Prosti brojevi oblika \(x^2\)+\(ny^2\)

Andrašek, Alen

Prosti brojevi oblika \(x^2\)+\(ny^2\)

Andrašek, Alen

Master's thesis / Diplomski rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:804311

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Alen Andrašek

PROSTI BROJEVI OBLIKA $x^2 + ny^2$

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Filip Najman

Zagreb, studeni, 2020.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Notacija

O_K	Prsten algebarskih cijelih brojeva u polju K
d_K	diskriminanta polja brojeva K
$h(D)$	Broj klasa formi diskriminante D
$C(D)$	Grupa klasa formi diskriminante D
$h(O_K)$	Broj klasa ideala u prstenu O_K
$C(O_K)$	Grupa klasa ideala u prstenu O_K
$h(K)$, $C(K)$	Isto što i $h(O_K)$, $C(O_K)$ (respektivno)
$\mathrm{SL}_2(\mathbb{Z})$	2x2 matrice determinante 1 s koeficijentima iz $\mathbb{Z}$
$\mathrm{Gal}(L/K)$	Galoisova grupa konačnog proširenja $K \subset L$
$[L : K]$	Stupanj konačnog proširenja $K \subset L$
$[x_1, ..., x_n]$	Ideal generiran elementima $x_1, ..., x_n$ u nekom prstenu
$N(\mathfrak{a})$	Norma ideala $\mathfrak{a}$
I_K	Grupa razlomljenih ideala u O_K
P_K	Grupa glavnih razlomljenih ideala u O_K
$I_K(f)$	Grupa razlomljenih O_K-ideala relativno prostih s f
$I(O, f)$	Grupa razlomljenih O-ideala relativno prostih s f
$((L/K)/\mathfrak{B})$	Artinov simbol od $\mathfrak{B} \subset O_L$
$((L/K)/\mathfrak{p})$	Artinov simbol od $\mathfrak{p} \subset O_K$ (Abelovski slučaj)

Uvod

Reprezentacija brojeva kvadratnim formama je jedan od najpoznatijih problema u teoriji brojeva. Uveo ga je veliki francuski matematičar Pierre de Fermat. On je prvi uočio svojstvo da za neparne proste brojeve p vrijedi:

$$p = x^2 + y^2 \iff p = 4k + 1, \tag{1}$$

gdje su x, y, k neki cijeli brojevi. U uvodu ćemo vidjeti da promatranje ovog problema za proste brojeve rješava problem i općenito za prirodne brojeve. Stoga se ovaj rad koncentrira na *proste brojeve oblika* $x^2 + ny^2$.
U uvodu ćemo raspraviti o elementarnim tehnikama i njihovim dosezima. Navest ćemo kratki povijesni razvoj i posebne slučajeve čijom generalizacijom ćemo doći do iskaza glavnog teorema koji ovaj rad obrađuje.
Nakon uvoda posvetit ćemo se dokazu glavnog teorema o reprezentaciji brojeva u obliku $x^2 + ny^2$. U pravilu će se koristiti dobro poznate metode iz algebre. Jedino za postojanje polja klasa ćemo se pozvati na teške teoreme teorije polja klasa koju nećemo izvoditi u potpunosti, ali se nadamo ilustrirati upravo primjenom na ovaj problem. Usput ćemo dokazati i slavni Kronecker-Weberov teorem kao lagani korolar.
Potrebno predznanje obuhvaća standardni kurs algebre i algebarske teorije brojeva (iako se većina pojmova može brzo pojmiti i bez predznanja algebarskih tehnika). Elementarni dio teorije ćemo uglavnom navoditi bez dokaza.
Za kraj ćemo ilustrirati konkretni algoritam koji će nam dati eksplicitno rješenje glavnog problema. Nećemo dokazivati valjanost jer se tu radi o teoriji kompleksnog množenja koja bi nas odvela predaleko. Primjere iz uvoda ćemo riješiti općenitim algoritmom i pokazati kako posebni slučajevi iz uvoda (jednostavno) slijede iz opće teorije koju ćemo razviti. Promotrit ćemo još pokoji posebno odabrani primjer.
Glavni izvor na kojem se temelji rad je [1]. Povijesni citati će biti uglavnom iz [2]. Pokoju informaciju smo uzeli iz izvornih članaka koji će biti citirani.

Poglavlje 1

Povijest

1.1 Fermat i Euler

Od najranijih povijesnih razmatranja ljudi su uočavali zanimljiva svojstva brojeva. Jedno od prvih takvih pitanja je bilo: kada je moguće *kvadrat* prikazati kao sumu dva kvadrata tj. pitanje postojanja Pitagorinih trojki $a^2 + b^2 = c^2$. Ako su a, b, c relativno prosti, poznata je parametrizacija

$$\begin{aligned} a &= m^2 - n^2, \\ b &= 2mn, \\ c &= m^2 + n^2, \end{aligned}$$

gdje su m, n relativno prosti. Dakle, ako je c^2 suma dva (relativno prosta) kvadrata, onda je i c suma dva (relativno prosta) kvadrata.

Nešto općenitije probleme je razmatrao grčki matematičar Diofant, no, zbog slabog generalnog napretka u matematici prvi značajni rezultati nakon njega su se pojavili tek u novom vijeku. Rezultat koji je sve započeo, naveo je Pierre de Fermat 1640. [2, str. 64]:

$$p = x^2 + y^2 \iff p = 4k + 1, \tag{1.1}$$

za prosti broj p. Iz te tvrdnje i famoznog Brahmaguptinog identita:

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2, \tag{1.2}$$

slijedi teorem o reprentabilnosti proizvoljnog prirodnog broja kao suma dva kvadrata:

Teorem 1.1.1. *Prirodan broj n može se prikazati kao suma dva kvadrata ako i samo ako se svaki njegov prosti faktor oblika* $4k + 3$ *javlja s parnim eksponentom u faktorizaciji od n.*

Tvrdnje koje navodi 1654. u pismu Pascalu [2, str. 80]:

$$\begin{aligned} p = x^2 + 2y^2 &\iff p = 8k + 1 \text{ ili } p = 8k + 3, \\ p = x^2 + 3y^2 &\iff p = 3 \text{ ili } p = 3k + 1, \end{aligned} \tag{1.3}$$

mogu poslužiti za sličnu analizu kada je bilo koji prirodan broj nekog od tih oblika. Iako opći slučaj reprezentacije formom $x^2 + ny^2$ za sve prirodne brojeve *neće* slijediti direktno iz slučaja za proste, svejedno su oni uvijek bazni slučaj koji treba razmotriti. Poteškoće koje mogu nastati možemo vidjeti u zadnjem slučaju koji spominje Fermat. Kao slutnju navodi (vidi [2, str. 82],[1, str. 8]) u pismu Digbyju:

$$\begin{aligned} p &\equiv 3, 7 \bmod 20 \\ q &\equiv 3, 7 \bmod 20 \end{aligned} \qquad \Longrightarrow \qquad pq = x^2 + 5y^2. \tag{1.4}$$

(Ostaci od p, q mogu biti 3 ili 7 u bilo kojoj kombinaciji.) Na primjer, $3 \cdot 7 = 21 = 4^2 + 5 \cdot 1^2$, ali ni 3 ni 7 nisu toga oblika.

Dokaze dosad navedenih tvrdnji za $n = 1, 2, 3$ možemo po prvi put naći kod Eulera. On je koristio Fermatovu metodu beskonačnog spusta. U radu iz 1744, Euler je reformulirao Fermatovu slutnju ([8], [1, str. 17-18]):

$$\begin{aligned} p = x^2 + 5y^2 &\iff p \equiv 1, 9 \bmod 20, \\ 2p = x^2 + 5y^2 &\iff p \equiv 3, 7 \bmod 20. \end{aligned} \tag{1.5}$$

Vidimo da se stvari počinju kompliciratи te bismo se mogli lako izgubiti u svim posebnih pravilima koje se može uočiti u daljnjim slučajevima. Ipak, navedimo još jedan slučaj koji je karakterističan i koji ćemo riješiti generalnim argumentom:

$$\begin{aligned} p = \begin{Bmatrix} x^2 + 14y^2 \\ 2x^2 + 7y^2 \end{Bmatrix} &\iff p \equiv 1, 9, 15, 23, 25, 39 \bmod 56, \\ 3p = x^2 + 14y^2 &\iff p \equiv 3, 5, 13, 19, 27, 45 \bmod 56, \end{aligned} \tag{1.6}$$

Ovdje su u prvom slučaju forme stavljene zajedno jer se samo iz kongruencija *ne može* reći kojom od navedenih formi su predstavljeni. Npr. $23 = 3^2 + 14 \cdot 1^2$, ali $79 = 2 \cdot 6^2 + 7 \cdot 1^2$.

1.2 Začeci moderne teorije

Prvu sistematičnu obradu kvadratnih formi je dao Lagrange. Uveo je pojam ekvivalentnosti kvadratnih formi (u dvije varijable):

Definicija 1.2.1. *Kažemo da su dvije kvadratne forme f i g ekvivalentne ako:*

$$f(x, y) = g(px + qy, rx + sy) \qquad \text{i} \qquad ps - qr = 1. \tag{1.7}$$

Ovdje je riječ o anakronizmu jer je Lagrange dopuštao transformacije sa $ps - qr = \pm 1$, no kasnije se pokazalo da je gornja definicija bolja u praksi. U modernoj terminologiji, jednu formu iz druge možemo dobiti transformacijom koordinata iz $\mathrm{SL}_2(\mathbb{Z})$. To znači da ako neka forma reprezentira dani cijeli broj, onda to čini i svaka njoj ekvivalentna. Gornja relacija je naravno relacija ekvivalencije (odmah slijedi iz toga što je $\mathrm{SL}_2(\mathbb{Z})$ grupa). Bitno svojstvo te relacije je da *čuva* diskriminantu (što se lako provjeri).

Primjer 1.2.2. *Prisjetimo se prvog primjera: forme $f(x, y) = x^2 + y^2$. Njena diskrimanta je $D = -4$. Neka forma ekvivalentna toj je npr. $2x^2 + 6xy + 5y^2$. Uistinu, nalazimo:*

$$2x^2 + 6xy + 5y^2 = (x + 2y)^2 + (x + y)^2,$$
$$x^2 + y^2 = 2(2y - x)^2 + 6(2y - x)(x - y) + 5(x - y)^2.$$

Dakle, $x^2 + y^2$ i $2x^2 + 6xy + 5y^2$ su ekvivalentne jer se mogu svesti jedna na drugu cjelobrojnom transformacijom. Primijetimo i da uistinu imaju istu diskriminantu.

Ustvari *sve* forme diskriminante -4 su ekvivalentne. U to bi se lako uvjerili za koji god primjer, ali to nije odmah očito - zašto ne bi postojala neka druga klasa? Da bi se dao odgovor na to, korisno je izabrati "najboljeg" predstavnika neke klase. Zato je Lagrange uveo pojam reducirane forme.

Definicija 1.2.3. *Kvadratna forma $ax^2 + bxy + cy^2$ naziva se* primitivna *ako je $(a, b, c) = 1$. Primitivna pozitivno definitna kvadratna forma $ax^2 + bxy + cy^2$ naziva se* reducirana *ako vrijedi*

$$|b| \leq a \leq c \quad \text{i} \quad b \geq 0 \text{ ako } |b| = a \text{ ili } a = c.$$

Primijetimo da se u definiciji najednom pojavljuje uvjet *pozitivne definitnosti*. Iako postoji u principu slična teorija za indefinitne forme, ona je složenija te kako su $x^2 + ny^2$ pozitivno definitne, nećemo ju razmatrati. Za (pozitivno definitne) forme vrijedi da se u svakoj klasi ekvivalentnih formi nalazi točno jedna reducirana. Dakle, broj klasa jednak je broju reduciranih formi. Kako je forma pozitivno definitna, vrijedi $D < 0$ pa vidimo da je

$$D = b^2 - 4ac \geq a^2 - 4a^2 = -3a^2,$$

dakle vrijedi $a \leq \sqrt{\frac{-D}{3}}$. Kako je b omeđen s a, ista ograda vrijedi i za b, a c je određen iz relacije $D = b^2 - 4ac$. Stoga smo pokazali:

Teorem 1.2.4. *Broj reduciranih formi dane diskriminante je konačan. Stoga je i broj klasa ekvivaletnih kvadratni formi dane diskriminante konačan. Taj broj označavamo s $h(D)$.*

Vidjet ćemo da će broj klasa biti od fundamentalne važnosti. Broj klasa je barem jedan, o čemu nam govori iduća trivijalna propozicija.

Propozicija 1.2.5. *Za diskriminantu kvadratne forme vrijedi* $D \equiv 0, 1 \bmod 4$. *Obratno, za svaki cijeli broj* $D \equiv 0, 1 \bmod 4$ *postoji barem jedna forma s tom diskriminantom, naime:*

$$\begin{aligned} D &\equiv 0 \bmod 4 \qquad x^2 + \frac{-D}{4}y^2, \\ D &\equiv 1 \bmod 4 \qquad x^2 + xy + \frac{1-D}{4}y^2. \end{aligned} \tag{1.8}$$

Te forme nazivamo glavne *forme.*

Dosad nismo još spomenuli kako točno ovo pomaže pri reprezentaciji brojeva kao kvadratne forme. Odgovor daje iduća tvrdnja [1, Lema 2.5].

Teorem 1.2.6. *Neka je* n *cijeli broj i* p *neparan prost broj koji ne dijeli* n. *Tada je* $\left(\frac{-n}{p}\right) = 1$ *ako i samo ako je* p *reprezentiran reduciranom formom diskriminante* $-4n$.

Dokaz je vrlo elementaran i jednostavan - vidi [1, str. 23-24]. Iz ovoga vidimo da će nužan uvjet za reprezentabilnost prostog broja formom $x^2 + ny^2$ biti $\left(\frac{-n}{p}\right) = 1$ odnosno $p \mid x^2 + ny^2$ za neke rel. proste $x, y \neq 0$. Iznenađujuće je da je taj uvjet katkada i dovoljan! Za primjer, sjetimo se Fermatovih razmatranja za $n = 1, 2, 3$.

Na redu je da sve ovo ilustriramo primjerima. Kada ćemo istraživati koji su prosti brojevi oblika $x^2 + 14y^2$, riječ će biti dakle o formi diskriminante $D = -4 \cdot 14 = -56$.

Primjer 1.2.7. *Nađimo sve reducirane forme diskriminante* $D = -56$. *Metoda je jednostavno prebrojavanje slučajeva. Možemo promatrati po a ili po b. Vrijedi* $|b| \leq a \leq \sqrt{\frac{-D}{3}} < 5$ *pa tražimo* $b \in \{-3, 2, -1, 0, 1, 2, 3, 4\}$ *iz jednadžbe* $b^2 - 4ac = -56$.
Odmah se vidi da je b paran. Ako je $b = 0$ *imamo* $ac = 14$ *i dobivamo* $(a, c) = (1, 14), (2, 7)$. *Za* $b = \pm 2$ *bi vrijedilo* $ac = 15$ *iz čega* $(a, c) = (3, 5)$. *Napokon, za* $b = 4$ *slijedi* $ac = 18$ *no niti jedan a takav da* $b \leq a \leq c$ *ne zadovoljava to. Dakle reducirane forme diskriminante* $D = -56$ *su:*

$$x^2 + 14y^2, \quad 2x^2 + 7y^2, \quad 3x^2 + 2xy + 5y^2, \quad 3x^2 - 2xy + 5y^2.$$

Napomena 1.2.8. *U idućoj tablici navodimo kao primjer većinu reduciranih formi koje će nam u ovom radu trebati.*

$D = -4n$	*Reducirane forme diskriminante* D
-4	$x^2 + y^2$
-8	$x^2 + 2y^2$
-12	$x^2 + 3y^2$
-20	$x^2 + 5y^2$, $2x^2 + 2xy + 3y^2$
-56	$x^2 + 14y^2$, $2x^2 + 7y^2$, $3x^2 \pm 2xy + 5y^2$
-108	$x^2 + 27y^2$, $4x^2 \pm 2xy + 7y^2$
-124	$x^2 + 31y^2$, $5x^2 \pm 4xy + 7y^2$
-256	$x^2 + 64y^2$, $4x^2 + 4xy + 17y^2$, $5x^2 \pm 2xy + 13y^2$

Kompozicija formi

Prisjetimo se Brahmaguptinog identiteta 1.2 - on nam govori da množenjem sume dva kvadrata opet dobivamo sumu dva kvadrata. To nas motivira na definiciju fundamentalnog koncepta *kompozicije* dviju kvadratnih formi.

Definicija 1.2.9. *Neka su $f(x, y)$ i $g(x, y)$ kvadratne forme* iste *diskrimante.* Kompozicija *te dvije forme je kvadratna forma $h(x, y)$ takva da vrijedi:*

$$f(x, y)g(z, w) = h(A_1(x, y, z, w), A_2(x, y, z, w)) \tag{1.9}$$

i A_i su oblika $a_ixz + b_ixw + c_iyz + d_iyw$.

I $h(x, y)$ je diskriminante D. Drugim riječima, množenjem dvije reducirane forme iste diskriminante dobit ćemo izraz koji će opet biti reprezentiran nekom formom te diskriminante. U općem obliku je ovo prvi promatrao Legendre. Nažalost, koeficijenti se mogu namjestiti tako da rezultirajuća forma ne mora ležati uvijek u istoj klasi (vidi [1, str. 38]). Da popravimo situaciju, možemo zahtjevati da kompozicija bude *direktna*.

Definicija 1.2.10. *Direktna kompozicija dvije forme je kompozicija kao gore uz uvjete*

$$a_1b_2 - a_2b_1 = f(1, 0), \qquad a_1c_2 - a_2c_1 = g(1, 0).$$

Kompozicija klasa formi se čini preko kompozicije reprezentanata. S tom definicijom Gauss je u Disquisitiones Arithmeticae [7] dokazao (još jedan) fundamentalni teorem:

Teorem 1.2.11. *Klase formi čine grupu obzirom na direktno komponiranje. Tu grupu nazivamo* grupa klasa formi *i označavamo $C(D)$.*

Dokaz se naravno nalazi u Disquisitiones, ali to je samo jedan način definiranja te operacije, te se u [1] mogu naći jednostavniji načini bazirani na radu Dirichleta i kasnijoj teoriji ideala. Poanta je poistovjetiti prvo forme s idealima pa na njima definirati množenje. Kasnije ćemo navesti nešto od potrebne teorije, ali nećemo ulaziti u detalje. Navedimo samo eksplicitni primjer komponiranja formi diskriminante -20 koji je prvi dao Lagrange (primijetimo da je kompozicija direktna):

Propozicija 1.2.12. *Neka su $f_0(x, y) = x^2+5y^2$ i $f_1(x, y) = 2x^2+2xy+3y^2$, dakle reducirane forme s $D = -20$. Vrijedi:*

$$\begin{aligned} f_0(x, y)f_0(z, w) &= f_0(xz - 5yw, xw + yz), \\ f_0(x, y)f_1(z, w) &= f_1(xz - yz - 3yw, xw + 2yz + yw), \\ f_1(x, y)f_1(z, w) &= f_0(2xz + xw + yz - 2yw, xw + yz + yw). \end{aligned} \tag{1.10}$$

Sada je jasnija i Eulerova slutnja (1.5) kao poseban slučaj komponiranja ($2 = 2 \cdot 1^2 + 2 \cdot 1 \cdot 0 + 3 \cdot 0^2$). Iz ovoga se lako izvede tvrdnja o reprezentaciji prostog broja formom $x^2 + 5y^2$. Vidi [1, str. 30].

Vidimo da je $x^2 + 5y^2$ neutralni element obzirom na komponiranje! Općenito glavne forme (1.2.5) čine neutralni element u grupi klasa formi. I elemente reda 2 možemo lako prepoznati (vidi [1, str. 47]):

Propozicija 1.2.13. *Reducirana forma $f(x, y) = ax^2 + bxy + cy^2$ diskriminante D ima red ≤ 2 u grupi klasa formi ako i samo ako je $b = 0$ ili $a = b$ ili $a = c$.*

1.3 Gauss i zakoni reciprociteta

Ne stajući pri istraživanju kvadratnih formi i kvadratnog reciprociteta, Gauss je dokazao prilikom istraživanja kubnog i bikvadratnog reciprociteta iduće dvije (Eulerove) slutnje:

$$\begin{aligned} p = x^2 + 27y^2 &\iff \left(\frac{-3}{p}\right) = 1,\ t^3 \equiv 2 \bmod p, \\ p = x^2 + 64y^2 &\iff \left(\frac{-1}{p}\right) = 1,\ u^4 \equiv 2 \bmod p, \end{aligned} \tag{1.11}$$

za neke $t, u \in \mathbb{Z}$ tj. 2 je kubni (respektivno, bikvadratni) ostatak mod p. Dokazi su standardni korolari viših zakona reciprociteta (posebno za broj 2 postoje suplementarni zakoni, slično kao kod kvadratnog reciprociteta). Ovdje dajemo elementarni dokaz druge tvrdnje, od Dirichleta. Navedimo prvo pravila igre - i za više zakone reciprociteta možemo definirati analogon Legendreovog simbola. Nama će trebati samo bikvadratni simbol:

$$\left(\frac{a}{p}\right)_4 = a^{\frac{p-1}{4}}.$$

Primijetimo da ovo podsjeća na Eulerov kriterij. Uistinu, ako je simbol jednak 1 tada je $a^{\frac{p-1}{2}} = 1$, pa je a kvadratni ostatak mod p, ali onda isti argument daje da je i $\sqrt{a}$ kvadratni ostatak mod p tj. a je bikvadratni ostatak mod p. Obratno, ako je $t^4 \equiv a \bmod p$ za neki t, onda je $a^{\frac{p-1}{4}} = t^{p-1} = 1$.

Teorem 1.3.1. *Vrijedi $p = x^2 + 64y^2$ ako i samo ako je $p = 4k + 1$ i 2 bikvadratni ostatak mod p.*

Dokaz. Neka je $p = 4k + 1$. Tada je p suma dva kvadrata $p = a^2 + b^2$ i recimo da je a neparan. Imamo:

$$\left(\frac{a+b}{p}\right) \equiv (a+b)^{\frac{p-1}{2}} \equiv (2ab)^{\frac{p-1}{4}} \equiv 2^{\frac{p-1}{4}}(-1)^{\frac{p-1}{8}} a^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right)_4 (-1)^{\frac{p-1}{8}} \left(\frac{a}{p}\right) \bmod p.$$

Legendreove simbole iz gornje relacije možemo elementarno izračunati. Kako je a neparan, možemo koristiti svojstva Jacobijevog simbola:

$$\left(\frac{a+b}{p}\right) = \left(\frac{p}{a+b}\right) = \left(\frac{2p}{a+b}\right)\left(\frac{2}{a+b}\right) = \left(\frac{(a+b)^2+(a-b)^2}{a+b}\right)\left(\frac{2}{a+b}\right) = (-1)^{\frac{(a+b)^2-1}{8}},$$
$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{a^2+b^2}{a}\right) = 1.$$

Spajajući, dobivamo:

$$\left(\frac{2}{p}\right)_4 = (-1)^{\frac{(a+b)^2-1}{8} - \frac{a^2+b^2-1}{8}} = i^{\frac{ab}{2}}.$$

Odavde odmah vidimo - izraz je 1 ako i samo je b djeljiv s 8. □

1.4 Glavni teorem

Dalje tokom povijesti ovaj problem se rješavao sporadično. Tako npr. Kronecker navodi idući teorem:

Teorem 1.4.1. *Vrijedi ekvivalencija*

$$p = x^2 + 31y^2 \iff (t^3 - 10t)^2 + 31(t^2-1)^2 \equiv 0 \bmod p.$$

za neki $t \in \mathbb{Z}$. Ovo se možda čini malo različito od prijašnjeg - gdje je uvjet $\left(\frac{-31}{p}\right) = 1$? Ustvari i nije duboko sakriven - vidimo da je zahtjev ekvivalentan:

$$(t^3 - 10t)^2 \equiv -31(t^2-1)^2 \bmod p$$

pa -31 mora biti kvadratni ostatak mod p. Nakon korjenovanja nam preostaje odrediti rješivost nekog od dva kubna polinoma - vidjet ćemo da je svejedno koji uzmemo. Ovaj teorem od Kroneckera je proizašao kao korolar proučavanja tzv. Abelovskih jednadžbi. Prirodno su se tu pojavljivali i *singularni moduli* vezani uz tzv. *kompleksno množenje*. O ovom nećemo puno moći reći, no generalni rezultat koji će biti naveden na kraju slijedi upravo iz te teorije.

Promotrimo sve primjere koje smo do sada naveli (gdje je prost broj $p > n$ da izbjegnemo trivijalne kontraprimjere):

$$\begin{aligned}
p = x^2 + y^2 &\iff \left(\frac{-1}{p}\right) = 1,\\
p = x^2 + 2y^2 &\iff \left(\frac{-2}{p}\right) = 1,\\
p = x^2 + 3y^2 &\iff \left(\frac{-3}{p}\right) = 1,\\
p = x^2 + 5y^2 &\iff \left(\frac{-5}{p}\right) = 1 \text{ i } t^2 + 1 \equiv 0 \bmod p \text{ ima rješenje},\\
p = x^2 + 27y^2 &\iff \left(\frac{-27}{p}\right) = 1 \text{ i } t^3 \equiv 2 \bmod p \text{ ima rješenje},\\
p = x^2 + 64y^2 &\iff \left(\frac{-64}{p}\right) = 1 \text{ i } t^4 \equiv 2 \bmod p \text{ ima rješenje},\\
p = x^2 + 31y^2 &\iff \left(\frac{-31}{p}\right) = 1 \text{ i } t^3 - 10t + \sqrt{-31}(t^2 - 1) \equiv 0 \bmod p.
\end{aligned}$$

Prvi uvjet nas ne treba iznenaditi jer je nužan po (1.2.6). Puno zanimljiviji je drugi uvjet - vidimo da se kao uvjet pojavljuje rješivost neke polinomijalne jednadžbe. U Gaussovim korolarima su to posebni slučajevi zakona reciprociteta od 2, ali vidimo da je u Kroneckerovom slučaju nužno nešto kompliciranije. Primijetimo samo da je moguće zaobići pojavu $\sqrt{-31}$ u zadnjem polinomu tako da se uzme neki cijeli broj čiji je kvadrat 31 modulo p. Obzirom na prvi uvjet, takav postoji.

Kao u Kroneckerovom teoremu, ne bi bilo teško sakriti uvjet s Legendreovim simbolom u polinom dvostruko većeg stupnja, no preferiramo ovaj pristup koji će ispasti prirodniji.

Razmislimo sada o problemu na malo drugačiji način. Za $n = 27$ vidimo da je uvjet zdesna ekvivalentan tome da u $\mathbb{F}_p$ moraju postojati $\sqrt{-27}$ i $\sqrt[3]{2}$ (kao pripadni elementi polja). Promotrimo koje elemente tražimo da postoje:

$$\begin{aligned}
p = x^2 + y^2 &\iff \text{Postoji } \sqrt{-1} \bmod p,\\
p = x^2 + 2y^2 &\iff \text{Postoji } \sqrt{-2} \bmod p,\\
p = x^2 + 3y^2 &\iff \text{Postoji } \sqrt{-3} \bmod p,\\
p = x^2 + 5y^2 &\iff \text{Postoje } \sqrt{-5} \text{ i } \sqrt{-1} \bmod p,\\
p = x^2 + 27y^2 &\iff \text{Postoje } \sqrt{-27} \text{ i } \sqrt[3]{2} \bmod p,\\
p = x^2 + 64y^2 &\iff \text{Postoje } \sqrt{-64} \text{ i } \sqrt[4]{2} \bmod p,\\
p = x^2 + 31y^2 &\iff \text{Postoje } \sqrt{-31} \text{ i } t \bmod p,
\end{aligned}$$

gdje je u zadnjem primjeru t nultočka polinoma $t^3 - 10t + \sqrt{-31}(t^2 - 1)$. Vidjet ćemo da će nam se na putu do rješenja problema prirodno pojaviti proširenja od $\mathbb{Q}$ algebarskim cijelim brojevima koje smo upravo naveli. Dakle, radit će se o nekim poljima brojeva. To će upravo biti *Hilbertovo polje klasa*, odnosno općenitije *polje prstena klasa*.

I prije no što navedemo glavni teorem, uputimo pozornost čitatelja na još samo jednu zanimljivu slučajnost. Promatrajući polinome zdesna vrlo pažljivi čitatelj će uočiti kako stupanj svakog od tih polinoma odgovara pripadnom broju klasa $h(-4n)$! Ako je broj klasa 1, polinom je linearan pa rješivost nije upitna. Ovo je nevjerojatna slučajnost - toliko nevjerojatna, da je se autor ovog rada nikad ne bi usudio istaknuti - kad bi bila slučajnost!

Teorem 1.4.2. *(Glavni teorem) Neka je n prirodan broj. Tada postoji normirani polinom $f_n(X)$ stupnja $h(-4n)$ takav da za sve neparne proste brojeve koji ne dijele n, vrijedi*

$$p = x^2 + ny^2 \iff \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ i } f_n(X) \equiv 0 \bmod p \\ \textit{ima cjelobrojno rješenje} \end{cases} .$$

Nadalje, postoji algoritam za naći $f_n(X)$.

Poglavlje 2

Teorija polja klasa

Iako će se čitatelj moći uvjeriti u istinost gornjih posebnih slučajeva glavnog teorema, htjeli bismo utvrditi općeniti princip. Posebno se nalaže pitanje: kako se broj klasa pojavio kao stupanj nekog polinoma? Ustvari, algoritam koji ćemo dati kasnije će nam upravo dati polinom stupnja $h(-4n)$ - svaka nultočka tog polinoma će doći od neke reducirane forme. U ovom poglavlju ćemo pokazati da je razlog za to postojanje *polja klasa* L takvog da je za imaginarno kvadratno polje K:

$$C(D) \cong \mathrm{Gal}(L/K).$$

Dakle, Galoisova grupa tog proširenja nad K će upravo biti izomorfna grupi klasa formi! I odatle naziv *polje klasa* koji potječe još od Hilberta. Pripadni polinom iz teorema će jednostavno biti minimalni polinom primitivnog elementa od L nad K.

Kao što je Gauss dokazao gornje slučajeve pomoću zakona reciprociteta, ne treba čuditi da je krajnja generalizacija upravo zakona reciprociteta dovela do uspješnog rješenja danog problema. Ta generalizacija naziva se *teorija polja klasa (Class Field Theory)*. Doduše, rezultati su egzistencijalne prirode, no uz teoriju kompleksnog množenja tvrdnje poprimaju konstruktivni oblik.

Tokom dokazivanja bit će nam potrebno slobodno prelaziti sa kvadratnih formi na ideale. To možemo zbog ključnog rezultata:

Teorem 2.0.1. *Za kvadratno slobodan* $n \equiv 1, 2 \bmod 4$*, grupa klasa ideala polja brojeva* $C(\mathbb{Q}(\sqrt{-n}))$ *izomorfna je grupi klasa formi diskriminante* $C(-n)$.

Hilbert je uspio definirati polje koje odgovara toj grupi. Pokazat ćemo da polje ima svojstva koja nam trebaju za dokaz glavnog teorema. Nažalost, ovo će raditi samo u posebnom slučaju kada je $O_K = \mathbb{Z}[\sqrt{-n}]$ - kada je n kvadratno slobodan i $n \not\equiv 3 \bmod 4$. Kako bismo to zaobišli, definirati ćemo pojam *reda* koji je generalizacija prstena cijelih brojeva.

2.1 Hilbertovo polja klasa

U ovom poglavlju ćemo dokazati idući posebni slučaj glavnog teorema:

Teorem 2.1.1. *Neka je n prirodan broj takav da*

$$n \text{ je kvadratno-slobodan, } n \not\equiv 3 \bmod 4.$$

Tada postoji normiran ireducibilni polinom $f_n(x) \in \mathbb{Z}[x]$ stupnja $h(-4n)$ takav da za prost broj p koji ne dijeli n niti $disc(f_n)$ vrijedi:

$$p = x^2 + ny^2 \iff \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ i } f_n(x) \equiv 0 \bmod p \\ \textit{ima cjelobrojno rješenje.} \end{cases}$$

Ponovimo, uvjet na n je takav da je O_K upravo jednak $\mathbb{Z}[\sqrt{-n}]$. Čitatelj će se lako uvjeriti da to ne vrijedi za n koje smo izostavili. Ovaj teorem vrijedi za beskonačno n, ali vidimo da neke već spomenute primjere ne obuhvaća. Ipak, ovo je korisna ilustracija generalnog rješenja koje je u istom duhu.

Prisjetimo se prvo malo algebre.

Definicija 2.1.2. *Proširenje L od K naziva se* normalno *ako je polje razlaganja nekog polinoma s koeficijentima u K. Ekvivalentno, za svaki element, polje sadrži sve njegove konjugate. Ekvivalentno, svako ulaganje u $\mathbb{C}$ je automorfizam.*
Normalno proširenje se naziva Abelovo *ako je Galoisova grupa* $\mathrm{Gal}(L/K)$ *Abelova grupa.*

(Općenito, *Galoisovo* proširenje je ono koje je normalno *i separabilno*, no za polja karakteristike nula, kao što je $\mathbb{Q}$, sva proširenja su separabilna. Tako Galoisovo i normalno postaju sinonimi.)

Za definiciju Hilbertovog polja klasa trebat će nam pojam *nerazgranatog* proširenja polja brojeva K. Logično zvuči da će to biti proširenje u kojem se prosti ideali ne granaju, ali postoje još posebni, "beskonačni prosti ideali" za koje moramo definirati pojam grananja. U tom kontekstu, proste brojeve, odnosno proste ideale, nazivamo *mjesta*.

Definicija 2.1.3. Realno beskonačno mjesto *je ulaganje $\sigma : K \to \mathbb{R}$.*
Kompleksno beskonačno mjesto *je* par *(različitih) kompleksnih ulaganja $\sigma, \bar{\sigma} : K \to \mathbb{C}$.*
Za proširenje L od K kažemo da se beskonačno mjesto σ grana *u L ako je σ realan, ali ima proširenje na L koje je kompleksno.*

Obični prost ideal u O_K nazivamo *konačno mjesto*. Za grananje beskonačnih mjesta treba samo promotriti realna beskonačna mjesta. Jasno je da su beskonačna mjesta samo formalni konstrukt koji nemaju smisla kao ideali, ali imaju svrhe u idućoj definiciji:

Definicija 2.1.4. *Proširenje je* nerazgranato *ako je nerazgranato u svim mjestima - konačnim i beskonačnim.*

Navodimo sada ključni teorem koji ćemo dokazati teorijom polja klasa kasnije.

Teorem 2.1.5. *Za dano polje brojeva K postoji konačno Galoisovo proširenje L od K tako da:*

(i) *L je nerazgranato Abelovo proširenje od K.*

(ii) *Svako nerazgranato Abelovo proširenje od K leži u L.*

To polje naziva se *Hilbertovo polje klasa* od K. To je dakle maksimalno nerazgranato Abelovo proširenje od K.

Teorija polja klasa navodi se kao krajnja generalizacija zakona reciprociteta koje su proučavali Gauss i svi kasnije. U tu svrhu ćemo definirati dalekosežnu generalizaciju Legendreovog simbola - no prvo navedimo lemu čiji dokaz je u [1, str. 95]:

Lema 2.1.6. *Neka je $K \subset L$ Galoisovo proširenje i $\mathfrak{p}$ prost u O_K koji je nerazgranat u L. Ako je $\mathfrak{B}$ prost ideal u O_L sadrži $\mathfrak{p}$ tada postoji jedinstveni element $\sigma \in Gal(L/K)$ tako da za sve $\alpha \in O_L$:*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{B},$$

gdje je $N(\mathfrak{p}) = |O/\mathfrak{p}|$ je norma od $\mathfrak{p}$.

Jedinstveni element σ iz leme nazivamo *Artinov simbol* i označava se $((L/K)/\mathfrak{B})$ jer općenito ovisi o prostom idealu $\mathfrak{B}$ iz L (no vidjet ćemo da za Abelovo proširenje ovisi samo o $\mathfrak{p} = \mathfrak{B} \cap O_K$). Promotrimo svojstva Artinovog preslikavanja:

Teorem 2.1.7. *Neka je $K \subset L$ Galoisovo proširenje i neka je $\mathfrak{p}$ nerazgranato prosti ideal od K. Za dani prosti ideal $\mathfrak{B}$ od L koji sadrži $\mathfrak{p}$ imamo:*

(i) *Ako je $\sigma \in Gal(L/K)$, tada*

$$\left(\frac{L/K}{\sigma(\mathfrak{B})}\right) = \sigma\left(\frac{L/K}{\mathfrak{B}}\right)\sigma^{-1}.$$

(ii) *Red od $((L/K)/\mathfrak{B})$ je inercijski stupanj $f = f_{\mathfrak{B}|\mathfrak{p}}$.*

(iii) *$\mathfrak{p}$ se potpuno razlaže u L ako i samo ako $((L/K)/\mathfrak{B}) = 1$.*

Dokaz: (i) Koristimo jedinstvenost Artinova simbola. $\left(\frac{L/K}{\sigma(\mathfrak{B})}\right)$ je jedini automorfizam sa svojstvom:

$$\left(\frac{L/K}{\sigma(\mathfrak{B})}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \sigma(\mathfrak{B}).$$

S druge strane:

$$\left(\frac{L/K}{\mathfrak{B}}\right)(\sigma^{-1}(\alpha)) \equiv (\sigma^{-1}(\alpha))^{N(\mathfrak{p})} \equiv \sigma^{-1}(\alpha^{N(\mathfrak{p})}) \bmod \mathfrak{B}$$
$$\Longrightarrow \sigma\left(\frac{L/K}{\mathfrak{B}}\right)\sigma^{-1}(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \sigma(\mathfrak{B}).$$

Zaključujemo da se radi o istim preslikavanjima.

(ii) Vidi [1, str. 96].

(iii) $\mathfrak{p}$ se potpuno razlaže ako je $e = f = 1$ za sve proste nad $\mathfrak{p}$. Po prepostavci $\mathfrak{p}$ je nerazgranat pa je $e = 1$, a po (ii) je $f = 1$ (red identite je 1). Q.E.D.

Propozicija 2.1.8. *Kada je $K \subset L$ Abelovo proširenje, Artinov simbol ovisi samo o prostom $\mathfrak{p} = \mathfrak{B} \cap O_K$.*

Dokaz: Neka je $\mathfrak{B}'$ neki drugi prost ideal u O_L nad $\mathfrak{p}$. Jer je L Galoisovo proširenje, postoji σ t.d. je $\mathfrak{B}' = \sigma(\mathfrak{B})$ (vidi [3]). Iz prethodnog teorema odmah slijedi:

$$\left(\frac{L/K}{\mathfrak{B}'}\right) = \left(\frac{L/K}{\sigma(\mathfrak{B})}\right) = \sigma\left(\frac{L/K}{\mathfrak{B}}\right)\sigma^{-1} = \left(\frac{L/K}{\mathfrak{B}}\right)$$

gdje je zadnji korak upravo opravdan komutativnošću. Q.E.D.

Artinov simbol smo definirali za proste ideale $\mathfrak{B}$ u O_L koji leže nad nerazgranatim $\mathfrak{p}$ u O_K. U prethodnoj propoziciji smo vidjeli da Artinov simbol u Abelovom proširenju ovisi samo o prostom $\mathfrak{p}$. Stoga će situacija biti najljepša kada razmotrimo upravo slučaj *nerazgranatog Abelovog proširenja*.

Razlomljeni ideal iz $\mathfrak{a} \in I_K$ možemo napisati kao:

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i}, \qquad r_i \in \mathbb{Z},$$

za (različite) proste ideale $\mathfrak{p}_i$. Definirano Artinov simbol za proizvoljni ideal kao

$$\left(\frac{(L/K)}{\mathfrak{a}}\right) = \prod_{i=1}^{r}\left(\frac{L/K}{\mathfrak{p}}\right)^{r_i}.$$

Tako nam Artinovo preslikavanje daje homomorfizam

$$\left(\frac{(L/K)}{\cdot}\right) : I_K \longrightarrow \mathrm{Gal}(L/K).$$

Primijetimo, u slučaju da proširenje nije bilo nerazgranato, Artinovo preslikavanje ne bi bilo definirano na cijelom I_K. Ta prepreka čini formuliranje teorema u punoj općenitosti (bez pretpostavke nerazgranatosti) vrlo složenom.

Prisjetimo se našeg cilja. Želimo uspostaviti izomorfizam između grupe klasa ideala i Galoisove grupe prikladnog polja. Artinovo preslikavanje nas je dovelo na dobar trag i preostaje nam izreći

Teorem 2.1.9. *(Artinov teorem reciprociteta) Ako je L Hilbertovo polje klasa brojeva K, tada je Artinovo preslikavanje*

$$\left(\frac{(L/K)}{\cdot}\right) : I_K \longrightarrow Gal(L/K)$$

surjektivno, a jezgra je P_K - grupa glavnih (razlomljenih) ideala. Stoga Artinovo preslikavanje inducira izomorfizam:

$$C(O_K) \cong Gal(L/K)$$

Dokaz ovog rezultata ćemo dobiti iz teorije polja klasa. Ovaj teorem nam omogućuje karakterizaciju prostih u K koji se potpuno razlažu u Hilbertovom polju klasa:

Korolar 2.1.10. *Neka je L Hilbertovo polje klasa brojeva K i neka je $\mathfrak{p}$ prost ideal u O_K. Tada*

$$\mathfrak{p} \textit{ se razlaže potuno u } L \Longleftrightarrow \mathfrak{p} \textit{ je glavni ideal.}$$

Dokaz: Iz teorema (2.1.7) $\mathfrak{p}$ se potpuno razlaže ako i samo ako $((L/K)/\mathfrak{p}) = 1$. Zbog izomorfizma između $C(O_K)$ i $\mathrm{Gal}(L/K)$, identiteta odgovara trivijalnoj klasi ideala, a to su glavni ideali. Q.E.D.

2.2 $x^2 + ny^2$ za beskonačno n

Sada kada znamo nešto o Hilbertovom polju klasa možemo dokazati prvu verziju glavnog teorema. Prvo, dakako, trebamo vidjeti kakve veze polje klasa ima s reprezentacijom prostih brojeva:

Teorem 2.2.1. *Neka je L Hilbertovo polje klasa od $K = \mathbb{Q}(\sqrt{-n})$. Neka je n takav da je $O_K = \mathbb{Z}[\sqrt{-n}]$. Ako je p neparan prost broj koji ne dijeli n, tada*

$$p = x^2 + ny^2 \Longleftrightarrow p \text{ se potpuno razlaže u } L. \tag{2.1}$$

Dokaz: Neka je p prost koji ne dijeli diskriminantu - po poznatom teoremu, on je tada nerazgranat. Dokazat ćemo iduće ekvivalencije:

$$\begin{aligned} p = x^2 + ny^2 &\iff pO_K = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}} \text{ i } \mathfrak{p} \text{ je glavni u } O_K \\ &\iff pO_K = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}} \text{ i } \mathfrak{p} \text{ se potpuno razlaže u } O_L \\ &\iff p \text{ se potpuno razlaže u } L \end{aligned} \tag{2.2}$$

i time će biti dokazan sami teorem.

(i) Za prvu ekvivalenciju, neka je $p = x^2 + ny^2 = (x + \sqrt{-n}y)(x - \sqrt{-n}y)$. Stavljajući $\mathfrak{p} = (x + \sqrt{-n}y)O_K$, tada $pO_K = \mathfrak{p}\bar{\mathfrak{p}}$ je faktorizacija u proste od pO_K. Primijetimo da $\mathfrak{p} \neq \bar{\mathfrak{p}}$ jer p ne dijeli diskriminantu pa se ne grana. Također $\mathfrak{p}$ jest prost - norma mu je p.

(ii) Odmah iz korolara (2.1.10).

(iii) Za ovo dokažimo prvo lemu:

Lema 2.2.2. *Neka je L Hilbertovo polje klasa za imaginarno kvadratno polje K i neka je τ kompleksno konjugiranje. Tada je $\tau(L) = L$ i stoga je L Galoisovo nad $\mathbb{Q}$.*

Dokaz: Primijetimo prvo da je i $\tau(L)$ nerazgranato Abelovo proširenje od $\tau(K) = K$. Kako je L maksimalno takvo te istog stupnja, slijedi da je $\tau(L) = L$. L je Galoisovo nad K pa su sva K-ulaganja automorfizmi. Svako K-ulaganje σ je i $\mathbb{Q}$-ulaganje. S druge strane je i $\tau \circ \sigma$ jedno $\mathbb{Q}$-ulaganje (koje nije K-ulaganje jer ne fiksira K). Kako je K kvadratno proširenje, tako dobivamo sva ulaganja od L nad $\mathbb{Q}$ i vidimo da je svako automorfizam. Stoga je L Galoisovo nad $\mathbb{Q}$. Q.E.D.

Da dokažemo ekvivalenciju (iii) primijetimo da uvjet:

$$pO_K = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}} \text{ i } \mathfrak{p} \text{ se potpuno razlaže u } O_L$$

kaže da se p razlaže potpuno nad K i prosti ideal $\mathfrak{p}$ nad p se potpuno razlaže L. Kako je L Galoisovo nad $\mathbb{Q}$, svi indeksi grananja su isti $e = 1$ i $2n = ref = rf$, gdje je r broj različitih prostih faktora. Vrijedi $r > n$ iz čega odmah slijedi $f = 1$. Vidimo da se p potpuno razlaže u L. Q.E.D.

Idući korak je dati elementarniji kriterij razlaganja.

Propozicija 2.2.3. *Neka je K imaginarno kvadratno polje i L Hilbertovo polje klasa od K. Tada:*

(i) *Postoji realni $\alpha \in O_K$ takav da je $L = K(\alpha)$.*

(ii) *Za takav α kao u (i), neka je f(x) njegov minimalni polinom. Ako je p prost broj koji ne dijeli diskriminantu od f(x), tada:*

$$p \text{ se potpuno razlaže u } L \iff \begin{cases} \left(\frac{d_K}{p}\right) = 1 \text{ i } f(x) \equiv 0 \bmod p \\ \text{ima cjelobrojno rješenje} \end{cases} \tag{2.3}$$

Dokaz: Vrijedi

$$[L : K][K : \mathbb{Q}] = [L : \mathbb{Q}] = [L : L \cap \mathbb{R}][L \cap \mathbb{R} : \mathbb{Q}].$$

Kako je K kvadratno proširenje imamo $[K : \mathbb{Q}] = 2$. Po prethodnoj propoziciji je $\tau \in \mathrm{Gal}(L/\mathbb{Q})$. Stoga je $[L : L \cap \mathbb{R}] = 2$ i slijedi

$$[L : K] = [L \cap \mathbb{R} : \mathbb{Q}].$$

Onda za primitivni element α od $L \cap \mathbb{R}$ nad $\mathbb{Q}$ vrijedi da je primitivni element od L nad K jer je

$$K(\alpha) = \mathbb{Q}(\sqrt{-n})(\alpha) = \mathbb{Q}(\alpha)(\sqrt{-n}) = L \cap \mathbb{R}(\sqrt{-n}) = L.$$

Njegov minimalni polinom ima koeficijente u $\mathbb{Z}$ jer je primitivni element od $L \cap \mathbb{R}$.
Za (ii), neka je p prost broj koji ne dijeli diskriminantu od $f(x)$. Zašto nam je taj uvjet važan? To znači da je $f(x)$ separabilan modulo p. Jer se p grana ako i samo ako p dijeli diskriminantu polja, vrijedi

$$pO_K = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}} \Longleftrightarrow \left(\frac{d_K}{p}\right) = 1.$$

Dakle p se potpuno razlaže u K tako da je $\mathbb{Z}/p\mathbb{Z} \cong O_K/\mathfrak{p}$. Kako je $f(x)$ separabilan nad $\mathbb{Z}/p\mathbb{Z}$, separabilan je i nad $O_K/\mathfrak{p}$. Sada se sjetimo kako se ideali razlažu (vidi prop. 5.11. [1] ili teorem 27. [3]). Ovdje imamo

$$\begin{aligned} \mathfrak{p} \text{ se potpuno razlaže u } L &\Longleftrightarrow f(x) \equiv 0 \bmod \mathfrak{p} \text{ ima rješenje u } O_K \\ &\Longleftrightarrow f(x) \equiv 0 \bmod p \text{ ima rješenje u } \mathbb{Z}. \end{aligned}$$

Zadnja od tri ekvivalencije (2.2) sada daje tvrdnju. Q.E.D.

I sada možemo dokazati ekvivalenciju u posebnom slučaju glavnog teorema (2.1.1). Neka je L Hilbertovo polje klasa nad $K = \mathbb{Q}(\sqrt{-n})$. Neka je $L = K(\alpha)$ s minimalnim polinom $f_n(x)$ i p prosti broj koji ne dijeli diskriminantu od $f_n(x)$. Sada samo spojimo dokazane ekvivalencije:

$$p = x^2 + ny^2 \overset{(2.1)}{\Longleftrightarrow} p \text{ se potpuno razlaže u } L \overset{(2.3)}{\Longleftrightarrow} \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ i } f_n(x) \equiv 0 \bmod p \\ \text{ima cjelobrojno rješenje} \end{cases}.$$

Primijetimo da smo u zadnjem izrazu pojednostavili Legendreov simbol $\left(\frac{d_K}{p}\right) = \left(\frac{-4n}{p}\right) = \left(\frac{-n}{p}\right)$. Ali zašto je stupanj jednak $h(-4n)$? Uz gore navedenu teoriju razlog je jednostavan:

$$[L : K] = |\mathrm{Gal}(L/K)| = |C(O_K)|.$$

$C(O_K)$ je grupa klasa ideala, a ona je pak izomorfna grupi klasa formi $C(-4n)$. Polje K je imaginarno kvadratno polje $K = \mathbb{Q}(\sqrt{-n})$, pa je $|C(O_K)|$ jednak broju klasa formi $h(-4n)$.

Sada smo objasnili oblik teorema. Ovaj argument je bio valjan kada je vrijedilo $\mathrm{disc}O_K = d_K = -4n$. Preostaje nam poopćiti argument tako da nađemo polje klasa koje će odgovarati $C(-4n)$ kad n nije takav.

2.3 Redovi u imaginarnim kvadratnim poljima

Riješili smo dakle naš uvodni problem za beskonačno mnogo slučajeva, ali smo isto tako izostavili beskonačno slučajeva, među njima slučajeve koje smo dobili kao korolare Gaussovih zakona reciprociteta. No, i ti slučajevi slijede istu šablonu, pa želimo pokazati da teorem vrijedi i bez gornjeg ograničenja. Za to ćemo se prvo morati upoznati bolje sa strukturom koju nosi $\mathbb{Z}[\sqrt{-n}\,]$.

Uzeli smo gore n s takvim svojstvima da je prsten algebarskih cijelih brojeva u $\mathbb{Q}(\sqrt{-n}\,)$ jednak $\mathbb{Z}[\sqrt{-n}\,]$. Općenito ako nije tako, ne čine Dedekindovu domenu - to je glavni razlog zašto moramo proširiti diskusiju, ali će $\mathbb{Z}[\sqrt{-n}\,]$ svejedno imati dovoljno posebnih svojstva da možemo dokazati naš teorem. Ustvari će svojstva takvih prstena biti prirodna generalizacija onoga što vrijedi za algebarske cijele brojeve.

Definicija 2.3.1. Red *O u kvadratnom polju K je podskup od O_K t.d.*

(i) *O je podprsten od K s jedinicom.*

(ii) *O je konačno generiran kao $\mathbb{Z}$-modul.*

(iii) *O sadrži $\mathbb{Q}$-bazu za K.*

(ii) i (iii) ekvivalentno je tome da je O slobodni $\mathbb{Z}$-modul ranga 2. Zbog (iii), K je polje razlomaka od O. Na red se može gledati kao na generalizaciju prstena alg. cijelih brojeva. Ustvari, zbog (i) i (ii) za sve redove vrijedi $O \subset O_K$. Tako algebarski cijeli brojevi čine *maksimalni red*.

Redove možemo vrlo eksplicitno opisati. Maksimalni red O_K možemo zapisati kao:

$$O_K = [1, w_K], \qquad w_k = \frac{d_k + \sqrt{d_k}}{2}, \tag{2.4}$$

(ovo su samo oba slučaja $d_k \equiv 0, 1 \bmod 4$ sažeti u jedan).

Zapis ostalih redova u kvadratnim poljima je jednako jednostavan:

Lema 2.3.2. *Neka je O red u kvadratnom polju diskriminante d_K. Tada O ima konačan indeks u O_K i ako stavimo $f = [O_K : O]$, tada*

$$O = \mathbb{Z} + fO_K = [1, fw_K], \tag{2.5}$$

gdje je w_K kao gore.

Dokaz: Kako je $O \subset O_K$, O je generiran s nekim alg. cijelim brojevima a, b koji zbog eksplicitnog opisa cijelih u kv. poljima su $a = \alpha + \beta w_K$ i $b = \gamma + \delta w_K$, sa cijelim koeficijentima $\alpha, \beta, \gamma, \delta$. Ako iskoristimo još da se 1 nalazi u O dobivamo:

$$O = [a, b] = [\alpha + \beta w_K, \gamma + \delta w_K] = [1, \alpha + \beta w_K, \gamma + \delta w_K] = [1, fw_K].$$

Vrijednost f iz gornjeg opisa je upravo indeks od O u O_K. Time je lema dokazana. Q.E.D

Vidimo da je općenito $Z[\sqrt{-n}\,]$ red indeksa 1 ili 2 u O_K.

Obratno lemi, svaki potprsten $[1, fw_K]$ u O_K jest red. Za dani red O, indeks f iz leme nazivamo *konduktor*. Diskriminantu reda definiramo isto kao i za prstene brojeva. Označimo s α' konjugat od α. Tada je *diskriminanta* od $O = [\alpha, \beta]$:

$$D = \begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix}^2 .$$

Diskriminanta je neovisna o $\mathbb{Z}$-bazi i ako računamo D pomoću baze $[1, fw_K]$ iz leme, dobivamo da je

$$D = f^2 d_K. \tag{2.6}$$

Red O je prsten te želimo promatrati ideale u redu. Krenimo sa svojstvom analognim kao kod ideala u O_K:

Propozicija 2.3.3. *Svaki ideal* $\mathfrak{a}$ *u redu* O *kvadratnog polja* K *je konačnog indeksa.*

Dokaz: Pokažimo da O sadrži neki cijeli broj. Po eksplicitnom prikazu reda (2.5) je $f\bar{w}_K \in O$ pa je $f\bar{w}_K = f\frac{d_K - \sqrt{d_K}}{2} = fd_K - f\frac{d_K + \sqrt{d_K}}{2}$, pa je kompleksno konjugiranje je automorfizam od O. Sada kao u ([3, Teorem 14]), uzmimo $\alpha \in \mathfrak{a}$. Kako je $\mathfrak{a}$ ideal, onda je i $\bar{\alpha}\alpha \in \mathfrak{a}$, dakle imamo cijeli broj $m = |\alpha|^2$ u $\mathfrak{a}$. Ali onda je

$$[O : \mathfrak{a}] \leq [O : (m)] = m^2.$$

Dakle, indeks je konačan. Q.E.D.

Definicija 2.3.4. Norma *ideala* $\mathfrak{a}$ *u redu* O *je*

$$N(\mathfrak{a}) = [O : \mathfrak{a}] = |O/\mathfrak{a}|.$$

Isto kao i O_K, svaki red O je Noetherin prsten, no *nije* integralno zatvoren za $f > 1$. Dakle, ideali ne moraju imati jedinstvenu faktorizaciju!

Ipak, uz ostala svojstva od O, motivirani smo definirati pojmove koji bi nam omogućili analogni rad s redovima. Ovdje će biti spretnije raditi s razlomljenim idealima. *Razlomljeni* ideal u O je podskup od K koji je ne-nul konačno generirani O-modul. Svaki takav je oblika $\alpha\mathfrak{a}$ gdje je $\alpha \in K$, a $\mathfrak{a}$ obični ideal. Sada definiramo dva "nova" tipa ideala.

Definicija 2.3.5. *Kažemo da je razlomljeni ideal* $\mathfrak{a}$ pravi *kada vrijedi*

$$O = \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}.$$

Razlomljeni ideal $\mathfrak{a}$ *je* invertibilan *ako postoji* $\mathfrak{b}$ *tako da je*

$$\mathfrak{a}\mathfrak{b} = O.$$

Primijetimo da su glavni razlomljeni ideali αO očito invertibilni. Glavni rezultat vezan uz ova dva pojma je da se u kvadratnim poljima podudaraju.

Teorem 2.3.6. *Neka je O red u kvadratnom polju K i neka je $\mathfrak{a}$ razlomljeni O-ideal. Tada je $\mathfrak{a}$ pravi ako i samo ako je invertibilan.*

Dokaz: Neka je $\mathfrak{a}$ invertibilan s inverzom $\mathfrak{b}$. Ako je $\beta \in K$ takav da je $\beta\mathfrak{a} \subset \mathfrak{a}$ imamo:

$$\beta O = \beta(\mathfrak{a}\mathfrak{b}) = (\beta\mathfrak{a})\mathfrak{b} \subset \mathfrak{a}\mathfrak{b} = O$$

pa je $\beta \in O$. Kako je β bio proizvoljan slijedi da je $O = \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}$ pa je $\mathfrak{a}$ pravi ideal.

Za obrat dokažimo prvo lemu.

Lema 2.3.7. *Neka je $K = \mathbb{Q}(\tau)$ kvadratno polje i $ax^2 + bx + c$ minimalni polinom od τ, gdje su a, b, c relativno prosti cijeli brojevi. Tada je $[1, \tau]$ pravi razlomljeni ideal reda $[1, a\tau]$ od K.*

Dokaz: Uzmimo $\beta \in K$ i promotrimo tvrdnju $\beta[1, \tau] \subset [1, \tau]$. Uzmimo neke jednostavne elemente iz $[1, \tau]$ npr. $1, \tau$ i promotrimo njihove produkte s β. Oni opet moraju biti u $[1, \tau]$. Stoga je za $\beta = m + n\tau$, $m, n \in \mathbb{Z}$

$$\begin{aligned}\beta\tau &= m\tau + n\tau^2 = m\tau + n\frac{-b\tau - c}{a} \\ &= \frac{-nc}{a} + \left(\frac{-bn}{a} + m\right)\tau.\end{aligned}$$

Kako bi koeficijenti bili u $\mathbb{Z}$ mora biti $a \mid -nc$, a kako su a, b, c relativno prosti mora biti $a|n$, to jest $\beta \in [1, a\tau]$. Stoga je

$$\{\beta \in K : \beta[1, \tau] \subset [1, \tau]\} = [1, a\tau].$$

Time je pokazano da je $[1, \tau]$ pravi ideal u $[1, a\tau]$. Q.E.D.

Sada možemo dokazati obratni smjer teorema (2.3.6). Primijetimo da je (ne-razlomljeni) ideal $\mathfrak{a}$ od O kao aditivna podgrupa također $\mathbb{Z}$-modul. Kako je indeks od $\mathfrak{a}$ konačan, mora biti da je ranga 2, a ne 1. Sada to posebno vrijedi za razlomljene ideale jer su oblika $\alpha\mathfrak{a}$.

Neka je $\mathfrak{a} = [\alpha, \beta]$ za neke $\alpha, \beta \in K$. Možemo pisati $\mathfrak{a} = \alpha[1, \tau]$ gdje je $\tau = \beta/\alpha$. Neka je $ax^2 + bx + c$ minimalni polinom od τ. Po prethodnoj lemi $O = [1, a\tau]$. Označimo s $\beta \to \beta'$ netrivijalni automorfizam od K. Onda je $\mathfrak{a}' = \alpha'[1, \tau']$ pravi ideal $[1, a\tau'] = [1, a\tau] = O$. Tvrdimo da je

$$a\mathfrak{a}\mathfrak{a}' = N(\alpha)O,$$

Ovo se dokaže idućim jednostavnim računom:

$$a\mathfrak{a}\mathfrak{a}' = a\alpha\alpha'[1, \tau][1, \tau'] = N(\alpha)[a, a\tau, a\tau', a\tau\tau'].$$

Po Vietovim formulama $\tau + \tau' = -b/a$ i $\tau\tau' = c/a$ pa možemo pojednostaviti

$$a\mathfrak{a}\mathfrak{a}' = N(\alpha)[a, a\tau, -b, c] = N(\alpha)O$$

jer je $(a, b, c) = 1$. Preostaje podijeliti s $N(\alpha)$ i vidimo da je $\mathfrak{a}$ invertibilan. Q.E.D.

Za red O označimo s $I(O)$ skup pravih razlomljenih O-ideala. Kako su pravi ideali invertibilni, $I(O)$ je grupa (obzirom na množenje ideala). Glavni O-ideali $P(O)$ su očito podgrupa od $I(O)$, te promotrimo idući kvocijent:

$$C(O) = I(O)/P(O),$$

koji nazivamo *grupa klasa ideala* reda O. Za maksimalni red O_K, ova definicija se preklapa s već danom te ćemo prikladno označiti $I(O_K) = I_K$ i $P(O_K) = P_K$.

Ovime smo postigli generalizaciju algebarskih cijelih brojeva i njihove grupe klasa ideala. Preostaje nam generalizirati Hilbertovo polje klasa. No, ovo je prikladno mjesto da prije toga navedemo već najavljenu jaku vezu između grupa klasa ideala i kvadratnih formi.

Za imaginarna kvadratna polja K postoji izomorfizam između grupe klasa ideala $C(O)$ reda O u K i grupe klasa formi diskriminante D reda O.

Teorem 2.3.8. *Neka je O red diskriminante D u imaginarnom kvadratnom polju K. Tada:*

(i) *Ako je $f(x, y) = ax^2 + bxy + cy^2$ primitivna pozitivno definitna kvadratna forma diskriminante D, tada je $[a, (-b + \sqrt{D})/2]$ ideal od O.*

(ii) *Preslikavanje koje šalje forme $f(x, y)$ u ideale $[a, (-b+\sqrt{D})/2]$ inducira izomorfizam između grupe klasa formi $C(D)$ i grupe klasa ideala $C(O)$.*

(iii) *Prirodni broj m reprezentiran je formom $f(x, y)$ ako i samo ako je m norma $N(\mathfrak{a})$ za neki ideal iz korespondirajuće klase ideala u $C(O)$.*

Dokaz: Dokaz je elementaran no predug da ga navedemo. Vidi [1, Teorem 7.7].

Ovo nam omogućuje da slobodno prelazimo s formi na ideale, kako nam je prikladno. Idući korolar će nam zatrebati malo kasnije.

Korolar 2.3.9. *Neka je O red u imaginarnom kvadratnom polju. Za dani $M \in \mathbb{N}$, svaka klasa ideala u $C(O)$ sadrži O-ideal čija je norma relativno prosta s M.*

Dokaz: Po trećem stavku prošlog teorema, vidimo da je pitanje ekvivalentno tome reprezentira li pripadna primitivna forma $f(x, y) = ax^2 + bxy + cy^2$ neki broj relativno prost s M. Ovo je dokazao još Gauss [7, §228]. Dokaz je elementaran. Promotrimo neki prost djelitelj p od M.

Ako $p \mid a$ i $p \nmid c$ onda je dovoljno uzeti x djeljiv s p i y koji nije, pa $f(x, y)$ nije djeljiv s p (jer će prva dva sumanda biti djeljiva, a treći neće).

Ako $p \nmid c$ i $p \mid c$ onda uzmemo x koji nije djeljiv s p i y koji jest.

Ako $p \mid a$ i $p \mid c$, kako je O bio pravi ideal, dakle forma primitivna, mora biti da onda $p \nmid b$. Onda uzimajući x, y koji nisu djeljivi s p dobivamo vrijednost $f(x, y)$ koja također nije djeljiva s p.

Konačno, možemo uzeti kao x produkt svih faktora tako da vrijedi prvi slučaj i kao y produkt svih faktora da vrijedi drugi slučaj i tada će $f(x, y)$ biti relativno prost s M. Q.E.D.

Ideali relativno prosti s konduktorom

Vidjeli smo da je Hilbertovo polje klasa formulirano za grupu klasa ideala polja brojeva. Zato ćemo sada O-ideale u nekom redu prevesti u O_K-ideale.

Definicija 2.3.10. *Neka je O red konduktora f. Kažemo da je O-ideal* $\mathfrak{a}$ relativno prost s f *ako je* $\mathfrak{a} + fO = O$.

Skratit ćemo "relativno prost s" na "prost s". Obzirom da se suma ideala interpretira kao najveći zajednički djelitelj pa je *relativno prost* s konduktorom upravo ono što bismo očekivali. Za takve ideale vrijedi:

Lema 2.3.11. *Neka je O red konduktora f.*

(i) *O-ideal $\mathfrak{a}$ je prost s f ako i samo ako je norma $N(\mathfrak{a})$ relativno prosta s f.*

(ii) *Svaki O-ideal prost s f je pravi ideal.*

Dokaz: (i) Neka je $m_f : O/\mathfrak{a} \to O/\mathfrak{a}$ množenje s f. Tada je $\mathfrak{a} + fO = O$ ako i samo ako je m_f surjektivno (to se vidi uzimanjem kvocijenta $/\mathfrak{a}$). Ako je m_f surjekcija, onda je automatski bijekcija zbog konačnosti $O/\mathfrak{a}$. K tomu je množenje homomorfizam pa zaključujemo da je m_f *izomorfizam*. $O/\mathfrak{a}$ je konačna Abelova grupa pa po strukturnom teoremu o Abelovim grupama, vidimo da m_f može biti izomorfizam ako i samo ako je $|O/\mathfrak{a}| = N(\mathfrak{a})$ relativno prosto s f.

(ii) Provjerimo po definiciji pravog ideala. Neka je β takav da vrijedi $\beta\mathfrak{a} \subset \mathfrak{a}$. Tada je $\beta \in O_K$ i imamo

$$\beta O = \beta(\mathfrak{a} + fO) = \beta\mathfrak{a} + \beta f O \subset \mathfrak{a} + bfO_K.$$

Kako je $fO_K \subset O$ slijedi da je $\beta O \subset O$. Dakle $\beta \in O$, pa je $\mathfrak{a}$ pravi ideal. Q.E.D.

O-ideali relativno prosti s f čine podgrupu u grupi pravih ideala $I(O)$ (zbog multiplikativnosti norme i prethodne leme, produkt ideala prostih s konduktorom je opet prost s konduktorom). Označimo je s $I(O, f)$ i njenu podgrupu glavnih ideala s $P(O, f)$. Uzimajući kvocijent očekujemo da možemo definirati analogon grupe klasa ideala. Ustvari dobijemo upravo ranije već definiranu grupu klasa ideala.

Propozicija 2.3.12.

$$I(O,f)/P(O,f) \cong I(O)/P(O) \cong C(O)$$

Dokaz: Preslikavanje $I(O,f) \to C(O)$ je surjektivno po prethodnoj lemi (svaka klasa ideala u $C(O)$ sadrži neki O-ideal prost s f), a jezgra je $I(O,f) \cap P(O)$. Želimo pokazati

$$I(O,f) \cap P(O) = P(O,f)$$

$P(O,f)$ je podskup i od $I(O,f)$ i od $P(O)$ tako da je očito $P(O,f) \subset I(O,f) \cap P(O)$. Za obratnu inkluziju, uzmimo element iz $I(O,f) \cap P(O)$. To je glavni razlomljeni ideali $\alpha O = \mathfrak{a}\mathfrak{b}^{-1}$ gdje je $\alpha \in K$ i napisali smo ga kao kvocijent običnih O-ideala $\mathfrak{a}, \mathfrak{b}$ rel. prostih s f. Neka je $m = N(\mathfrak{b})$. Tada je $mO = N(\mathfrak{b})O = \mathfrak{b}\bar{\mathfrak{b}}$ leži u $P(O,f)$ i k tome je $m\mathfrak{b}^{-1} = \bar{\mathfrak{b}}$. Stoga

$$m\alpha O = \mathfrak{a} \cdot m\mathfrak{b}^{-1} = \mathfrak{a}\bar{\mathfrak{b}} \subset O$$

pa je $m\alpha O \in P(O,f)$. Stoga je $\alpha O = m\alpha O(mO)^{-1}$ je također u $P(O,f)$ i time je propozicija dokazana. Q.E.D.

Za svaki red O, ideali prosti s konduktorom su u dobrom odnosu s O_K. Naime, za dani $m \in \mathbb{Z}$ definiramo da je O-ideal $\mathfrak{a}$ prost s m ako je $\mathfrak{a} + mO_K = O_K$. Kao i u lemi (2.3.11), to je ekvivalentno s $(N(\mathfrak{a}), m) = 1$. Stoga, unutar grupe razlomljenih O_K-ideala I_K, $I_K(m)$ čini podgrupu generiranu O_K-idealima prostima s m.

Propozicija 2.3.13. *Neka je O red konduktora f u imaginarnom kvadratnom polju K. Tada:*

(i) *Ako je $\mathfrak{a}$ O-ideal prost s f, tada je $\mathfrak{a} \cap O$ O-ideal prost s f i to iste norme kao i $\mathfrak{a}$.*

(ii) *Ako je $\mathfrak{a}$ O-ideal prost s f, tada je $\mathfrak{a}O_K$ O_K-ideal prost s f i to iste norme kao i $\mathfrak{a}$.*

(iii) *Preslikavanje $\mathfrak{a} \mapsto \mathfrak{a} \cap O$ inducira izomorfizam $I_K(f) \cong I(O,f)$ i inverz tog preslikavanje je dan s $\mathfrak{a} \mapsto \mathfrak{a}O_K$.*

Dokaz: [1, str. 131]

Ova propozicija nam omogućava da shvatimo O-ideale proste s konduktorom reda kao O_K-ideale - gdje imamo jedinstvenu faktorizaciju. Slijedi da svaki O-ideal prost s konduktorom je produkt O-ideala prostih s konduktorom reda O.

Propozicija 2.3.14. *Neka je O red konduktora f u imaginarnom kvadratnom polju K. Tada postoje prirodni izomorfizmi*

$$C(O) \cong I(O,f)/P(O,f) \cong I_K(f)/P_{K,\mathbb{Z}}(f),$$

gdje je $P_{K,\mathbb{Z}}(f)$ podgrupa od $I_K(f)$ generirana glavnim idealima oblika αO_K gdje αO_K zadovoljava $\alpha \equiv a \bmod fO_K$ za neki cijeli broj a relativno prost s f.

Kasnije ćemo koristiti ovu propoziciju da povežemo $C(O)$ s teorijom polja klasa za K.

2.4 Teorija polja klasa

Definicija 2.4.1. Modulus *u polju brojeva K je formalni produkt*

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

nad svim prostim mjestima $\mathfrak{p}$*, konačnim ili beskonačnim s time da tražimo:*

(i) $n_{\mathfrak{p}} \geq 0$ *i najviše konačno mnogo njih je različito od* 0*,*

(ii) $n_{\mathfrak{p}} = 0$ *ako je* $\mathfrak{p}$ *kompleksni beskonačni prost,*

(iii) $n_{\mathfrak{p}} \leq 1$ *kad je* $\mathfrak{p}$ *realni beskonačni prost.*

Vidimo da modulus možemo napisati kao produkt običnog ideala $\mathfrak{m}_0$ i formalnog $\mathfrak{m}_\infty$

$$\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty.$$

Kada su svi $n_{\mathfrak{p}} = 0$ stavimo $\mathfrak{m} = 1$ (kao prazan produkt).

Za čisto imaginarna polja K (bez realnih ulaganja), $\mathfrak{m}_\infty$ je trivijalan pa modulus možemo jednostavno shvatiti kao ideal u K.

Još jednom ćemo generalizirati pojam *grupe klasa ideala*. Za dani modulus $\mathfrak{m}$ neka je $I_K(\mathfrak{m})$ grupa razlomljenih ideala od O_K relativno prostih s $\mathfrak{m}$ (to jest s $\mathfrak{m}_0$) i neka je $P_{K,1}(\mathfrak{m})$ podgrupa od $I_K(\mathfrak{m})$ generirana glavnim idealima αO_K gdje je $\alpha \in O_K$ takav da

$$\alpha \equiv 1 \bmod \mathfrak{m}_0 \text{ i } \sigma(\alpha) > 0 \text{ za svaki realni beskonačni prost } \sigma \text{ koji dijeli } \mathfrak{m}_\infty$$

Važan rezultat je da je $P_{K,1}(\mathfrak{m})$ konačnog indeksa u $I_K(\mathfrak{m})$. Za dokaz vidi [4, Teorem IV.I]

Podgrupa $H \subset I_K(\mathfrak{m})$ naziva se *kongruencijska podgrupa* za $\mathfrak{m}$ ako zadovoljava

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m}),$$

a kvocijent

$$I_K(\mathfrak{m})/H$$

naziva se *generalizirana grupa klasa ideala* za $\mathfrak{m}$.

Uzmimo za primjer slučaj kad je modulus $\mathfrak{m} = 1$. Tada je $P_K = P_{K,1}(1)$ kongruencijska podgrupa pa je grupa klasa ideala $C(O_K) = I_K/P_K$ generalizirana grupa klasa ideala.

Još jedan primjer možemo vidjet kod reda O konduktora f. U propoziciji (2.3.14) smo vidjeli da se grupa klasa ideala $C(O)$ može zapisati kao

$$C(O) \cong I_K(f)/P_{K,\mathbb{Z}}(f),$$

gdje je $P_{K,\mathbb{Z}}(f)$ grupa generirana glavnim idealima αO_K za neki $\alpha \equiv a \bmod fO_K, a \in \mathbb{Z}$ i $(a, f) = 1$. Uzmimo za modulus $\mathfrak{m} = fO_K$. Tada po definiciji od $P_{K,1}(fO_K)$ vidimo da je

$$P_{K,1_s}(fO_K) \subset P_{K,\mathbb{Z}}(f) \subset I_K(f) = I_K(fO_K)$$

pa je $P_{K,\mathbb{Q}}(f)$ kongruencijska podgrupa za fO_K što pak povlači da je $C(O)$ generalizirana grupa klasa ideala od K za modulus fO_K.

Osnovna ideja teorije polja klasa da generalizirane grupe klase ideala odgovaraju Galoisovim grupama svih Abelovih proširenja od K i izomorfizam je dan Artinovim preslikavanjem. Definiramo sada Artinovo preslikavanje za Abelovo proširenje L od K.

Neka je $\mathfrak{m}$ modulus djeljiv sa svim *razgranatim* prostim idealima Abelovog proširenja L od K. Za prost $\mathfrak{p}$ koji ne dijeli $\mathfrak{m}$ imamo Artinov simbol

$$\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$$

kao prije.

Faktorizirajući ideal na proste faktore, proširimo Artinovo preslikavanje po multiplikativnosti na cijeli $I_K(\mathfrak{m})$ tako da dobijemo homomorfizam

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K)$$

koji nazivamo Artinovo preslikavanje za $K \subset L$ i $\mathfrak{m}$. Katkada ćemo pisati i $\Phi_{L/K,\mathfrak{m}}$ kada želimo naglasiti o kojem se proširenju radi.

Prvi teorem teorije polja klasa nam govori da je $\mathrm{Gal}(L/K)$ generalizirana grupa klasa ideala za neki modulus:

Teorem 2.4.2. *Neka je $K \subset L$ Abelovo proširenje i neka je $\mathfrak{m}$ modulus djeljiv sa svim mjestima od K, konačnim ili beskonačnim, koji se granaju u L. Tada:*

(i) *Artinovo preslikavanje $\Phi_{\mathfrak{m}}$ je surjektivno.*

(ii) *Ako su eksponenti konačnih prostih faktora od $\mathfrak{m}$ dovoljno veliki, tada je* $\mathrm{Ker}(\Phi_{\mathfrak{m}})$ *kongruencijska podgrupa za $\mathfrak{m}$ tj.*

$$P_{K,1}(\mathfrak{m}) \subset \mathrm{Ker}(\Phi_{\mathfrak{m}}) \subset I_K(\mathfrak{m}),$$

i zbog toga izomorfizam

$$I_K(\mathfrak{m})/\,\mathrm{Ker}(\Phi_{\mathfrak{m}}) \cong \mathrm{Gal}(L/K)$$

pokazuje da je $\mathrm{Gal}(L/K)$ *generalizirana grupa klasa ideala za modulus* $\mathfrak{m}$.

Dokaz: Vidi [4, Teorem 5.7].

Ovaj teorem se katkada naziva *Artinov zakon reciprociteta*. Promotrimo sada jedan važan primjer.

Primjer 2.4.3. *Neka je $L = \mathbb{Q}(\zeta_m)$ gdje je ζ_m m-ti primitivni korijen jedinice i $K = \mathbb{Q}$. Neka je modulus $\mathfrak{m} = m\infty$, gdje je ∞ beskonačni prosti od $\mathbb{Q}$. Dobro je poznato da se prost broj grana u $\mathbb{Z}(\zeta_m)$ ako i samo ako dijeli m. Slijedi da je Artinovo preslikavanje*

$$\Phi_{\mathfrak{m}} : I_{\mathbb{Q}}(\mathfrak{m}) \longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$$

dobro definirano. Preslikavanje $\Phi_{\mathfrak{m}}$ možemo opisati ovako: za dani $\frac{a}{b}\mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m})$ (gdje je $\frac{a}{b} > 0$ i $(a, m) = (b, m) = 1$), vrijedi

$$\Phi_{\mathfrak{m}}\left(\frac{a}{b}\mathbb{Z}\right) = [a][b]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^*. \tag{2.7}$$

Dokažimo to. Dovoljno je promotriti djelovanje na prostim idealima $p\mathbb{Z}$ prostim s m, a to možemo vidjeti koristeći lemu (2.1.6) kojom smo i definirali Artinovo preslikavanje. Dovoljno je promotriti djelovanje na ζ_m. Primijetimo da je $N(p\mathbb{Z}) = |\mathbb{Z}/p\mathbb{Z}| = p$, pa je

$$\left(\frac{L/K}{p\mathbb{Z}}\right)(\zeta_m) \equiv \zeta_m^p \bmod \mathfrak{p}$$

Kako se korijeni iz jedinice razlikuju mod $\mathfrak{p}$ ($x^m - 1$ je separabilan za $m \notin \mathfrak{p}$), zaključujemo da ustvari mora vrijediti jednakost (a ne samo kongruencija)

$$\left(\frac{L/K}{p\mathbb{Z}}\right)(\zeta_m) = \zeta_m^p.$$

Stoga je $\Phi_m(p\mathbb{Z}) = [p] \in (\mathbb{Z}/m\mathbb{Z})^*$ i tvrdnja slijedi iz multiplikativnosti. Jezgra preslikavanja su očito $a/b \equiv 1 \bmod m$ tj.

$$\mathrm{Ker}(\Phi_{\mathfrak{m}}) = P_{\mathbb{Q},1}(\mathfrak{m}) \tag{2.8}$$

Uskoro ćemo ovaj račun iskoristiti pri dokazu slavnog teorema.

Neka je modulus $\mathfrak{n}$ djeljiv s $\mathfrak{m}$ (tj. $\mathfrak{n} = \mathfrak{o}\mathfrak{m}$ za neki ideal $\mathfrak{o}$) i $P_{K,1} \subset \mathrm{Ker}(\Phi_{\mathfrak{m}})$, tada

$$P_{K,1}(\mathfrak{m}) \subset \mathrm{Ker}(\Phi_{\mathfrak{m}}) \Rightarrow P_{K,1}(\mathfrak{n}) \subset \mathrm{Ker}(\Phi_{\mathfrak{n}}) \tag{2.9}$$

pa je $\mathrm{Gal}(L/K)$ generalizirana grupa klasa ideala za beskonačno modulusa. Ipak se jedan modulus može izdvojiti.

Teorem 2.4.4. *(Teorem o konduktoru) Neka je $K \subset L$ Abelovo proširenje. Tada postoji modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ takav da*

(i) *Mjesto od K, konačno ili beskonačno, grana se u L ako i samo ako dijeli* $\mathfrak{f}$.

(ii) *Neka je* $\mathfrak{m}$ *modulus djeljiv sa svim mjestima od K koji se granaju u L. Tada je* $\mathrm{Ker}(\Phi_m)$ *kongruencijska podgrupa za* $\mathfrak{m}$ *ako i samo ako* $\mathfrak{f} \mid \mathfrak{m}$.

Dokaz: Vidi ([4, Teorem 12.7]).

Modulus $\mathfrak{f}$ je jedinstveno određen s $K \subset L$ i naziva se *konduktor* proširenja i odatle naziv teorema.

Još preostaje navesti jedan od glavnih teorema teorije polja klasa, a to je

Teorem 2.4.5. *(Teorem o egzistenciji) Neka je* $\mathfrak{m}$ *modulus za K, i neka je H kongruencijska podgrupa za* $\mathfrak{m}$ *tj.*

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m}).$$

Tada postoji jedinstveno Abelovo proširenje L od K, čija sva razgranata prosta mjesta, konačna ili beskonačna, dijele $\mathfrak{m}$ *tako da za*

$$\Phi_m : I_K(\mathfrak{m}) \longrightarrow Gal(L/K)$$

Artinovo preslikavanje od $K \subset L$ *vrijedi*

$$H = \mathrm{Ker}(\Phi_m).$$

Dokaz: Vidi ([4, Teorem 9.16].)

Ovaj teorem nam omogućuje konstrukciju Abelovih proširenja od K s unaprijed određenim Galoisovim grupama i određenim grananjem.

Iako smo dokaze preskočili, dokazat ćemo neposrednu korist ovih teorema. Prvo navedimo korolar jedinstvenosti iz teorema o egzistenciji.

Korolar 2.4.6. *Neka su L i M Abelova proširenja od K. Tada je* $L \subset M$ *ako i samo ako postoji modulus* $\mathfrak{m}$*, djeljiv sa svim prostima od K koji se granaju u L ili u M, tako da*

$$P_{K,1}(\mathfrak{m}) \subset \mathrm{Ker}(\Phi_{M/K,\mathfrak{m}}) \subset \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}}).$$

Dokaz: Neka je $L \subset M$ i preslikavanje $r : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ restrikcija na L. Po Artinovom zakonu reciprociteta (2.4.2) i (2.9), postoji modulus $\mathfrak{m}$ takav da su $\mathrm{Ker}(\Phi_{M/K,\mathfrak{m}})$ i $\mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$ obje kongruencijske podgrupe od $\mathfrak{m}$. [1, Exercise 5.16] pokazuje da je $r \circ \Phi_{M/K,\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}}$ pa je $\mathrm{Ker}(\Phi_{M/K,\mathfrak{m}}) \subset \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$.

Obratno, neka je $P_{K,1}(\mathfrak{m}) \subset \mathrm{Ker}(\Phi_{M/K,\mathfrak{m}}) \subset \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$. Tada uz preslikavanje $\Phi_{M/K,\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(M/K)$, podgrupa $\mathrm{Ker}(\Phi_{L/K,\mathfrak{m}}) \subset I_K(\mathfrak{m})$ se preslika u podgrupu $H \subset \mathrm{Gal}(M/K)$. Po Galoisovoj teoriji, H odgovara međupolju $K \subset \tilde{L} \subset M$. Po prvom dijelu dokaza, za $\tilde{L} \subset M$, vrijedi $\mathrm{Ker}(\Phi_{\tilde{L}/K,\mathfrak{m}}) = \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$. Tada po jedinstvenosti u (2.4.5) vrijedi $L = \tilde{L} \subset M$ i dokazali smo tvrdnju. Q.E.D.

Za primjer, pokazat ćemo da je konduktor proširenja $L = \mathbb{Q}(\zeta_m)$ od $K = \mathbb{Q}$ jednak

$$\mathfrak{f}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \begin{cases} 1 & m = 1, 2, \\ (m/2)\infty & m = 2n,\ n > 1 \text{ neparan}, \\ m\infty & \text{inače}. \end{cases}$$

Promotrimo po slučajevima. Za $m = 1, 2$ $L = \mathbb{Q}$ pa je tvrdnja trivijalna. Za $m > 2$ koristimo teorem o konduktoru. Po tvrdnji (i) $\mathfrak{f}$ mora biti djeljiv sa svim prostim mjestima koji se granaju u L stoga je oblika $\mathfrak{n} = n\infty$ za neki prirodan broj n. Po (ii) n mora dijeliti m.

Može se pokazati iz korolara (2.4.6) da je $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$. No, to znači da $\phi(m) \mid \phi(n)$, pa je $\phi(n) = \phi(m)$. Ako je m oblika $2k$, gdje je k neparan prirodan broj, onda možemo uzeti $n = m/2$. Inače, $n = m$.

Navest ćemo samo dvije primjene koje će nadamo se prisvojiti čitatelja. Kao jednostavni korolar dobivamo slavni teorem koji kaže da je svako abelovo proširenje od $\mathbb{Q}$ sadržano u nekom ciklotomskom polju.

Teorem 2.4.7. *(Kronecker-Weber) Neka je L Abelovo proširenje od $\mathbb{Q}$. Tada postoji prirodni broj m tako da je*

$$L \subset \mathbb{Q}(\zeta_m), \qquad \zeta_m = e^{2\pi i/m}.$$

Dokaz: Po Artinovom teoremu o reciprocitetu (2.4.2), postoji modulus $\mathfrak{m}$ takav da je $P_{\mathbb{Q},1}(\mathfrak{m}) \subset \mathrm{Ker}(\Phi_{L/\mathbb{Q},\mathfrak{m}})$ i po (2.9) možemo pretpostaviti $\mathfrak{m} = m\infty$. Po (2.8) znamo da je $P_{\mathbb{Q},1}(\mathfrak{m}) = \mathrm{Ker}(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}})$ pa je

$$P_{\mathbb{Q},1}(\mathfrak{m}) = \mathrm{Ker}(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}, \mathfrak{m}) \subset \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}}).$$

Tada po prethodnom korolaru (2.4.6) slijedi $L \subset \mathbb{Q}(\zeta_m)$. Q.E.D.

Ovo je jedna lijepa primjena teorije polja klasa, iako postoji i elementaran dokaz. Ipak za postojanje Hilbertova polja klasa, ova diskusija je neophodna. Možemo ga definirati na idući način. Uzmimo modulus $\mathfrak{m} = 1$ i podgrupu $P_K \subset I_K$ (ovdje $P_K = P_{K,1}(\mathfrak{m})$. Primjenjujući teorem o egistenciji (2.4.5), postoji jedinstveno Abelovo proširenje L od K, nerazagranato jer $\mathfrak{m} = 1$, tako da Artinovo preslikavanje inducira izomorfizam u

$$C(O_K) = I_K/P_K \cong \mathrm{Gal}(L/K). \tag{2.10}$$

Polje L je *Hilbertovo polje klasa* i vrijedi:

Teorem 2.4.8. *Hilbertovo polje klasa L je maksimalno nerazgranato Abelovo proširenje od K.*

Dokaz: Znamo da je L nerazgranato i Abelovo. Neka je M neko drugo takvo proširenje. Po teoremu o konduktoru (2.4.4) $\mathfrak{f}(M/K) = 1$ jer se mjesta granaju ako i samo dijele konduktor. Po drugom dijelu teorema o konduktoru, znamo da je $\mathrm{Ker}(\Phi_{M/K,1})$ kongruencijska podgrupa za modulus 1. Stoga je

$$P_K \subset \mathrm{Ker}(\Phi_{M/K,1}).$$

Po definiciji Hilbertova polja klasa, to postaje

$$P_K = \mathrm{Ker}(\Phi_{L/K,1} \subset \mathrm{Ker}(\Phi_{M/K,1})$$

i $M \subset L$ slijedi po korolaru (2.4.6). Q.E.D.

2.5 Polje prstena klasa

Nakon zadnje diskusije možemo dokazati glavni teorem (1.4.2) u općem slučaju. Dokaz (i rezultat) će nalikovati već danome - samo sada koristeći ideale u O. Nakon toga će preostati dati algoritam za računanje $f_n(x)$.

Rješenje koje smo dosad izveli se sastojalo u konstruiranju Hilbertova polja klasa - koje je bilo izomorfno grupi klasa ideala u prstenu cijelih brojeva. Sada ćemo analogno definirati polje prstena klasa, ovaj puta za redove.

Za polje brojeva K, ideal $\mathfrak{m}$ u O_K možemo shvatiti kao modulus kao u definiciji(2.4.1). Prethodno smo definirali grupe ideala $I_K(\mathfrak{m})$ i $P_{K,1}(\mathfrak{m})$. Ako je $\mathfrak{m} = \alpha O_K$ glavni ideal, iste grupe ćemo označavati s $I_K(\alpha)$ i $P_{K,1}(\alpha)$.

Kao najavljeno, promotrimo red O u imaginarnom kvadratnom polju K. Znamo iz propozicije (2.3.14) da se grupa klasa ideala $C(O)$ može napisati kao

$$C(O) = I_K(f)/P_{K,\mathbb{Z}}(f).$$

Iz teorije polja klasa zaključili smo da

$$P_{K,1}(f) \subset P_{K,\mathbb{Z}}(f) \subset I_K(f),$$

pa je $C(O)$ generalizirana grupa klasa ideala od K za modulus fO_K. Po teoremu o egzistenciji (2.4.5), ovo određuje jedinstveno Abelovo proširenje L od K, koje se naziva *polje prstena klasa* reda O.

Dva svojstva tog polja su da razgranata mjesta od K u L dijele f te da Artinovo preslikavanje nam daje izomorfizam

$$C(O) \cong I_K(f)/P_{K,\mathbb{Z}}(f) \cong \mathrm{Gal}(L/K). \tag{2.11}$$

Ovo napokon objašnjava zašto je stupanj polinoma iz glavnog teorema jednak baš broju klasa. Primijetimo da je svako Hilbertovo polje klasa isto polje prstena klasa (za maksimalni red O_K). Vidjet ćemo da će biti malo razlike između ovog općenitijeg slučaja i već obrađenog.

Navodimo sada glavni teorem, za sve proste brojeve:

Teorem 2.5.1. *Neka je n prirodan broj. Tada postoji normirani ireducibilni polinom $f_n(x) \in \mathbb{Z}[x]$ stupnja $h(-4n)$ takav da za neparan prost broj p koji ne dijeli n niti diskriminantu od $f_n(x)$ vrijedi:*

$$p = x^2 + ny^2 \iff \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ i } f_n(x) \equiv 0 \text{ mod } p \\ \text{ima cjelobrojno rješenje} \end{cases}$$

Za $f_n(x)$ se može uzeti minimalni polinom realnog *algebarskog cijelog broja α za koji je $L = K(\alpha)$ polje prstena klasa reda $\mathbb{Z}[\sqrt{-n}]$.*

Konačno, ako je $f_n(x)$ bilo koji normirani polinom stupnja $h(-4n)$ za koji gornja ekvivalencija vrijedi, tada je $f_n(x)$ ireducibilan nad $\mathbb{Z}$ i minimalni polinom je polinom primitivnog elementa polje prstena klasa L.

Dokaz će se provoditi analognu dokazu posebnog slučaja (2.1.1).

Prvo dokažimo općenitu lemu o poljima prstena klasa.

Lema 2.5.2. *Neka je L polje prstena klasa reda O u imaginarnom kvadratnom polju K. Tada je L Galoisovo proširenje od $\mathbb{Q}$ i Galoisova grupa nad $\mathbb{Q}$ je semidirektni produkt*

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(L/K) \rtimes \mathbb{Z}/2\mathbb{Z},$$

gdje netrivijalni element od $\mathbb{Z}/2\mathbb{Z}$ djeluje na $Gal(L/K)$ tako da šalje σ u σ^{-1}.

Dokaz: Primijetimo da smo već dio dokazali za Hilbertovo polje klasa (2.2.2). Neka je τ kompleksno konjugiranje. Pokažimo da je τ automorfizam. Neka je modulus $\mathfrak{m} = fO_K$ i primijetimo $\tau(\mathfrak{m}) = \mathfrak{m}$. Kako je $\mathrm{Ker}(\Phi_{L/K,\mathfrak{m}}) = P_{K,\mathbb{Z}}(f)$, lako se vidi da je

$$\mathrm{Ker}(\Phi_{\tau(L)/K,\mathfrak{m}}) = \tau(\mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})) = \tau(P_{K,\mathbb{Z}}(f)) = P_{K,\mathbb{Z}}(f).$$

Što se tiče prve jednakosti, Φ djeluje jednako na $\tau(L)$ kao i na L samo je sve konjugirano:

$$\Phi_{L/K,\mathfrak{m}}(\mathfrak{a})(\alpha) = \alpha,$$
$$\Phi_{\tau(L)/K,\mathfrak{m}}(\tau(\mathfrak{a}))(\tau(\alpha)) = \tau(\alpha).$$

Stoga je

$$\mathrm{Ker}(\Phi_{L/K,\mathfrak{m}}) = \tau(\mathrm{Ker}(\Phi_{\tau(L)/K,\mathfrak{m}}))$$

i preostaje primijeniti τ. Za treću jednakost, $\tau(\mathfrak{m}) = \mathfrak{m} = fO_K$, isto kao u (2.3.3), pa je

$$\begin{aligned} P_{K,\mathbb{Z}}(f) &= \{\alpha O_K | \alpha \equiv a \bmod fO_K\} \\ &= \{\alpha O_K | \tau(\alpha) \equiv \tau(a) \bmod \tau(fO_K)\} \\ &= \{\alpha O_K | \tau(\alpha) \equiv a \bmod fO_K)\} \\ &= \tau(P_{K,\mathbb{Z}}(f)), \end{aligned}$$

te imamo zadnju jednakost. Vidimo da je $\mathrm{Ker}(\Phi_{\tau(L)/K,\mathfrak{m}}) = \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$ i po korolaru (2.4.6), slijedi $\tau(L) = L$.

Isto kao i u lemi (2.2.2), $\tau(L) = L$ i to da je L Galoisovo nad K povlači da je L Galoisovo nad $\mathbb{Q}$ pa imamo egzaktni niz

$$1 \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow 1$$

gdje je $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$. Prema tome je $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(L/K) \rtimes (\mathbb{Z}/2\mathbb{Z})$, tako da netrivijalni element iz $\mathbb{Z}/2\mathbb{Z}$ djeluje konjugiranjem s τ. Za prosti ideal $\mathfrak{p}$ od K konjugiranje s τ rezultira s:

$$\tau\left(\frac{L/K}{\mathfrak{p}}\right)\tau^{-1} = \left(\frac{L/K}{\tau(\mathfrak{p})}\right) = \left(\frac{L/K}{\bar{\mathfrak{p}}}\right)$$

po teoremu (2.1.7). Ako je $\mathfrak{a}$ ideal u $I_K(f)$, tada $\mathfrak{a}\bar{\mathfrak{a}} = N(\mathfrak{a})O_K$ leži u $P_{K,\mathbb{Z}}(f)$ jer je $N(\mathfrak{a})$ prosto s f. Stoga je $\bar{\mathfrak{a}}$ inverz od $\mathfrak{a}$ u kvocijentu $I_K(f)/P_{K,\mathbb{Z}}(f)$. Za $\sigma \in \mathrm{Gal}(L/K)$ dobili smo σ^{-1} i time je lema dokazana.

Q.E.D.

Teorem 2.5.3. *Neka je n prirodan broj i L polje prstena klasa reda $\mathbb{Z}[\sqrt{-n}]$. Ako je p prost broj koji ne dijeli $-4n$, tada*

$$p = x^2 + ny^2 \iff p \text{ se potpuno razlaže u } L$$

Dokaz: Neka je $O = \mathbb{Z}[\sqrt{-n}]$. Diskriminanta od O je $-4n = f^2 d_K$, gdje je f konduktor od O. Neka je p neparan prost broj koji ne dijeli $-4n$. Tada p ne dijeli diskriminantu reda $f^2 d_K$ pa ni d_K pa je p nerazgranat u K. Dokaz možemo opet podijeliti u nekoliko ekvivalencija:

$$\begin{aligned} p = x^2 + ny^2 &\iff pO_K = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}}, \text{ i } \mathfrak{p} = \alpha O_K, \text{za neki } \alpha \in O \\ &\iff pO_K = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}}, \text{ i } \mathfrak{p} \in P_{K,\mathbb{Z}}(f) \\ &\iff pO_K = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}}, \text{ i } ((L/K)/\mathfrak{p}) = 1 \\ &\iff pO_K = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}}, \text{ i } \mathfrak{p} \text{ se potpuno razlaže u } L \\ &\iff p \text{ se potpuno razlaže u } L. \end{aligned}$$

(i) Neka je $p = x^2 + ny^2 = (x + \sqrt{-n}y)(x - \sqrt{-n}y)$. Stavljajući $\mathfrak{p} = (x + \sqrt{-n}y)O_K$, vidimo da je $pO_K = \mathfrak{p}\bar{\mathfrak{p}}$ faktorizacija u proste od pO_K u O_K. Vrijedi da je $\mathfrak{p} \neq \bar{\mathfrak{p}}$ jer je p nerazgranat u O_K i $\mathfrak{p} = \alpha O_K$ gdje je $\alpha = x + \sqrt{-n}y \in O$. Obratno, ako je $pO_K = \mathfrak{p}\bar{\mathfrak{p}}$, ideal $\mathfrak{p}$ u O je oblika $\mathfrak{p} = (x + \sqrt{-n}y)$ za neke $x, y \in \mathbb{Z}$. Jedina realna pozitiva jedinica u imaginarnom kvadratnom polju je 1 i slijedi da je $p = x^2 + ny^2$.

(ii) p ne dijeli f pa ovo slijedi iz propozicije (2.3.14).

(iii) Izomorfizam između $C(O) = I_K(f)/P_{K,\mathbb{Z}}(f)$ dan Artinovim preslikavanjem pokazuje da je $\mathfrak{p} \in P_{K,\mathbb{Z}}(f)$ ako i samo ako je $((L/K)/\mathfrak{p}) = 1$.

(iv) Tada je po teoremu (2.1.7) $((L/K)/\mathfrak{p}) = 1$ ako i samo ako $\mathfrak{p}$ se potpuno razlaže u L.

(v) Iz (2.5.2) slijedi da je L Galoisovo nad $\mathbb{Q}$. Stoga je dokaz zadnje ekvivalencije isti kao i kod Hilbertova polja klasa (2.2). Q.E.D.

Spremni smo dokazati glavnu ekvivalenciju teorema 2.5.1. Po lemi (2.5.2) polje prstena klasa L je Galoisovo nad $\mathbb{Q}$ i po propozoziji (2.2.3) možemo naći realni algebarski cijeli broj tako da je $L = K(\alpha)$. Neka je $f_n(x) \in \mathbb{Z}[x]$ minimalni polinom od α nad K. Kako je O diskriminante $-4n$, stupanj proširenja je $[L : K] = h(O) = h(-4n)$. Tada kombiniranjem 2.5.3 i zadnjeg dijela propozicije (2.2.3), imamo:

$$\begin{aligned} p = x^2 + ny^2 &\iff p \text{ se potpuno razlaže u } L \\ &\iff \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ i } f_n(x) \equiv 0 \bmod p \\ \text{ima cjelobrojno rješenje,} \end{cases} \end{aligned}$$

kada god je p neparan prost broj koji ne dijeli n ili diskriminantu od $f_n(x)$. Time je napokon dokazan naš glavni teorem!

Preostaje ipak još komentirati "sporedni" dio teorema. Vidimo da je dovoljno da je $f_n(x)$ minimalni polinom primitivnog elementa RCF(-n). Ustvari polinom *mora* biti minimalni polinom nekog primitivnog elementa od RCF(-n) (odnosno $f_n(x)$ mora imati polje razlaganja RCF(-n)). Za dokaz vidi [1, str. 165].

Još navedimo da se može maknuti uvjet da p ne dijeli $\operatorname{disc} f_n(x)$ za određeni polinom $f_n(x)$, no to slijedi iz vrlo komplicirane teorije (Gross-Zagier). Time smo napokon objasnili teorem iz uvoda (1.4.2).

Poglavlje 3

Primjene

Dolazimo do zadnjeg dijela našeg teorema, a to je eksplicitno određivanje polinoma iz glavnog teorema. Objasnit ćemo općenitu numeričku metodu, a potom i razmotriti pokoji posebni slučaj. Posebno ćemo raspisati one slučajeve koji su u [1] riješeni na druge, vrlo posebne načine. Ovime želimo istaknuti kako se problem općenito može riješiti ovom metodom. Iako je ovaj postupak potpuno efektivan, veličina brojeva koji se pojavljuju u računu ipak čini ovaj problem dosta nespretnim za veće n.

3.1 j-invarijanta

Definirajmo objekt iz naslova. Prvo definiramo za kompleksni τ, Im $\tau > 0$ Eisensteinove redove:

$$g_2(\tau) = 60 \sum_{m,n}{}' \frac{1}{(m+n\tau)^4},$$
$$g_3(\tau) = 140 \sum_{m,n}{}' \frac{1}{(m+n\tau)^6},$$

gdje znak sume s crticom označava da sume idu po svim m, n cijelim brojevima osim $m = n = 0$. Redovi apsolutno konvergiraju. Sada se definira j-invarijanta:

$$j(\tau) = 1728 \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2}. \tag{3.1}$$

Trebat ćemo računati j-invarijantu, i iako bismo je mogli i ovako računati iz definicije, odvojimo ipak koju riječ o efektivnijem načinu.

Primijetimo da su $g_2(\tau)$ i $g_3(\tau)$ periodične funkcije od τ s periodom 1 pa je prirodno zapitati se o njihovim Fourierovim redovima. Koristeći zanimljive, ali dobro poznate trikove

oni se mogu lako izračunati (vidi knjigu od Apostola [5], str. 18-20)

$$g_2(\tau) = \frac{4\pi^2}{3}\left(1 + 240\sum_{k=1}^{\infty}\sigma_3(k)e^{2\pi ikt}\right),$$
$$g_3(\tau) = \frac{8\pi^6}{27}\left(1 - 504\sum_{k=1}^{\infty}\sigma_5(k)e^{2\pi ikt}\right),$$

gdje je $\sigma_p(k) = \sum_{d|k} d^p$ dobro poznata multiplikativna funkcija. Sada ako označimo $\Delta(\tau) = g_2(\tau)^2 - 27g_3(\tau)^3$ imamo i Fourierov razvoj te funkcije (vidi [5], str. 20-21)

Teorem 3.1.1. *Za* $\operatorname{Im}\tau > 0$ *imamo Fouerirov red:*

$$\Delta(\tau) = (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)e^{2\pi int},$$

gdje su koeficijenti $\tau(n)$ *cijeli brojevi.*

Funkcija $\tau(n)$ je slavna Ramanujanova τ funkcija. Promatrajući $\tau(n)$ moglo bi se pomisliti da se (po aps. vrijednosti) povećava no otvorena je slutnja da je $\tau(n) \neq 0$ za sve n. Napokon smo spremni za glavni teorem o Fourierovom redu j-invarijante (vidi [5], str. 21):

Teorem 3.1.2. *Za* $\operatorname{Im}\tau > 0$ *vrijedi Fourierov red:*

$$j(\tau) = e^{-2\pi it} + 744 + \sum_{n=1}^{\infty} c(n)e^{2\pi int},$$

gdje su $c(n)$ *cijeli brojevi.*

Često se označava $q = e^{2\pi it}$ pa se red prikaže kao Laurentov. Za alternativni izvod vidi Coxa [1]. Preferiramo izvod u Apostolu jer ne prikazuje svojstvo dubljim nego što jest.

Navodimo slavni teorem o j-invarijanti i razlog zašto smo je uveli ovdje. Primitivnoj kvadratnoj formi smo dosad pridružili ideal, a sada ćemo pridružiti i kompleksan broj na idući način:

$$ax^2 + bxy + cy^2 \longleftrightarrow \mathfrak{a} = \left[a, \frac{-b + \sqrt{D}}{2}\right] \longleftrightarrow \tau = \frac{-b + \sqrt{D}}{2a}$$

Ako stavimo $j(\mathfrak{a}) = j(\tau)$, tada vrijedi idući teorem:

Teorem 3.1.3. *Neka je* O *red u* $K = \mathbb{Q}(\sqrt{(-n)})$ *i* $\mathfrak{a}$ *pravi razlomljeni ideal u* O*. Tada je j-invarijanta* $j(\mathfrak{a})$ *algebarski cijeli broj i* $K(j(\mathfrak{a}))$ *polje prstena klasa reda* O*.*

Ovdje se od čitatelja traži povjerenje na riječ, što za ovakvu tvrdnju sigurno i nije malen zahtjev! Dokaz se može naći u [1]. U svakom slučaju, teorem će nam dati konkretne rezultate, u koje ćemo se eksplicitno uvjeriti.

Fiksirajmo red O u imaginarnom kvadratnom polju K.

Teorem 3.1.4. *Za ideale* $\mathfrak{a}$ *koji odgovaraju reduciranim formama diskriminante* $D = disc\ O$*, vrijedi da su* $j(\mathfrak{a})$ *konjugati.*

Kako je broj reduciranih formi jednak $h(O)$, to je $j(\mathfrak{a})$ ustvari algebarski cijeli broj stupnja $h(O)$! I ovaj teorem je dokazan u [1]. Promotrimo ovo na primjerima.

Računanje s j-invarijantom

Primjer 3.1.5. *Ramanujanova konstanta. Slavna "slučajnost" u teoriji brojevi je bliskost* $e^{\pi\sqrt{163}}$ *cijelom broju. Ustvari nas to i ne treba začuditi. Uvrstimo* $\tau = \frac{-1+\sqrt{-163}}{2}$ *u*

$$j(\tau) = e^{-2\pi i\tau} + 744 + 196884e^{2\pi i\tau} + ...$$

S lijeve strane, znamo da je $j(\tau)$ *algebarski cijeli broj stupnja* $h(-163) = 1$ *- dakle cijeli broj, konkretno* -640320^3*. S desne strane, promatrajući pojedine članove reda*

$$j(\tau) = -e^{\pi\sqrt{163}} + 744 + 196884e^{-\pi\sqrt{163}} + ...$$

možemo vidjeti da već nakog drugog člana red konvergira tako brzo da ih možemo za prvu aproksimaciju zanemariti, a tada dobivamo

$$e^{\pi\sqrt{163}} \approx 640320^3 + 744.$$

Slične identitete dobivamo i za druge diskriminante čiji je broj klasa 1.

Primjer 3.1.6. *Naveli smo bili reducirane forme za* $D = -56$*. Promotrimo pripadne* τ*:*

$f(x,y)$	τ	$j(\tau)$
$x^2 + 14y^2$	$\sqrt{-14}$	16220257532.0595
$2x^2 + 7y^2$	$\frac{\sqrt{-14}}{2}$	128104.319158248
$3x^2 + 2xy + 5y^2$	$\frac{-1+\sqrt{-14}}{3}$	$-562.18933047290 - 2127.76194138925i$
$3x^2 - 2xy + 5y^2$	$\frac{1+\sqrt{-14}}{3}$	$-562.18933047290 - 2127.76194138925i$

Ovdje smo izračunali $j(\tau)$ *na* 15 *decimala. Nipošto nije jasno o kojim bi se algebarskim brojevima stupnja* 4 *radilo - iako znamo da moraju biti takvi. Ipak možemo (numerički) izračunati polinom u npr. Wolfram Mathematica, zaokružujući na najbliže cijele brojeve:*

$$\prod_{\tau}(X - j(\tau)) = X^4 - 16220384512X^3 + 2059647197077504X^2 + 225776734208891289 6X + 10064086044321563803648$$

Sada eksplicitnim rješavanjem jednadžbe četvrtog stupnja dobivamo konkretne algebarske izraze za $j(\tau)$. Tako je npr.

$$j(\sqrt{-14}) = 4055096128+2867386368\sqrt{2}+1792\sqrt{10241006292718 + 7241484995756\sqrt{2}}$$

Ostale nultočke se odmah dobiju prikladnom promjenom predznaka (ispred velikog korijena, i ispred svake pojave $\sqrt{2}$). Primijetimo da smo u prošlom primjeru, iako znamo da je vrijednost j-invarijante morala biti cijeli broj, dobili čak kub *cijelog broja. Tako i ovdje - uzimajući treći korijen, dobit ćemo opet (cijeli) algebarski broj 4. stupnja te ga možemo odrediti iz mininalnog polinoma. Vidimo da je i ovdje dakle j-invarijanta kub*

$$j(\sqrt{-14}) = 2^3\left(323 + 228\sqrt{2} + 7\sqrt{3925 + 2776\sqrt{2}}\right)^3.$$

Ovo se još malo može pojednostaviti [1, p. 226] *u*

$$j(\sqrt{-14}) = 2^3\left(323 + 228\sqrt{2} + 7(231 + 161\sqrt{2})\sqrt{2\sqrt{2} - 1}\right)^3.$$

Primjer 3.1.7. *Sada smo spremni navesti primjer našeg generalnog teorema: lako se vidi iz prethodnog primjera da je $\mathbb{Q}\left(j\left(\sqrt{-14}\right)\right) = \mathbb{Q}\left(\sqrt{2\sqrt{2}-1}\right)$. Minimalni polinom za taj primitivni element je X^4+2X^2-7. (Primijetimo da smo mogli uzeti i polinom iz prethodnog primjera ili minimalni polinom od $\sqrt[3]{j(\tau)}$.) Po glavnom teoremu (1.4.2)*

$$p = x^2 + 14y^2 \iff \left(\frac{-14}{p}\right) = 1 \quad \text{i} \quad X^4 + 2X^2 - 7 \equiv 0 \bmod p.$$

Dakle, u teoriji j-invarijantu nije teško izračunati na dovoljnu numeričku preciznost te se iz nje može izračunati jednadžba klasa. Pitanje je kako j-invarijantu svesti na jednostavniji algebarski broj koji generira isto polje. Jedan način je koristiti neki manji broj npr. ako znamo da je j-invarijanta kub, uzet ćemo treći korijen. U 3.1.6 vidimo da smo nekako pojednostavili izraz $3925 + 2776\sqrt{2} = \left(232 + 161\sqrt{2}\right)^2\left(2\sqrt{2} - 1\right)$. Ustvari to i nije tako bilo teško - $h(\mathbb{Q}(\sqrt{2})) = 1$ tako da postoji jedinstvena faktorizacija do na jedinice. Za teže slučajeve CAS Sage je vrlo dobro opremljen (besplatna online verzija je dostupna na stranici `https://www.sagemath.org/`).

Promotrimo primjer iz Gaussovih zakona višeg reciprociteta.

Primjer 3.1.8. *Dokažimo da je*

$$p = x^2 + 27y^2 \iff \left(\frac{-27}{p}\right) = 1 \text{ i } t^3 \equiv 2 \bmod p \text{ ima rješenje.}$$

Kao u prethodnom primjeru, napravimo popis reduciranih formi. Vidimo da će jednadžba klasa biti polinom stupnja 3 *jer imamo* 3 *reducirane forme te diskriminante:*

$$x^2 + 27y^2, 4x^2 - 2xy + 7y^2, 4x^2 + 2xy + 7y^2.$$

Sada računamo jednadžbu klasa:

$$\prod_{\tau}(X - j(\tau)) =$$

$$X^3 - 151013228706000X^2 + 224179462188000000X - 1879994705688000000000$$

Rješavajući je u Wolfram Mathematici dobivamo da je

$$j\left(\sqrt{-27}\right) = 6000(8389623817 + 6658848836 \cdot 2^{1/3} + 5285131824 \cdot 2^{2/3}).$$

Stoga je $RCF(-27) = \mathbb{Q}(\sqrt{-27}, \sqrt[3]{2})$. *Dakle, po glavnom teoremu* -27 *mora biti kvadrat, a* 2 *mora biti kub modulo p.*

Zadnjim primjerom je ilustrirano koliko je jaka teorija kompleksnog množenja - jer iz nje dobivamo poznate teoreme kao trivijalne korolare.

3.2 Dodaci

Problem broja klasa za parne diskriminante

Famozni problem od Gaussa je pitanje: za koje sve diskriminante je broj klasa jednak 1? Kako je Gauss promatrao forme oblika $ax^2 + 2bxy + cy^2$ tj. one sa srednjim koeficijentom parnim, njegovo pitanje je jednostavnije nego problem za općenite forme s neparnim b. Primijetimo ako je D paran onda je zbog $D = b^2 - 4ac$ i b paran. Za forme oblika $x^2 + ny^2$ diskriminanta je $-4n$ pa je uvijek parna. Dakle, ako riješimo Gaussov problem saznat ćemo za koje je forme $x^2 + ny^2$ dovoljan samo uvjet $\left(\frac{-n}{p}\right) = 1$. Navodimo rješenje od Landaua.

Teorem 3.2.1. *Jedine parne diskriminante* $D < 0$ *s brojem klasa* $h(D) = 1$ *su* $D = -4, -8, -12, -16, -28$.

Dokaz: Eksplicitnom konstrukcijom ćemo pokazati da za svaki drugi slučaj postoji još jedna forma. Za ovih 5 slučajeva se onda lako provjeri da postoji samo jedna.

Prvo, neka n nije potencija prostog broja. Tada je $n = ac$ gdje možemo uzeti $1 < a < c$ i $gcd(a, c) = 1$ i onda je forma

$$ax^2 + cy^2$$

reducirana i diskriminante $-4ac = -4n$. Stoga je $h(-4n) > 1$.

Iduće, pretpostavimo da $n = 2^r$. Ako je $r \geq 4$, tada

$$4x^2 + 4xy + (2^{r-2} + 1)y^2$$

ima relativno proste koeficijente i reducirana je jer je $4 \leq 2^{r-2} + 1$. Računajući diskriminantu, vidimo da je jednaka $-4n$ pa smo našli još jednu forme dane diskriminante. Za $n = 8$, izračuna se $h(-4 \cdot 8) = 2$, pa preostaje $h(-4 \cdot 2) = h(-4 \cdot 4) = 1$.

Napokon, neka je $n = p^r$ gdje je p neparan prost broj. Ako se $n + 1$ može napisati kao umnožak dva broja $n + 1 = ac$, s $2 \leq a < c$ i $gcd(a, c) = 1$, tada je

$$ax^2 + 2xy + cy^2$$

reducirana forma diskriminante $-4n$. Ako se $n + 1$ ne može faktorizirati na rel. proste faktore, mora biti potencija prostog broja. Kako je $n = p^r$ neparan, moralo bi biti $n = 2^s$. Možemo isključiti ovaj slučaj pozivajući se na, sada dokazanu, Catalanovu slutnju, ili primjećujući u duhu cijelog dokaza da je za $s \geq 6$

$$8x^2 + 6xy + (2^{s-3} + 1)y^2$$

reducirana forma diskriminante $-4n$. Za $s = 1, 2, 3, 4, 5$ direktnim računom provjere se preostali slučajevi. Time su svi slučajevi provjereni i teorem dokazan. Q.E.D.

Cohnov primjer

Promotrimo proste brojeve oblika $4k + 1$. Primijetimo da je svaki ustvari oblika $x^2 + 4y^2$. Što je s $x^2 + 16y^2$? Jasno je da je takav oblika $8k + 1$. S druge strane ako je broj oblika $8k + 1$ onda jest suma dva kvadrata pa je oblika $x^2 + 16y^2$. Vidimo da za $n = 64$ su stvari ipak dosta drukčije postale i više nisu jednostavni kongruencijski uvjeti. No, primijetimo:

$$p = x^2 + 4y^2 \iff u^2 \equiv -1 \bmod p, \text{ za neki } u \in \mathbb{Z},$$

$$p = x^2 + 16y^2 \iff \begin{cases} u^2 \equiv -1 \bmod p \\ v^2 \equiv 2 \bmod p \end{cases} \quad \text{za neke } u, v \in \mathbb{Z},$$

$$p = x^2 + 64y^2 \iff \begin{cases} u^2 \equiv -1 \bmod p \\ v^2 \equiv 2 \bmod p \\ w^2 \equiv v \bmod p \end{cases} \quad \text{za neke } u, v, w \in \mathbb{Z}.$$

Ustvari, ([6]) daje idući rekurzivni niz kongruencija koje moraju biti zadovoljene:

$$p = x^2 + 4 \cdot 4^t y^2 \iff \begin{cases} r_0^2 \equiv -1 \bmod p \\ r_1^2 \equiv 9/8 \bmod p \\ r_{s+1}^2 \equiv (r_s + 3)^2/(8(r_s + 1)) \end{cases} \quad \text{za neke } r_i \in \mathbb{Z}.$$

Ovdje se pod dijeljenjem naravno podrazumijeva množenje s inverzom mod p. Vidi ([6]) za još sličnih primjera.

3.3 Zaključak

U idućoj tablici navodimo popis polja prstena klasa i pripadnih minimalnih polinoma nad K za prvih 50 n.

n	RCF$(-4n)$	$f_n(x)$
1	$\mathbb{Q}(\sqrt{-1})$	–
2	$\mathbb{Q}(\sqrt{-2})$	–
3	$\mathbb{Q}\left(\sqrt{-3}\right)$	–
4	$\mathbb{Q}(\sqrt{-4})$	–
5	$\mathbb{Q}(\sqrt{-5}, \sqrt{5})$	$x^2 - 5$
6	$\mathbb{Q}(\sqrt{-6}, \sqrt{2})$	$x^2 - 2$
7	$\mathbb{Q}(\sqrt{-7})$	–
8	$\mathbb{Q}(\sqrt{-8}, \sqrt{2}) = \mathbb{Q}(\zeta_8)$	$x^2 - 2$
9	$\mathbb{Q}(\sqrt{-9}, \sqrt{3})$	$x^2 - 3$
10	$\mathbb{Q}(\sqrt{-10}, \sqrt{5})$	$x^2 - 5$
11	$\mathbb{Q}(\sqrt{-11}, \sqrt[3]{17 + 3\sqrt{33}} - \sqrt[3]{-17 + 3\sqrt{33}})$	$x^3 + 6x - 34$
12	$\mathbb{Q}(\sqrt{-12}, \sqrt{3})$	$x^2 - 3$
13	$\mathbb{Q}(\sqrt{-13}, \sqrt{13})$	$x^2 - 13$
14	$\mathbb{Q}(\sqrt{-14}, \sqrt{2\sqrt{2} - 1})$	$x^4 + 2x^2 - 7$
15	$\mathbb{Q}(\sqrt{-15}, \sqrt{5})$	$x^2 - 5$
16	$\mathbb{Q}(\sqrt{-16}, \sqrt{2})$	$x^2 - 2$
17	$\mathbb{Q}(\sqrt{-17}, \sqrt{\frac{1+\sqrt{17}}{2}})$	$x^4 - x^2 - 4$
18	$\mathbb{Q}(\sqrt{-18}, \sqrt{6})$	$x^2 - 6$
19	$\mathbb{Q}(\sqrt{-19}, \sqrt[3]{-2197 + 291\sqrt{57}} - \sqrt[3]{2197 + 291\sqrt{57}})$	$x^3 + 6x + 4394$
20	$\mathbb{Q}(\sqrt{-20}, \sqrt{\sqrt{5} - 2})$	$x^4 + 4x^2 - 1$
21	$\mathbb{Q}(\sqrt{-21}, \sqrt{-3}, \sqrt{-7})$	$x^2 - 3, x^2 - 7$
22	$\mathbb{Q}(\sqrt{-22}, \sqrt{2})$	$x^2 - 2$
23	$\mathbb{Q}(\sqrt{-23}, \sqrt[3]{\frac{25-3\sqrt{69}}{2}} + \sqrt[3]{\frac{25+3\sqrt{69}}{2}})$	$x^3 - 3x - 25$
24	$\mathbb{Q}(\sqrt{-24}, \sqrt{2}, \sqrt{3})$	$x^2 - 2, x^2 - 3$
25	$\mathbb{Q}(\sqrt{-25}, \sqrt{5})$	$x^2 - 5$
26	$\mathbb{Q}(\sqrt{-26}, \sqrt{13}, t)$	$x^2 - 13, x^3 - 3x - 162 + 44\sqrt{13}$
27	$\mathbb{Q}(\sqrt{-27}, \sqrt[3]{2})$	$x^3 - 2$
28	$\mathbb{Q}(\sqrt{-28}, \sqrt{7})$	$x^2 - 7$

29	$\mathbb{Q}(\sqrt{-29}, \sqrt[3]{28-3\sqrt{87}}+\sqrt[3]{28+3\sqrt{87}})$	$x^3-3x-56$
30	$\mathbb{Q}(\sqrt{-30}, \sqrt{2}, \sqrt{5})$	x^2-2, x^2-5
31	$\mathbb{Q}(\sqrt{-31}, \sqrt[3]{\frac{3\sqrt{93}+29}{2}}+\sqrt[3]{\frac{-3\sqrt{93}+29}{2}})$	$x^3-3x-29$
32	$\mathbb{Q}(\sqrt{-32}, \sqrt{\sqrt{2}-1})$	x^4+2x^2-1
33	$\mathbb{Q}(\sqrt{-33}, \sqrt{3}, \sqrt{11})$	x^2-3, x^2-11
34	$\mathbb{Q}(\sqrt{-34}, \sqrt{\frac{\sqrt{17}-3}{2}})$	x^4-3x^2-2
36	$\mathbb{Q}(\sqrt{-36}, \sqrt{-3+2\sqrt{3}})$	x^4+6x^2-3
37	$\mathbb{Q}(\sqrt{-37}, \sqrt{37})$	x^2-37
38	$\mathbb{Q}(\sqrt{-38}, -\sqrt[3]{\sqrt{513}-\sqrt{512}}+\sqrt[3]{\sqrt{513}+\sqrt{512}})$	$x^6+6x^4+9x^2-2048$
39	$\mathbb{Q}(\sqrt{-39}, \sqrt{\frac{\sqrt{13}-1}{2}})$	x^4+x^2-3
40	$\mathbb{Q}(\sqrt{-40}, \sqrt{7+2\sqrt{10}})$	x^4-14x^2+9
41	$\mathbb{Q}(\sqrt{-41}, u)$	$x^8-90x^6-48x^4+10x^2-1$
42	$\mathbb{Q}(\sqrt{-42}, \sqrt{6}, \sqrt{14})$	x^2-6, x^2-14
43	$\mathbb{Q}(\sqrt{-45}, \sqrt{3}, \sqrt{5})$	x^2-3, x^2-5
46	$\mathbb{Q}(\sqrt{-46}, \sqrt{-3+4\sqrt{2}})$	x^4+6x^2-23
47	$\mathbb{Q}(\sqrt{-47}, z)$	$x^5-2x^4+2x^3-x^2+1$
48	$\mathbb{Q}(\sqrt{-48}, \sqrt{2}, \sqrt{3})$	x^2-2, x^2-3
49	$\mathbb{Q}(\sqrt{-49}, \sqrt{2\sqrt{7}})$	x^4-28
50	$\mathbb{Q}(\sqrt{-50}, \sqrt{5}, \sqrt[3]{35+15\sqrt{6}}-\sqrt[3]{-35+15\sqrt{6}})$	$x^2-5, x^3+15x-70$

Ako u tablici piše neko slovo, onda se odnosi na rješenje pripadnog polinoma zdesna koje je bilo preveliko za navesti. Primijetimo da nema jedinstveni način za zapisati takva polja - ipak smo se trudili staviti što jednostavnije generatore. Katkada je umjesto minimalnog polinoma bilo spretnije staviti dva polinoma čije nultočke zajedno generiraju polje prstena klasa (uz $\sqrt{-n}$). Do generatora smo dolazili eksplicitnim raspisom rješenja, i faktorizacijom. U nekim primjerima smo ad hoc metodama dodatno smanjili koeficijente. Možda je vrijedno spomenuti kako su se u svim primjerima pojavljivale domene jedinstvene faktorizacije (postoji mnoštvo realnih kvadratnih polja s brojem klasa 1). Alternativni načini računanja se mogu naći kod Schertza [9] i Lemmermeyera [10].

Uočimo nekoliko zanimljivih svojstava iz tablice. Katkada je grupa klasa izomorfna $(\mathbb{Z}/2\mathbb{Z})^n$ (npr. $n = 24$). Tada je moguće ustanoviti reprezentabilnost danom formom samo s Legenreovim simbolom tj. kongruencijama jer se pripadno polje prstena klasa može dobiti dodavanjem kvadratnih korijena nad $\mathbb{Q}$. Brojeva n s takvim svojstvom poznato je 65, i svih

65 je prvi pronašao Euler i nazvao ih *numeri idonei* (*prikladni brojevi*). 200 godina kasnije je dokazano da postoji najviše još jedan takav broj (te da je Eulerova lista ustvari potpuna uz pretpostavku generalizirane Riemannove hipoteze).

Činilo se možda da su 27 i 64 bili posebni kao potencije od 3 i 2 te da se zato radilo o kubnom i bikvadratnom reciprocitetu kod njih. Vidimo sada da to ipak nije izolirani fenomen. I za $n = 49$ je dovoljno promotriti bikvadratni reciprocitet od 28.

Primijetimo da se je dana polja moglo možda malo prirodnije napisati npr. $RCF(-42) = \mathbb{Q}(\sqrt{-42}, \sqrt{6}, \sqrt{14}) = \mathbb{Q}(\sqrt{-1}, \sqrt{-3}, \sqrt{-7})$. Zainteresirani čitatelj neka usporedi ovo s pojmom genus polja (vidi [1]). Vrijedi $RCF(-42) = RCF(-21)$ i slično. Primijetimo da imamo minus predznake ispod korijena kod prostih brojeva oblika $4k + 3$. To odgovora klasičnoj činjenici da je $\sqrt{\left(\frac{-1}{p}\right)p} \in \mathbb{Q}(\zeta_p)$. (Usporedi s Kronecker-Weber teoremom.)

Za kraj, napomenimo da bi se potpuno istom metodom mogla razmatrati i forma $x^2 + xy + ny^2$. Ustvari, rješenje je dano još kod Hilbertova polja klasa - razlog zašto smo morali uvoditi polje prstena klasa umjesto Hilbertova polja klasa je bio taj što nam Hilbertovo polje klasa za $n \equiv 3 \bmod 4$ ne bi dalo uvjet reprezentabilnosti za $x^2 + ny^2$ već upravo za $x^2 + xy + ny^2$.

Bibliografija

[1] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, John Wiley & Sons, 2011.

[2] André Weil, *Number Theory: An approach through history From Hammurapi to Legendre*, Springer Science & Business Media, 1987.

[3] Daniel A Marcus, *Number fields*, Springer, 1977.

[4] Gerald J Janusz, *Algebraic number fields*, American Mathematical Society, 1996.

[5] T Apostol, *Modular Functions and Dirichlet Series in Number Theory,*, Springer, New York, 1990.

[6] Harvey Cohn, *Introduction to the construction of class fields*, Courier Corporation, 1985.

[7] CF Gauss, *Disquisitiones Arithmeticae*, Leipzig Gerhard Fleischer, deutsche Übersetzung herausgegeben von H. Maser, 1889.

[8] Leonhard Euler, *Theoremata circa divisores numerorum in hac forma $pa^2 \pm qb^2$ contentorum*, Comm. Acad. Sci. Petersburg, 14(1744/46):151–181, 1751.

[9] Reinhard Schertz, *Weber's class invariants revisited,* J. Théor. Nombres Bordeaux, 14(1):325–343, 2002.

[10] Franz Lemmermeyer, *Class field towers,* `http://www.rzuser.uni-heidelberg.de/~hb3/publ/pcft.pdf`

Sažetak

U radu se promatra problem reprezentacije prostih brojeva formom x^2+ny^2. Nakon povijesnog uvoda koji upoznaje čitatelja s osnovama problema, prelazimo na tehnike apstraktne algebre, naročito teorije polja klasa te rješavamo problem u punoj općenitosti. Na kraju ilustriramo primjenu sa nekoliko računskih primjera.

Summary

In this work we treat the problem of representing prime numbers with the form $x^2 + ny^2$. After the historical introduction which introduces the reader with the basics, we switch to abstract algebra techniques, especially class field theory, and manage to solve the problem in full generality. In the end, we illustrate the applications with a few computational examples.

Životopis

Rođen sam 21. travnja 1993. u Bjelovaru. Pohađao sam III. osnovnu školu Bjelovar te Gimnaziju Bjelovar, prirodoslovno-matematički smjer. Sudjelovao sam na županijskim natjecanjima fizike, kemije, engleskog te državnim natjecanjima matematike i informatike.

Nakon srednjoškolskog obrazovanja upisujem studij matematike na zagrebačkom PMF-u, godina 2012/2013.. Preddiplomski studij sam završio s odličnim uspjehom te sam bio primatelj dvije stipendije zagrebačkog sveučilišta. Imao sam priliku biti demonstrator za kolegije: Matematička Analiza 1,2, Integralni Račun Funkcija Više Varijabli te Algebarske Strukture.

2015/2016. upisujem diplomski studij Teorijske Matematike. Na njemu sam položio 20 kolegija, ali ga nisam dovršio.

2017/2018. sam upisao diplomski studij Računarstvo i Matematika. 2018/2019. godinu sam pauzirao studij iz osobnih razloga. Sljedeće akademske godine sam nastavio te položio sve potrebne kolegije za polaganje diplomskog ispita.