem jedinica ako čini bazu za U_K (modulo torzija), tj. ako je svaku jedinicu u moguće jedinstveno prikazati u obliku

$$u = \zeta u_1^{m_1} \cdots u_{r+s-1}^{m_{r+s-1}}, \quad \zeta \in \mu(K), \quad m_i \in \mathbb{Z}.$$

Na primjer, za $K = \mathbb{Q}[\sqrt{d}]$, gdje je d kvadratno slobodan nenegativan cijeli broj, je $r = 2$, $s = 0$, pa je U_K grupa ranga 1, što znači da postoji $\epsilon \in K$ takav da je $U_K \cong \mu(K) \cdot < \epsilon >= \{\pm 1\} \cdot < \epsilon >$. Drugim riječima, U_K je izomorfna grupi $(\mathbb{Z}, \cdot)$. Za $d < 0$ je U_K trivijalna grupa (jer je $r = 0$, $s = 1$, pa je $r + s - 1 = 0$). Tada je

$$U_K = \begin{cases} \{\pm 1\} & ; \text{ za } d \neq -1, -3 \\ \{\pm 1, \pm i\} & ; \text{ za } d = -1 \\ \{\pm 1, \pm \rho, \pm \rho^2\} & ; \text{ za } d = -3 \end{cases}.$$

Galoisovo proširenje polja

Neka je L proširenje polja K takvo da je fiksno polje Galoisove grupe upravo polje K. Tada kažemo da je L Galoisovo proširenje polja K ili da je L Galoisovo nad K.

Na primjer, svako kvadratno proširenje je Galoisovo nad $\mathbb{Q}$, ciklotomska proširenja $\mathbb{Q}(\zeta)/\mathbb{Q}$ (ζ je $n-$ti korijen iz 1) su Galoisova, dok npr. $\mathbb{F}_p(X)/\mathbb{F}_p(X^p)$ nije Galoisovo ($\mathbb{F}_p$ je konačno polje s p elemenata, p prost broj).
Napomena: rezultat iz teorije polja kaže da je neko proširenje Galoisovo ako i samo ako je normalno i separabilno.

Glavni razlomljeni ideal

vidi Razlomljeni ideal

Globalno polje

Globalno polje je ili proširenje konačnog stupnja polja $\mathbb{Q}$ ili proširenje konačnog stupnja polja $\mathbb{F}_q(X)$ racionalnih funkcija jedne varijable, gdje je $\mathbb{F}_q$ neko konačno polje.

Grupa cijepanja

Neka je L Galoisovo proširenje konačnog stupnja polja brojeva K i neka je $G = \mathrm{Gal}(L/K)$ pripadna Galoisova grupa. Za valuaciju w od L označimo sa $\sigma\omega$ valuaciju takvu da je $|\sigma\alpha|_{\sigma\omega} = |\alpha|_\omega$, tj. $|\alpha|_{\sigma\omega} = |\sigma^{-1}\alpha|_\omega$.
Grupa G djeluje na skupu točaka ("primes") polja L koji leže nad fiksnom točkom ("prime") $v \in K$. Grupa cijepanja ili dekompozicijska grupa valuacije ω definira se kao stabilizator za ω u G, tj. kao grupa

$$G_\omega = \{\sigma \in G | \sigma\omega = \omega\}.$$

Napomena: usporedi s definicijom Frobeniusovog elementa - zbog $1-1$ korespondencije između prostih ideala i klasa ekvivalencija diskretnih valuacija grupa cijepanja može se definirati i kao $G(\mathfrak{P})$, gdje je $\mathfrak{P}$ ideal u korespondenciji s klasom diskretnih valuacija čiji je ω predstavnik.
Na primjer, za $K = \mathbb{Q}(\sqrt{d})$ kvadratno proširenje je $G = \{1, \sigma := a + b\sqrt{d} \mapsto a - b\sqrt{d}\}$. Imamo nekoliko mogućnosti:

(1) ako je ω nearhimedska diskretna valuacija koja odgovara idealu $\mathfrak{p}$ iznad ideala (p) (p prost), tj. $\mathfrak{p} \cap \mathbb{Z} = (p)$, onda je:

- (a) ako je $(p) = \mathfrak{p} \cdot \mathfrak{p}'$ za neki $\mathfrak{p}' \neq \mathfrak{p}$, onda je $G(\mathfrak{p}) = \{1\}$
- (b) ako je $(p) = \mathfrak{p}$ prost, onda je $G(\mathfrak{p}) = \{1, \sigma\}$
- (c) ako je $(p) = \mathfrak{p}^2$, onda je $G(\mathfrak{p}) = \{1, \sigma\}$.

(2) ako je ω arhimedska i:

- (a) $d < 0$, onda je $G(\omega) = \{1, \sigma\}$
- (b) $d > 0$, onda je $G(\omega) = \{1\}$.

vidi primjer uz Frobeniusov element

Grupa grananja

Neka je L Galoisovo proširenje konačnog stupnja potpunog polja K s diskretnom nearhimedskom valuacijom takvog da je rezidualno polje k od K savršeno.

Prema rezultatu iz teorije brojeva Galoisova grupa $G = \mathrm{Gal}(L/K)$ čuva valuaciju na L. Posebno, G čuva

$$B = \{\alpha \in L \| \alpha| \leq 1\}, \quad \mathfrak{p} = \{\alpha \in L \| \alpha| < 1\}.$$

Neka je Π prost element u L (takav da je $\mathfrak{p} = (\Pi)$). Definiramo niz podgrupa $G \supset G_0 \supset G_1 \supset \cdots$ sljedećim uvjetima:

$$\sigma \in G_i \Leftrightarrow |\sigma\alpha - \alpha| < |\Pi|^i, \quad \text{za sve } \alpha \in B.$$

Grupu G_0 zovemo inercijska grupa, grupu G_1 grupa grananja, a grupe G_i, $i > 1$, više grupe grananja od L nad K.

Grupa klasa ideala

Neka je A Dedekindova domena. Grupa klasa ideala od A, u oznaci $\mathrm{Cl}(A)$, definira se kao $\mathrm{Cl}(A) := \mathrm{Id}(A)/\mathrm{P}(A)$, gdje je s $\mathrm{Id}(A)$ označena grupa razlomljenih ideala u A, a s $\mathrm{P}(A)$ grupa razlomljenih glavnih ideala u A.
U polju algebarskih brojeva K s $\mathrm{Cl}(K)$ često označavamo $\mathrm{Cl}(\mathcal{O}_K)$, gdje je $\mathcal{O}_K$ prsten cijelih brojeva od K.

Grupa $n-$tih korijena iz 1

Neka je K polje i n pozitivan cijeli broj. Element ζ zovemo $n-$ti korijen iz 1 ako je $\zeta^n = 1$. Lako se provjerava da skup svih $n-$tih korijena iz 1 u K čini multiplikativnu grupu koja je podgrupa grupe ne-nul elemenata polja K. Ta podgrupa je ciklička i generirana je primitivnim $n-$tim korijenom iz 1 (vidi Primitivni $n-$ti korijen iz 1).

Grupa $S-$jedinica

Neka je S konačan skup prostih ideala u polju brojeva K. Grupa $S-$jedinica je

$$U(S) = \mathcal{O}_K(S)^\times = \{\alpha \in K | \ \mathrm{ord}_\mathfrak{p}(\alpha) = 0 \text{ za sve } \mathfrak{p} \notin S\}.$$

Na primjer, za $K = \mathbb{Q}$ i $S = \{(2), (3), (5)\}$ je $U(S) = \{\pm 2^k 3^m 5^n | k, m, n \in \mathbb{Z}\}$.
Za $S = \emptyset$ je $U(S) = U_K$, tj. grupa $S-$jedinica odgovara grupi jedinica.

Henselova lema

Neka je k rezidualno polje potpunog prstena diskretne valuacije A. Za unitarni polinom $f(X) \in A[X]$ označimo s $\overline{f}(X)$ sliku od f u $k[X]$. Ako je $\overline{f}(X)$ moguće napisati u obliku $\overline{f} = g_0 h_0$, gdje su g_0 i h_0 unitarni i relativno prosti u $k[X]$, onda se i f može napisati u obliku $f = gh$, gdje su g i h unitarni i takvi da je $\overline{g} = g_o$ i $\overline{h} = h_0$. Dalje, g i h su jedinstveni i $(g, h) = A[X]$.

Hermitski normalni oblik matrice

Neka je A Euklidova domena i $M \in M_n(A)$ $n \times n$ matrica s koeficijentima iz A. Prema rezultatu iz algebre moguće je iz M dobiti gornjetrokutastu matricu sljedećim elementarnim retčanim operacijama:

(1) množenje elemenata jednog retka faktorom i dodavanje tako dobivenih elemenata odgovarajućim elementima drugog retka

(2) zamjena dva retka.

Ove operacije odgovaraju množenju slijeva invertibilnom matricom u $M_n(A)$. Stoga za matricu M postoji invertibilna matrica $U \in M_n(A)$ takva da je $T = (a_{ij}) = UM$ gornje trokutasta matrica koja (uz pretpostavku da je A uređen, npr. $A = \mathbb{Z}$ te da je $\det(M) \neq 0$) zadovoljava sljedeća svojstva:

(1) $a_{ii} > 0$ za sve $i = 1 \dots n$

(2) za fiksni j za sve elementei a_{ij} $j-$og stupca vrijedi $0 \leq a_{ij} < a_{jj}$.

Takva matrica T je jedinstvena i zovemo je Hermitski normalni oblik matrice M.

Hilbertovo polje klasa

Hilbertovo polje klasa polja brojeva K je maksimalno abelovo nerazgranato proširenje polja K.

Indeksi grananja

Neka je A Dedekindova domena i $\mathfrak{p}$ prost ideal u A različit od nul-ideala. U prstenu cijelih B od A definiramo ideal $\mathfrak{p}B := \{\sum a_i b_i | a_i \in \mathfrak{p}, b_i \in B\}$ ($\mathfrak{p}B$ je ideal u B, ali nije nužno prost). S obzirom da je i B Dedekindova domena, postoje prosti ideali $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ u B takvi da je $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$. Brojeve $e_1, \dots, e_g$ zovemo indeksi grananja ideala $\mathfrak{p}$ u pripadnom prstenu cijelih brojeva. Ako je $e_i \geq 2$ za neki $i = 1, \dots, g$, kažemo da se $\mathfrak{p}$ grana.

Inercijska grupa

vidi Grupa grananja

Ireducibilan element

Element integralne domene je ireducibilan ako nije nula niti invertibilan i ako ne može biti prikazan kao produkt dva neinvertibilna elementa.

Jako razgranato proširenje

Proširenje konačnog stupnja L potpunog polja K obzirom na nearhimedsku valuaciju $|\ |$ je jako razgranato ako char(k) $| \ e$, gdje je k rezidualno polje od K, a e pripadni indeks grananja.

Jedinica

Element integralne domene A zovemo jedinica ili invertibilan element ako ima inverz u A.

Kineski teorem o ostacima

Neka su $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ u parovima relativno prosti ideali u prstenu A. Tada za svaki izbor elemenata $x_1, \dots, x_n \in A$ sustav jednadžbi $x \equiv x_i \pmod{\mathfrak{a}_i}$ ima rješenje $x \in A$. Ako je x jedno takvo rješenje, onda su sva ostala rješenja zapisiva u obliku $x + a$ za neki $a \in \cap_{i=1}^n \mathfrak{a}_i$. Dalje, vrijedi $\cap_{i=1}^n \mathfrak{a}_i = \Pi_{i=1}^n \mathfrak{a}_i$. Drugim riječima, imamo egzaktan niz

$$0 \to \mathfrak{a} \to A \to \Pi_{i=1}^n A/\mathfrak{a}_i \to 0,$$

gdje je $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{a}_i = \Pi_{i=1}^{n} \mathfrak{a}_i$.

Kineski teorem o ostacima za module

Neka su $\mathfrak{a_1}, \ldots, \mathfrak{a_n}$ u parovima relativno prosti ideali u prstenu A i neka je M $A-$modul. Tada je niz

$$0 \to \mathfrak{a}M \to M \to \Pi_{i=1}^{n} M/\mathfrak{a}_i M \to 0$$

egzaktan, gdje je $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{a}_i = \Pi_{i=1}^{n} \mathfrak{a}_i$.

Konstanta Minkowskog

vidi Teorem o ogradi Minkowskog

Konveksan podskup vektorskog prostora

Kažemo da je podskup K vektorskog prostora V konveksan ako vrijedi $a, b \in K \Rightarrow \frac{1}{2}(a - b) \in K$.

$n-$ti korijen iz 1

vidi Grupa $n-$tih korijena iz 1

Krasnerova lema

Neka je K potpuno polje s diskretnom nearhimedskom valuacijom $|\ |$, a K^{al} neka je algebarsko zatvorenje od K s valuacijom koja je (jedinstveno) proširenje $|\ |$. Neka su $\alpha, \beta \in K^{al}$ i neka je α separabilan nad $K[\beta]$. Ako je α bliži β nego bilo kojem svom konjugatu (nad K), onda vrijedi $K[\alpha] \subset K[\beta]$.

Lokalan prsten

Prsten A je lokalan ako ima točno jedan maksimalan ideal.

Lokalan uniformizirajući parametar

Neka je K polje s diskretnom nearhimedskom valuacijom $|\ |$. Element $\pi \in K$ koji ima najveću vrijednost manju od 1 zovemo lokalan uniformizirajući parametar. Za takav π vrijedi $|K| = \{c^m | m \in \mathbb{Z}\} \cup \{0\}$, $c = |\pi|$.

Na primjer, za polje $\mathbb{Q}$ i $p-$adsku valuaciju $|\ |_p$ je $\pi = p$, jer je najveća vrijednost apsolutne vrijednosti koja je manja od 1 jednaka upravo $|p|_p = \frac{1}{p}$. U prstenu racionalnih funkcija jedne varijable definiranih u nuli $(\big\{ \frac{f(x)}{g(x)} | g(0) \neq 0 \big\})$, varijabla x je lokalni uniformizirajući parametar.

Lokalno polje

Lokalno polje je polje K s netrivijalnom valuacijom s obzirom na koju je lokalno kompaktno.

Maksimalan ideal

Ideal $\mathfrak{a}$ u prstenu A koji je različit od samog prstena zovemo maksimalan ako ne postoji ideal $\mathfrak{b}$ u A takav da je $\mathfrak{a} \subsetneqq \mathfrak{b} \subsetneqq A$.

Multiplikativan skup
Podskup $S \subset A$ integralne domene A zovemo multiplikativan skup ako $0 \notin S$, $1 \in S$ i S je zatvoren na množenje.

Multiplikativna valuacija
vidi Valuacija

Nakayamina lema
Neka je A lokalan Noetherin prsten i $\mathfrak{a}$ pravi ideal u A. Za konačno generirani $A-$modul M s generatorima $m_1, \ldots, m_n$ definiramo

$$\mathfrak{a}M = \{\sum_{i=1}^{n} a_i m_i | a_i \in \mathfrak{a}\}.$$

Vrijedi sljedeće:

(1) Ako $\mathfrak{a}M = M$, onda $M = 0$.

(2) Ako je N podmodul od M takav da je $N + \mathfrak{a}M = M$, onda $N = M$.

Nearhimedska točka
vidi Teorem o točkama ("primes") u polju brojeva

Nearhimedska valuacija
vidi Valuacija

Nedegenerirana bilinearna forma
Bilinearna forma ψ na konačnodimenzionalnom vektorskom prostoru V dimenzije n nad poljem K je nedegenerirana ako vrijedi neki od sljedećih ekvivalentnih uvjeta:

(1) ψ ima nenul diskriminantu u odnosu na neku (dakle svaku) bazu od V, tj. $\det(\psi(e_i, e_j)) \neq 0$ za bazu $\{e_1, \ldots, e_n\}$ od V

(2) lijeva jezgra od ψ ($\{v \in V | \psi(v, x) = 0$ za sve $x \in V\}$) je trivijalna

(3) desna jezgra od ψ je trivijalna.

Nerazgranat prosti ideal
vidi Razgranat prosti ideal

Nerazgranato proširenje
Proširenje L polja brojeva K je nerazgranato nad K ako nema prostog ideala u $\mathcal{O}_K$ koji je razgranat nad $\mathcal{O}_L$, gdje su $\mathcal{O}_K$ i $\mathcal{O}_L$ prsteni cijelih brojeva polja K i L, redom, tj. iz $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_k^{e_k}$ ($e_1, \ldots, e_k$ su pripadni indeksi grananja) za različite proste ideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ u $\mathcal{O}_L$, slijedi $e_i = 1$, $\forall i = 1, \ldots, k$.

Netrivijalna valuacija
vidi Trivijalna valuacija

Newtonova lema
Neka je A potpun prsten diskretne valuacije $|\ |$ i $f(X) \in A[X]$. Neka za $a_0 \in A$ vrijedi $|f(a_0)| < |f'(a_0)|^2$. Tada postoji jedinstveni korijen a od $f(X)$ takav da vrijedi

$$|a - a_0| \leq \left| \frac{f(a_0)}{f'(a_0)^2} \right|.$$

Newtonov poligon
Neka je K potpuno polje u odnosu na diskretnu valuaciju i ord odgovarajuća aditivna valuacija $\mathrm{ord} : K^\times \to \mathbb{Z}$. Proširimo ord do valuacije $\mathrm{ord} : K^{al} \to \mathbb{Q}$ na algebarskom zatvorenju K^{al} od K. Neka je

$$f(X) = X^n + a_1 X^{n-1} + \ldots + a_n, \quad a_i \in K.$$

Newtonov poligom od $f(X)$ definira se kao konveksna ljuska skupa točaka

$$P_i = (i, \mathrm{ord}(a_i)), \quad i = 0, \ldots, n, a_0 := 1.$$

Niz polja klasa
Neka je K_1 polje brojeva s brojem klasa ideala $h_{K_1} > 1$. Njegovo Hilbertovo polje klasa je nerazgranato proširenje K_2 od K_1 takvo da za pripadnu Galoisovu grupu vrijedi $\mathrm{Gal}(K_2/K_1) \cong \mathrm{Cl}(K_1)$, gdje s $\mathrm{Cl}(K_1)$ označavamo grupu klasa ideala polja K_1. Neka je K_3 Hilbertovo polje klasa od K_2 itd. Na ovaj način dolazimo do niza

$$K_1 \subset K_2 \subset \ldots$$

kojeg zovemo niz polja klasa.

Noetherin modul
Neka je R prsten. R-modul M zovemo Noetherin ako mu je svaki podmodul konačno generiran. Ekvivalentno, svaki rastući niz podmodula se stabilizira odnosno svaki neprazan skup S podmodula sadrži maksimalan element (tj. postoji $M_0 \in S$ takav da za svaki $N \in S$ za koji je $M_0 \subseteq N$ vrijedi $N = M_0$).

Noetherin prsten
Prsten A je Noetherin ako vrijedi neki od sljedećih ekvivalentnih uvjeta:

(1) svaki ideal u A je konačno generiran

(2) svaki rastući niz ideala $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_n \subset \cdots$ se stabilizira, tj. postoji $n_0 \in \mathbb{N}$ takav da je $\mathfrak{a}_n = \mathfrak{a}_{n_0}$ za sve $n \geq n_0$

(3) svaki neprazan skup S ideala u A ima maksimalni element, tj. postoji ideal $\mathfrak{a}$ u S koji nije sadržan ni u jednom idealu iz S.

Norma elementa u polju

Neka je K polje i L natpolje od K. Normu elementa $x \in L$ definiramo kao $N(x) := \Pi_\sigma \sigma x$, gdje je produkt po svim ulaganjima σ polja K u neko fiksirano algebarski zatvoreno polje Ω. Vrijedi: $N(x) \in K$ za svaki $x \in L$. Dalje, norma je multiplikativna funkcija.
Na primjer, neka je $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$. Tada je $\Omega = \mathbb{C}$ i $\sigma \in \{\mathrm{id}, a + b\sqrt{2} \mapsto a - b\sqrt{2}\}$ (to su jedina moguća ulaganja $L \hookrightarrow \mathbb{C}$). Za $x = 1 + \sqrt{2}$ je $N(x) = (1+\sqrt{2})(1-\sqrt{2}) = -1$, a za $x = 2$ je $N(2) = 2 \cdot 2 = 4$.

Norma ideala

Neka je K polje i L natpolje od K, te neka su A i B prsteni cijelih brojeva od K i L, redom. Tada za prosti ideal $\mathfrak{P}$ od B definiramo normu s $N_{L/K}(\mathfrak{P}) := \mathfrak{p}^f$, gdje je $\mathfrak{p} := \mathfrak{P} \cap A$, a f stupanj inercije ideala $\mathfrak{p}$ u $\mathfrak{P}$ dan s $f = [(B/\mathfrak{P}) : (A/\mathfrak{p})]$ (vidi Stupanj inercije). Ovako definiranu normu proširimo po multiplikativnosti − tako dobivamo normu koja idealima u B pridružuje ideale u A; zovemo je norma ideala.

Normalizirana valuacija

Neka je K polje algebarskih brojeva. U svakoj klasi ekvivalencije valuacija na K možemo odabrati tzv. normaliziranu valuaciju na sljedeći način:

(1) za prosti ideal $\mathfrak{p}$ u $\mathcal{O}_K$ ($\mathcal{O}_K$ je pripadni prsten cijelih brojeva) je $|a|_\mathfrak{p} := (\frac{1}{\mathbb{N}(\mathfrak{p})})^{\mathrm{ord}_\mathfrak{p}(a)}$ ($\mathbb{N}(\mathfrak{p})$ je numerička norma ideala $\mathfrak{p}$)

(2) za realno ulaganje $\sigma : K \to \mathbb{C}$ je $|a|_\sigma := |\sigma a|$, gdje je σ obična apsolutna vrijednost

(3) za kompleksno ulaganje $\sigma : K \to \mathbb{C}$ je $|a|_\sigma := |\sigma a|^2$.

Napomena: pod (3) se ne radi doista o valuaciji, jer ne zadovoljava nejednakost trokuta.

Numerička (apsolutna) norma ideala

Neka je $\mathfrak{a}$ nenul ideal u prstenu $\mathcal{O}_K$ cijelih brojeva polja brojeva K. Tada $\mathfrak{a}$ ima konačan indeks u $\mathcal{O}_K$. Numerička norma ideala $\mathfrak{a}$ definira se kao indeks $\mathbb{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$. To je multiplikativna funkcija, a ako je za prost ideal $\mathfrak{p}$ je $\mathbb{N}(\mathfrak{a})$ jednaka broju elemenata u rezidualnom polju.

Ograda Minkowskog

vidi Teorem o ogradi Minkowskog

$\mathfrak{p}$−adska apsolutna vrijednost ($\mathfrak{p}$−adska valuacija)

U polju brojeva K neka je dan nenul prost ideal $\mathfrak{p}$ (shvaćen kao razlomljen ideal). Za svaki nenul element $x \in K$ neka je r jedinstveni cijeli broj takav da $x \in \mathfrak{p}^r$ i $x \notin \mathfrak{p}^{r+1}$. Tada $\mathfrak{p}$−adsku apsolutnu vrijednost $|\ |_\mathfrak{p}$ elementa x definiramo s

$$|x|_\mathfrak{p} := \frac{1}{N(\mathfrak{p})^r},$$

gdje je $N(\mathfrak{p})$ norma ideala $\mathfrak{p}$. Za $x = 0$ definiramo $|0|_\mathfrak{p} := 0$.

Specijalno, u polju $\mathbb{Q}$ za dani prost broj p definiramo $p-$adsku apsolutnu vrijednost ne-nul elementa $x \in \mathbb{Q}$ s

$$|x| := p^{-r},$$

gdje je r cijeli broj definiran izrazom $x = p^r \frac{m}{n}$ za cijele brojeve m i n koji nisu djeljivi s p (takav r je jedinstven). Dalje, za $x = 0$ definiramo $|0|_p := 0$.

$\mathfrak{p}-$adska topologija

Neka je na polju K dana $\mathfrak{p}-$adska apsolutna vrijednost $|\ |_\mathfrak{p}$ koja definira metriku d danu s $d(a,b) := |a-b|_\mathfrak{p}$, a time i topologiju na K. Preciznije, za $a \in K$ skupovi $U(a,\epsilon) = \{x \in K | |x-a|_\mathfrak{p} < \epsilon\}$, $\epsilon > 0$, čine bazu okolina za a. Skup je otvoren ako i samo ako je prikaziv kao unija skupova oblika $U(a,\epsilon)$.

Ovu topologiju zovemo $\mathfrak{p}-$adska topologija na K.

PARI

PARI je program namijenjen radu s teorijom brojeva.

Vidi http://pari.home.ml.org/.

Polje algebarskih brojeva

Polje algebarskih brojeva je proširenje konačnog stupnja polja $\mathbb{Q}$.

Napomena: polje algebarskih brojeva treba razlikovati od polja *svih* algebarskih brojeva, koje je beskonačnog stupnja nad $\mathbb{Q}$ $-$ polje svih algebarskih brojeva je unija svih polja algebarskih brojeva (konačnog stupnja).

Polje razlaganja polinoma

Neka je K polje i $f \in K[X]$ polinom pozitivnog stupnja. Kažemo da je L/K (L je natpolje od K) polje razlaganja polinoma f ako je f moguće napisati kao produkt linearnih faktora s koeficijentima u L i ako je $L = K(u_1, \ldots, u_n)$, gdje su $u_1, \ldots, u_n$ korijeni polinoma f u L.

Polje razlomaka

Za integralnu domenu A polje razlomaka K je polje $K \supset A$ takvo da svaki $c \in K$ ima zapis $c = ab^{-1}$ za neke $a, b \in A$, $b \neq 0$.

Na primjer, $\mathbb{Q}$ je polje razlomaka prstena $\mathbb{Z}$, a $k(X)$ polje razlomaka od $k[X]$.

Potpuno polje

Neka je K polje s netrivijalnom apsolutnom vrijednosti $|\ |$. Polje K je potpuno ako svaki Cauchyjev niz $\{x_n\}$ elemenata iz K konvergira u smislu dane apsolutne vrijednosti $|\ |$.

Praktičan algoritam

Praktičan algoritam je algoritam primjenjiv na računalu.

Primitivni $n-$ti korijen iz 1

Element ζ polja K zovemo primitivni $n-$ti korijen iz 1 ako vrijedi $\zeta^n = 1$ i $\zeta^r \neq 1$ za sve $1 \leq r < n$. Vidi grupa korijena iz 1.

Prirodna gustoća

Neka je S neki podskup skupa svih prostih (cijelih) ideala polja K. Kažemo da S ima prirodnu gustoću δ ako vrijedi

$$\lim_{N\to\infty} \frac{\sharp\{\mathfrak{p} \in S | \mathbb{N}(\mathfrak{p}) \leq N\}}{\sharp\{\mathfrak{p} | \mathbb{N}(\mathfrak{p}) \leq N\}} = \delta,$$

gdje je $\mathbb{N}(\mathfrak{p})$ označava numeričku normu ideala $\mathfrak{p}$.

Prost element

Prost element p integralne domene A je ne-nul neinvertibilan element za koji vrijedi

$$p \mid ab \ (a, b \in A) \Rightarrow p \mid a \text{ ili } p \mid b.$$

vidi Ireducibilan element

Prost ideal

Ideal $\mathfrak{a}$ u prstenu A različit od samog prstena zovemo prost ideal ako vrijedi $ab \in \mathfrak{a} \Rightarrow a \in \mathfrak{a}$ ili $b \in \mathfrak{a}$.

Proširenje polja (konačnog stupnja)

Ako je polje K potpolje polja L, onda L zovemo proširenje polja K, u oznaci L/K. Ako je L (promatrano kao vektorski prostor) konačnodimenzionalni vektorski prostor nad K, onda kažemo da je L proširenje konačnog stupnja polja K, a inače govorimo o proširenju beskonačnog stupnja.

Prsten cijelih brojeva

Cijelo zatvorenje prstena $\mathbb{Z}$ u polju algebarskih brojeva L zovemo prsten cijelih brojeva u L i označavamo s $\mathcal{O}_L$.

Prsten diskretne valuacije

Prsten diskretne valuacije je domena glavnih ideala A koja zadovoljava sljedeća ekvivalentna svojstva:

(1) A ima točno jedan nenul prost ideal

(2) A ima točno jedan prost element, do na relaciju asociranosti

(3) A je lokalan prsten koji nije polje.

Ako je dano polje F s diskretnom valuacijom $|\ |$, onda je pripadni prsten diskretne valuacije $\{x \in F^\times | |x| \geq 0\} \cup \{0\}$.
Na primjer, prsten $\mathbb{Z}_{(p)} = \{\frac{m}{n} \in \mathbb{Q} | p \nmid n\}$ je prsten diskretne valuacije s prostim elementima $\pm p$ i prostim idealom $(p) = \{\frac{m}{n} \in \mathbb{Q} |\ p \,|\, m \text{ i } p \nmid n\}$.

Prsten $S-$cijelih brojeva

Neka je S konačan skup prostih ideala u polju brojeva K. Prsten $S-$cijelih brojeva je

$$\mathcal{O}_K(S) := \cap_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}} = \{\alpha \in K |\ \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0 \text{ za sve } \mathfrak{p} \notin S\}.$$

Za $S = \emptyset$ je $\mathcal{O}_K(S) = \mathcal{O}_K$, gdje je $\mathcal{O}_K$ pripadni prsten cijelih brojeva.

Prvi slučaj Fermatovog posljednjeg teorema

Neka je p neparan prost broj i ζ primitivni n-ti korijen iz 1, $n > 2$. Ako broj klasa od $\mathbb{Q}[\zeta]$ nije djeljiv s p, onda nema cjelobrojnog rješenja (x, y, z) jednadžbe $X^p + Y^p = Z^p$ takvog da $p \nmid xyz$.

Puna rešetka

vidi Rešetka

Razgranat prosti ideal

Neka je A Dedekindova domena i $\mathfrak{p}$ prost ideal u A različit od nul-ideala. U prstenu cijelih B od A definiramo ideal $\mathfrak{p}B := \{\sum a_i b_i | a_i \in \mathfrak{p}, b_i \in B\}$ ($\mathfrak{p}B$ jest ideal u B, ali nije nužno prost). S obzirom da je i B Dedekindova domena, postoje prosti ideali $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ u B takvi da je $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ ($e_1, \ldots, e_g$ su pripadni indeksi grananja). Ako je $e_i > 1$ za bar neki $i = 1, \ldots, g$, onda kažemo da je ideal $\mathfrak{p}$ razgranat u B (ili da se grana u B).

Ako to nije slučaj, kažemo da je prost ideal $\mathfrak{p}$ iz A nerazgranat u B (ili da se ne grana u B).

Razgranato proširenje

Proširenje L polja brojeva K je razgranato nad K ako postoji prosti ideal u $\mathcal{O}_K$ koji je razgranat nad $\mathcal{O}_L$, gdje su $\mathcal{O}_K$ i $\mathcal{O}_L$ prsteni cijelih brojeva polja K i L, redom.

Razlomljen ideal

Razlomljeni ideal u Dedekindovoj domeni A je nenul $A-$podmodul $\mathfrak{a}$ polja razlomaka K od A takav da vrijedi

$$d\mathfrak{a} := \{da | a \in \mathfrak{a}\} \subset A$$

za neki ne-nul $d \in A$ (ili K). Drugim riječima, to je nenul $A-$podmodul od K čiji elementi imaju zajednički nazivnik.

Važno je primijetiti da razlomljeni ideal nije ideal. Stoga $-$ kada je potrebno izbjeći zabunu $-$ ideale u A zovemo cijeli ideali.

Ekvivalentno, razlomljeni ideal od A može se definirati kao ne-nul konačno generirani $A-$podmodul od K: zajednički nazivnik generatora bit će zajednički nazivnik svih elemenata modula i obratno, ako je $a\mathfrak{a}$ cijeli ideal, onda je konačno generiran, što povlači da je i $\mathfrak{a}$ konačno generiran.

Svaki nenul element $b \in K$ definira razlomljeni ideal

$$(b) := bA := \{ba | a \in A\}.$$

Takav razlomljen ideal zovemo glavni (razlomljeni) ideal.

Regulator

Neka je K polje brojeva i $t = r + s - 1$, gdje je r broj realnih $(\sigma_1, \ldots, \sigma_r)$, a s broj parova $(\sigma_{r+1}, \overline{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \overline{\sigma}_{r+s})$ kompleksno-konjugiranih ulaganja K

u $\mathbb{C}$. Neka je $\{u_1, \ldots, u_t\}$ pripadni fundamentalni sistem jedinica. Vektori

$$L(u_i) := (\log|\sigma_1 u_i|, \ldots, \log|\sigma_r u_i|, 2 \cdot \log|\sigma_{r+1} u_i|, \ldots 2 \cdot \log|\sigma_{r+s-1} u_i|) \in \mathbb{R}^t$$

su linearno nezavisni i čine bazu pune rešetke $L(U)$ u $\mathbb{R}^t$. Regulator se definira kao determinanta matrice čiji je $i-$ti redak jednak $L(u_i)$. Regulator je (do na predznak) jednak volumenu fundamentalne domene za $L(U)$.

Relativno prosti ideali

Ideali $\mathfrak{a}$ i $\mathfrak{b}$ u prstenu A su relativno prosti ako vrijedi $\mathfrak{a} + \mathfrak{b} = A$, gdje se $\mathfrak{a} + \mathfrak{b}$ definira kao ideal generiran svim sumama oblika $a + b$, $a \in \mathfrak{a}$, $b \in \mathfrak{b}$.

Rešetka

Rešetka u $n-$dimenzionalnom realnom vektorskom prostoru V je svaka slobodna abelova podgrupa od V generirana nekim izborom linearno nezavisnih vektora prostora V, dakle svaka podgrupa oblika

$$\Lambda = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r,$$

gdje su $e_1, \ldots, e_r$ linearno nezavisni vektori iz V.

Ako je $r = n$, kažemo da je Λ puna rešetka.

Rezidualno polje

U lokalnom prstenu R postoji samo jedan maksimalan ideal $\mathfrak{m}$. Stoga R ima samo jedan kvocijentni prsten $R/\mathfrak{m}$ i on je polje. Ovo polje zovemo rezidualno polje lokalnog prstena R.

U teoriji brojeva se rezidualna polja često vežu uz proste ideale u Dedekindovim domenama. Naime, ako je A Dedekindova domena, onda je svaki ne-nul prost ideal $\mathfrak{p}$ ujedno i maksimalan, pa možemo gledati pripadno rezidualno polje $A/\mathfrak{p}$. Točnije: ako je $\mathfrak{p} \neq 0$ prost ideal u Dedekindovoj domeni A, onda je $A_\mathfrak{p}$ (lokalizacija u $\mathfrak{p}$) lokalni prsten s maksimalnim idealom $\mathfrak{p} \cdot A_\mathfrak{p}$. Vrijedi pritom $A_\mathfrak{p}/(\mathfrak{p} \cdot A_\mathfrak{p}) \cong A/\mathfrak{p} = \mathbb{F}_{\mathbb{N}(\mathfrak{p})}$ (gdje je $\mathbb{F}_{\mathbb{N}(\mathfrak{p})}$ konačno polje s $\mathbb{N}(\mathfrak{p})$ elemenata).

vidi primjer uz Frobeniusov element

Savršeno polje

Kažemo da je polje F savršeno ako vrijede sljedeći ekvivalentni uvjeti:

(1) za karakteristiku polja $\mathrm{char}(F)$ vrijedi ili $\mathrm{char}(F) = 0$ ili $F = F^{\mathrm{char}(F)}$

(2) svaki ireducibilan polinom u $F[X]$ je separabilan

(3) svako algebarsko zatvorenje F^{al} od F je Galoisov nad F

(4) svako algebarsko proširenje od F je separabilno nad F.

Separabilan element

Neka je L natpolje polja K i $u \in L$ algebarski nad K. Kažemo da je u separabilan element nad K ako je ireducibilni polinom tog elementa separabilan (ireducibilan polinom elementa u je polinom $f \in K[X]$ takav da je $\deg(f) \geq 1$, $f(u) = 0$ i za svaki $g \in K[X]$ vrijedi $g(u) = 0 \Leftrightarrow f|g$).

Separabilan polinom

Neka je F polje i $f \in F[X]$ ireducibilan polinom. Kažemo da je f separabilan polinom ako je u nekom polju razlaganja od f (a onda i u svakom) nad F svaki korijen od f jednostruk.

Separabilno proširenje polja

Proširenje L/K polja K je separabilno ako je svaki element tog polja separabilan nad K. To znači da svako konačno proširenje $L \supset M \supset K$ ima točno n ulaganja u fiksirano algebarski zatvoreno polje nad M, gdje je n stupanj proširenja $M \supset K$.

Skup simetričan u odnosu na ishodište

Konveksan skup S u vektorskom prostoru V je simetričan u odnosu na ishodište ako $a \in S$ povlači $-a \in S$ za sve $a \in S$.

Stickelbergerov teorem

Za polje algebarskih brojeva K vrijedi $D(\mathcal{O}_K/\mathbb{Z}) \equiv 0$ ili $1 \bmod 4$, gdje je s $D(\mathcal{O}_K/\mathbb{Z})$ označena diskriminanta proširenja $\mathcal{O}_K/\mathbb{Z}$.

Stupanj inercije

Neka je A Dedekindova domena i $\mathfrak{p}$ prost ideal u A različit od nul-ideala. U prstenu cijelih B od A definiramo ideal $\mathfrak{p}B := \{\sum a_i b_i | a_i \in \mathfrak{p}, b_i \in B\}$ ($\mathfrak{p}B$ jest ideal u B, ali nije nužno prost). S obzirom da je i B Dedekindova domena, postoje prosti ideali $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ u B takvi da je $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ ($e_1, \ldots, e_g$ su pripadni indeksi grananja). Neka prost ideal $\mathfrak{P}$ u B dijeli $\mathfrak{p}$, u oznaci $\mathfrak{P}|\mathfrak{p}$ (to znači da $\mathfrak{P}$ sudjeluje u gornjem rastavu ideala $\mathfrak{p}B$). Kako su A i B Dedekindove domene, to su $A/\mathfrak{p}$ i $B/\mathfrak{P}$ rezidualna polja. Dalje, $A/\mathfrak{p}$ se prirodno ulaže u $B/\mathfrak{P}$ (ulaganjem danim s $a + \mathfrak{p} \mapsto a + \mathfrak{P}$), pa je $B/\mathfrak{P}$ proširenje polja $A/\mathfrak{p}$. Stupanj inercije od $\mathfrak{p}$ u $\mathfrak{P}$, u oznaci $f(\mathfrak{P}/\mathfrak{p})$, definiramo s $f(\mathfrak{P}/\mathfrak{p}) := [B/\mathfrak{P} : A/\mathfrak{p}]$, gdje je s $[B/\mathfrak{P} : A/\mathfrak{p}]$ označen stupanj proširenja $(B/\mathfrak{P})/(A/\mathfrak{p})$.

Stupanj proširenja polja

Natpolje L polja K možemo shvatiti kao vektorski prostor nad K. Stupanj proširenja L/K, u oznaci $[L : K]$, definira se kao dimenzija tog vektorskog prostora: $[L : K] := \dim_K L$. Stupanj proširenja može biti i beskonačan.

Tenzorski produkt modula

Neka je A prsten i M, N i P $A-$moduli. Preslikavanje $f : M \times N \to P$ je $A-$bilinearno ako vrijedi:

(1) $f(m + m', n) = f(m, n) + f(m', n), \forall m, m' \in M, n \in N$

(2) $f(m, n + n') = f(m, n) + f(m, n'), \forall m \in M, n, n' \in N$

(3) $f(am, n) = af(m, n) = f(m, an), \forall a \in A, m \in M, n \in N,$

tj. ako je linearno u svakoj varijabi. Par (Q, f) koji se sastoji od $A-$modula Q i $A-$bilinearnog preslikavanja $f : M \times N \to Q$ zovemo tenzorski produkt $A-$modula M i N ako za svako drugo $A-$bilinearno preslikavanje $f' : M \times N \to P$ vrijedi $f' = \alpha \circ f$, gdje je $\alpha : Q \to P$ jedinstveno linearno preslikavanje. Tenzorski produkt modula postoji i jedinstven je do na jedinstveni izmorfizam (tj. ako su T_1 i T_2 tenzorski produkti modula M i N nad prstenom A, onda postoji jedinstveni izomorfizam abelovih grupa φ takav da je $\varphi(T_1) = T_2$). Označavamo ga s $M \otimes_A N$ i pišemo $(m, n) \mapsto m \otimes n$ za f.

Teorem gustoće Chebotareva

Neka je L Galoisovo proširenje konačnog stupnja polja brojeva K s Galoisovom grupom G i neka je C neka konjugacijska klasa u G (za neki $\tau \in G$ je $C = \{\sigma\tau\sigma^{-1} | \sigma \in G\}$). Promatrajmo skup prostih ideala $\mathfrak{p}$ od K nerazgranatih u L takvih da vrijedi sljedeće: za svaki prost ideal $\mathfrak{P}$ u L (ovdje je $\mathfrak{P}$ shvaćen kao klasa ekvivalencije valuacija na L) koji sadrži $\mathfrak{p}$ Frobeniusov element $(\mathfrak{p}, L/K)$ pripada klasi C. Tada promatrani skup ideala $\mathfrak{p}$ od K ima (prirodnu) gustoću $\delta = \sharp C / \sharp G$.

Napomena: Ako $\mathfrak{P}|\mathfrak{p}$, onda i $\sigma(\mathfrak{P})|\mathfrak{p}$ za $\sigma \in \mathrm{Gal}(L/K)$ i može se dogoditi da je $\sigma(\mathfrak{P}) \neq \mathfrak{P}$. No, u svakom slučaju su $(\mathfrak{P}, L/K)$ i $(\sigma(\mathfrak{P}), L/K)$ konjugirani. Tu klasu konjugiranosti zovemo Frobeniusov element od $\mathfrak{p}$ i označavamo s $(\mathfrak{p}, L/K)$.

Teorem o cijelom zatvorenju Dedekindove domene

Neka je A Dedekindova domena s pripadnim poljem razlomaka K. Cijelo zatvorenje B od A u separabilnom proširenju konačnog stupnja L od K je Dedekindova domena.

Teorem o ciklotomskim poljima

Neka je ζ primitivni $n-$ti korijen iz 1 polja K. Vrijedi:

(1) polje $\mathbb{Q}[\zeta]$ je stupnja $\varphi(n)$ nad $\mathbb{Q}$, gdje je $\varphi(n) = \sharp(\mathbb{Z}/n\mathbb{Z})^\times$

(2) prsten cijelih od $\mathbb{Q}[\zeta]$ je $\mathbb{Z}[\zeta]$

(3) ako je p razgranat u $\mathbb{Q}[\zeta]$, onda vrijedi $p \mid n$. Preciznije, ako je $n = p^r \cdot m$, gdje su m i p relativno prosti, onda je $(p) = (\mathfrak{p}_1 \cdots \mathfrak{p}_s)^{\varphi(p^r)}$ u $\mathbb{Q}[\zeta]$, za različite proste elemente $\mathfrak{p}_i$ iz $\mathbb{Q}[\zeta]$.

Teorem o faktorizaciji ideala u Dedekindovoj domeni

Svaki pravi ideal $\mathfrak{a}$ u Dedekindovoj domeni A može se zapisati u obliku $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p_n}^{r_n}$, gdje su $\mathfrak{p}_i$ jedinstveno određeni međusobno različiti prosti ideali te r_i također jedinstveni i takvi da je $r_i > 0$, $i = 1, \ldots, n$.

Teorem o faktorizaciji u proširenju

Neka je A Dedekindova domena s pripadnim poljem razlomaka K i L separabilno proširenje konačnog stupnja od K. Neka je B cijelo zatvorenje od A u L takvo da je $B = A[\alpha]$ za neki α te neka je $f(X)$ minimalni polinom od α nad K. Označimo s $\mathfrak{p}$ prost ideal u A. Neka su $g_1(X), \ldots, g_r(X) \in A[X]$ međusobno različiti (modulo $\mathfrak{p}$) unitarni polinomi koji su ireducibilni modulo $\mathfrak{p}$, takvi da je s $f(X) \equiv \Pi_{i=1}^r g_i(X)^{e_i}$ (modulo $\mathfrak{p}$) dana faktorizacija polinoma $f(X)$. Tada je s

$$\mathfrak{p}B = \Pi_{i=1}^r (\mathfrak{p}, g_i(\alpha))^{e_i}$$

dana faktorizacija od $\mathfrak{p}B$ u produkt potencija međusobno različitih prostih ideala (($\mathfrak{p}, g_i(\alpha)$) je oznaka za ideal generiran s $\mathfrak{p}$ i $g_i(\alpha)$). Vrijedi $B/(\mathfrak{p}, g_i(\alpha)) \approx (A/\mathfrak{p})[X]/(\overline{g}_i)$ (gdje je $\overline{g}_i = g_i \pmod{\mathfrak{p}}$), pa je stupanj inercije f_i jednak stupnju polinoma g_i, $i = 1, \ldots, r$.

Na primjer, neka je dano kvadratno proširenje $L = \mathbb{Q}(\sqrt{d})$ polja $K = \mathbb{Q}$ ($m = 2$), gdje je $d \in \mathbb{Z}$ različit od 0 i 1 i kvadratno slobodan. Ovdje je $\alpha = \sqrt{d}$ za $d \equiv 2, 3 \pmod 4$ i $\alpha = \frac{1+\sqrt{d}}{2}$ za $d \equiv 1 \pmod 4$; tražimo minimalni polinom $f(X)$ od α nad $\mathbb{Q}$. Imamo sljedeće mogućnosti za f:

(1) ako je $d \equiv 2, 3 \pmod 4$, onda je $f(X) = X^2 - d$

(2) ako je $d \equiv 1 \pmod 4$, onda je $f(X) = X^2 - X + \frac{1-d}{4}$.

Neka je sada $d = -5$ i $p = 2$. tražimo faktorizaciju prostog ideala $\mathfrak{p} = (2)$ u pripadnom prstenu cijelih brojeva $\mathcal{O}_L$ za $L := \mathbb{Q}(\sqrt{-5})$. Kako je $-5 \equiv 3 \pmod 4$, to je minimalni polinom za $\alpha = \sqrt{-5}$ dan s $f(X) = X^2 + 5$. Kako je $X^2 + 5 \equiv (X+1)^2 \pmod 2$, možemo uzeti da je $g_1(X) = X + 1$ ($e_1 = 2$), pa imamo $(2)\mathcal{O}_L = (2, g_1(\alpha))^2 = (2, \sqrt{-5} + 1)^2$. Time je dana faktorizacija ideala $(2)\mathcal{O}_L$ u produkt potencija prostih ideala u $\mathcal{O}_L$. Tu je diskriminanta $D = 4d$, tj. $2|D$, pa se (2) grana kako je eksplicitno i pokazano.

Za $d = -1$ imamo sljedeće:

(1) za $\mathfrak{p} = (2)$ je $f(X) \equiv (X+1)^2 \pmod 2$, tj. $e_1 = 2$ ((2) se cijepa)

(2) za $\mathfrak{p} = (3)$ je $f(X) \equiv X^2 + 1 \pmod 3$, tj. $e_1 = 1$ ((3) je prost)

(3) za $\mathfrak{p} = (5)$ je $f(X) \equiv (X-2)(X+2) \pmod 5$, tj. $e_1 = e_2 = 1$ ((5) se grana).

Teorem o grupi razlomljenih ideala

Neka je A Dedekindova domena. Skup $\mathrm{Id}(A)$ razlomljenih ideala u A čini slobodnu abelovu grupu s jedinicom generiranu prostim idealima. Umnožak dva razlomljena ideala $\mathfrak{a}$ i $\mathfrak{b}$ u A pri tom se definira na sljedeći način:

$$\mathfrak{a} \cdot \mathfrak{b} := \{\sum a_i b_i | a_i \in \mathfrak{a}, b_i \in \mathfrak{b}|\}.$$

Lako se provjeri da je $\mathfrak{a} \cdot \mathfrak{b}$ opet razlomljen ideal, tj. da je množenje dobro definirana binarna operacija. Također, nije teško provjeriti da na $(\mathrm{Id}(A), \cdot)$ vrijede aksiomi grupe. Neutralni element u ovoj grupi je A.

Teorem o invarijantnim faktorima

Neka je A Dedekindova domena, a $M \supset N$ konačno generirani torzijski slobodni $A-$moduli istog ranga m. Tada postoje elementi $e_1, \ldots, e_m \in M$, razlomljeni ideali $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ i cijeli ideali $\mathfrak{b}_1, \ldots, \mathfrak{b}_m$ takvi da je

$$M = \mathfrak{a}_1 e_1 \oplus \cdots \oplus \mathfrak{a}_m e_m, \qquad N = \mathfrak{a}_1 \mathfrak{b}_1 e_1 \oplus \cdots \oplus \mathfrak{a}_m \mathfrak{b}_m e_m.$$

Ideali $\mathfrak{b}_1, \ldots, \mathfrak{b}_m$ su jedinstveno određeni parom $M \supset N$ i zovu se invarijantni faktori modula N u M.

Teorem o jedinicama

Grupa jedinica U_K u polju brojeva K je konačno generirana grupa ranga $r+s-1$, gdje je r broj realnih, a s broj parova kompleksno-konjugiranih ulaganja K u $\mathbb{C}$.

vidi Fundamentalni sistem jedinica

Teorem o konstantama grananja

Neka A Dedekindova domena s pripadnim poljem razlomaka K, a B cijelo zatvorenje od A u separabilnom proširenju L/K konačnog stupnja m. Neka je dan $\mathfrak{p}$ prost ideal u A, različit od nul-ideala. Definiramo s $\mathfrak{p}B$ ideal u B generiran s $\mathfrak{p}$ na sljedeći način: $\mathfrak{p}B := \{\sum a_i b_i | a_i \in \mathfrak{p}, b_i \in B|\}$ (to jest ideal, ali nije nužno prost). Neka su $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ prosti ideali u B koji dijele ideal $\mathfrak{p}$, što znači da ti ideali sudjeluju u rastavu ideala $\mathfrak{p}B$ na proste faktore: $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_{\mathfrak{g}}{}^{e_g}$ ($e_1, \ldots, e_g$ su tzv. indeksi grananja). Dalje, neka su $f_i := [(B/\mathfrak{P}_{\mathfrak{i}}) : (A/\mathfrak{p})]$ pripadni stupnjevi inercije. Tada vrijedi

$$\sum_{i=1}^{g} e_i f_i = m.$$

Ako je L Galoisovo nad K, svi su indeksi grananja međusobno jednaki, kao i svi stupnjevi inercije, pa vrijedi

$$efg = m.$$

Na primjer, neka je dano kvadratno proširenje $L = \mathbb{Q}(\sqrt{d})$ polja $K = \mathbb{Q}$ ($m = 2$), gdje je d kvadratno slobodan cijeli broj različit od 0. Ako promatramo prost broj p u $A = \mathbb{Z}$, onda imamo nekoliko mogućnosti za faktorizaciju prostog ideala $\mathfrak{p} := (p)$ u prstenu cijelih brojeva $\mathcal{O}_L$ polja L:

(1) $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^2$ za neki prost ideal $\mathfrak{P}$ u $\mathcal{O}_L$. U ovom slučaju $\mathfrak{p}$ se grana i imamo $e = 2$, $f = 1$ (to je kada $p|D$, tj. $\left(\frac{D}{p}\right) = 0$, gdje je D diskriminanta od $K/\mathbb{Q}$)

(2) $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}$ za neki prost ideal $\mathfrak{P}$ u $\mathcal{O}_L$. Ovdje $\mathfrak{p}$ ostaje prost i vrijedi $e = 1$, $f = 2$ ($\left(\frac{D}{p}\right) = -1$)

(3) $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2$ za različite proste ideale $\mathfrak{P}_1$ i $\mathfrak{P}_2$ u $\mathcal{O}_L$. Ovdje je $e_1 = e_2 = 1$, $f_1 = f_2 = 1$ ($\left(\frac{D}{p}\right) = 1$).

Teorem o modulima nad Dedekindovom domenom

Neka je A Dedekindova domena. Vrijedi sljedeće:

(1) Svaki konačno generirani torzijski slobodan A-modul je izomorfan direktnoj sumi razlomljenih ideala

(2) Dva konačno generirana torzijski slobodna $A-$modula $M \approx \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m$ i $N \approx \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_n$ su izomorfni ako i samo ako je $m = n$ i $\Pi\mathfrak{a}_i \equiv \Pi\mathfrak{b}_i$ modulo glavni ideali.

Teorem o ogradi Minkowskog

Neka je K proširenje od $\mathbb{Q}$ stupnja n, a $\triangle_K$ diskriminanta proširenja $K/\mathbb{Q}$ (vidi Diskriminanta polja algebarskih brojeva). Neka je $2s$ broj čisto kompleksnih ulaganja polja K. Tada postoji skup reprezentanata grupe klasa ideala od K koji se sastoji od cijelih ideala $\mathfrak{a}$ takvih da vrijedi

$$\mathbb{N}(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s |\triangle_K|^{\frac{1}{2}},$$

gdje $\mathbb{N}(\mathfrak{a})$ označava numeričku normu ideala $\mathfrak{a}$. Broj s desne strane ove nejednakosti zovemo ograda Minkowskog, u oznaci B_K, a broj $C_K = \frac{n!}{n^n}(\frac{4}{\pi})^s$ konstanta Minkowskog.

Teorem o proširenju nearhimedske valuacije

Neka je K polje potpuno s obzirom na diskretnu nearhimedsku valuaciju $|\ |_K$, a L separabilno proširenje od K stupnja n. Valuacija $|\ |_K$ se na jedinstven način proširuje do diskretne valuacije $|\ |_L$ na L i L je potpuno u odnosu na $|\ |_L$. Za svaki $\beta \in L$ vrijedi

$$|\beta|_L = |\mathrm{N}_{L/K}(\beta)|_K^{\frac{1}{n}},$$

gdje je s $\mathrm{N}_{L/K}(\beta)$ označena norma elementa $\beta \in L$.

Teorem o prstenu cijelih

Skup cijelih elemenata u polju L nad integralnom domenom A čini prsten.

Teorem o razgranatim prostim idealima

Neka je L proširenje konačnog stupnja polja brojeva K, A Dedekindova domena u K s pripadnim poljem razlomaka K (npr. $A = \mathcal{O}_K$), a B cijelo zatvorenje od A u L. Uz pretpostavku da je K polje brojeva i B slobodni $A-$modul (to je točno ako je A domena glavnih ideala) vrijedi da se prosti ideal $\mathfrak{p}$ grana u L ako i samo ako $\mathfrak{p}|D(B/A)$ (s $D(B/A)$ je označena diskriminanta proširenja B/A). Posebno, samo konačno mnogo prostih ideala se grana.

Na primjer, neka je $A = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{d})$ i $B = \mathcal{O}_L$ (prsten cijelih polja L), gdje je d kvadratno slobodan cijeli broj različit od 0 i 1. Imamo dvije mogućnosti:

(1) ako je $d \equiv 2, 3 \pmod 4$, onda $D(B/A) = 4d$ i $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$

(2) ako je $d \equiv 1 \pmod 4$, onda $D(B/A) = d$ i $\mathcal{O}_L = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Ako je npr. $d = -1$, onda je $D = -4$, pa za $p = 2$ zbog $2|(-4)$ imamo grananje.

Teorem o točkama ("primes") u polju brojeva

Neka je K polje algebarskih brojeva. Točkama ("primes") u K zovemo klase ekvivalencija valuacija na K (vidi Ekvivalentne valuacije). Postoji točno jedna točka ("prime") u K:

(1) za svaki prost ideal $\mathfrak{p}$

(2) za svako realno ulaganje

(3) za svaki par konjugirano-kompleksnih ulaganja.

Na primjer, za $K = \mathbb{Q}$ nearhimedske točke odgovaraju prostim brojevima, a arhimedska arhimedskoj apsolutnoj vrijednosti (valuaciji) i označava se s ∞. Za $K = \mathbb{Q}(\sqrt{d})$ gdje je $d > 0$ kvadratno slobodan cijeli broj različit od 0 i 1 za svaki prosti ideal u pripadnom prstenu cijelih postoji po jedna nearhimedska točka i dvije arhimedske točke koje odgovaraju ulaganjima $a + b\sqrt{d} \mapsto a + b\sqrt{d}$, odnosno $a + b\sqrt{d} \mapsto a - b\sqrt{d}$. Za slučaj $d < 0$ imamo jednu nearhimedsku točku.

Teorem o točkama u rešetki

Neka je D_0 fundamentalni paralelepiped za punu rešetku Λ u konačnodimenzionalnom realnom vektorskom prostoru V i S izmjeriv podskup u V (u smislu mjere μ). Ako je $\mu(S) > \mu(D_0)$, onda S sadrži međusobno različite točke α i β takve da je $\beta - \alpha \in \Lambda$.

Teorem - produktna formula

Neka je K polje algebarskih brojeva. Nazovimo točkama ("primes") u K klase ekvivalencija valuacija na K (nearhimedskih i arhimedskih). Za svaku točku v neka je $|\ |_v$ pripadna normalizirana valuacija. Za svaki $\alpha \in K$ tada vrijedi

$$\Pi|\alpha|_v = 1,$$

gdje se u produktu nalaze sve točke iz K.

Specijalno, u polju $\mathbb{Q}$ za prost broj p označimo s $|\ |_p$ odgovarajuću normaliziranu valuaciju na $\mathbb{Q}$. Tada za svaki ne-nul racionalni broj a vrijedi

$$\Pi|a|_p = 1,$$

gdje se u produktu nalaze sve točke p, uključivši i ∞.

Točke ("primes") u polju brojeva

vidi Teorem o točkama ("primes") u polju brojeva

Torzijski slobodan modul

Modul M nad prstenom A bez djelitelja nule je torzijski slobodan $A-$modul ako jednakost $a.m = 0$ povlači $a = 0$ ili $m = 0$, za sve $a \in A$, $m \in M$. Primjeri torzijski slobodnih modula nad prstenom A: sam prsten A, kao i svi ne-nul lijevi ideali u A.

Trag elementa proširenja polja

Neka je L/K proširenje stupnja n polja K i neka je $\{a_1, \dots, a_n\}$ baza od L kao vektorskog prostora nad K. Tada proizvoljan $y \in L$ definira $K-$linearno preslikavanje $\varphi_y : x \mapsto yx$ na L. Trag tog preslikavanja je dobro definiran. Trag elementa y u L u bazi $\{a_1, \dots, a_n\}$, u oznaci $\mathrm{Tr}_{L/K}(y)$, definiramo s $\mathrm{Tr}_{L/K}(y) := \mathrm{tr}\varphi_y$. Takva definicija traga ne ovisi o izboru baze L nad K.

Trivijalna valuacija

vidi Valuacija

Valuacija

U polju K funkciju $x \to |x| : K \to \mathbb{R}$ zovemo (multiplikativna) (arhimedska) valuacija odnosno apsolutna vrijednost ako zadovoljava sljedeća svojstva:

(1) $|x| > 0$ za sve $x \in K$, osim za $x = 0$; $|0| = 0$

(2) $|xy| = |x| \cdot |y|$ za sve $x, y \in K$

(3) $|x + y| \leq |x| + |y|$ za sve $x, y \in K$ (nejednakost trokuta).

Ako umjesto (3) vrijedi jači uvjet

(3') $|x + y| \leq \max \{|x|, |y|\}$ za sve $x, y \in K$,

onda $|\ |$ zovemo nearhimedska valuacija.

Na svakom polju moguće je definirati trivijalnu valuaciju: $|a| = 1$ za sve $a \neq 0$. Specijalno, na konačnim poljima ne postoje valuacije različite od trivijalnih (zato što su svi nenul elementi konačnog reda korijeni iz 1).

Valuacija $|\ |$ je diskretna ako je $|K^{\times}|$ diskretna podgrupa od $\mathbb{R}_{>0}$.

vidi $\mathfrak{p}-$adska apsolutna vrijednost

Verižni razlomak

Izraz oblika

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

gdje je a_0 realan broj, a $a_1, a_2, \ldots$ pozitivni realni brojevi, zovemo veriži razlomak. Skraćeni zapis glasi $[a_0, a_1, a_2, \ldots]$.

Viša grupa grananja

vidi Grupa grananja