Teorija polja klasa i teorija kompleksnog množenja

Filip Najman

Prirodoslovno matematički fakultet, Matematički odsjek
2017/2018

Sadržaj

Poglavlje 1

Uvod

Povijesno, Teorija polja klasa (Class Field Theory ili skraćeno CFT) je motivirana Kronecker-Weberovim teoremom.

Definicija. Kažemo da je polje K *polje algebarskih brojeva (PAB)* ako je konačno proširenje od $\mathbb{Q}$, tj. $[K : \mathbb{Q}]$ je konačno.

Definicija. Kažemo da je proširenje polja L/K *Abelovo* ako je Galoisovo i ako je $\mathrm{Gal}(L/K)$ Abelova grupa. Kažemo da je proširenje polja L/K *cikličko* ako je Galoisovo i ako je $\mathrm{Gal}(L/K)$ ciklička grupa.

Teorem 1 (Kronecker-Weber)**.** *Neka je $K/\mathbb{Q}$ konačno Abelovo proširenje. Tada postoji $n \in \mathbb{N}$ takav da je $K \subseteq \mathbb{Q}(\zeta_n)$.*

Napomena. Teorem je prvi iskazao Kronecker 1853., davši djelomičan dokaz. Weber je zatim 1886. objavio dokaz, za koji se ispostavilo (90 godina kasnije) da ima grešaka. Prvi potpuni dokaz dao je Hilbert 1896.

Hilbert je 1900. dao listu od 23. tada nerješena problema, koja je smatrao važnima.

Problem (Hilbertov 12. problem/Kroneckerov "Jugendtraum" (san iz mladosti))**.** Za zadano PAB K, opisati sva Abelova proširenja od K.

Problem je još uvijek neriješen, te je u potpunosti riješen samo za imaginarna kvadratna polja čiji je broj klasa 1; u tom slučaju problem rješava toerija kompleksnog množenja, kojom ćemo se baviti u drugom dijelu kolegija.

Tri razvoja događaja iz kraja 19. stoljeća su doveli do razvoja CFT - veze između Abelovih proširenja nekog polja i grupe klasa tog polja, teoremi o gustoći prostih ideala (i L-funkcije), te zakoni reciprociteta (generalizacije kvadratnog reciprociteta).

Naziv "polja klasa" se odnosi na određenja proširenja polja koja imaju određeneu vezu s grupom klasa nekog polja. Jedan od glavnih teorema CFT je da su ta polja klasa isto što i Abelova proširenja. Može nas zanimati i kako se faktoriziraju prosti ideali od K u Abelovim proširenjima od K. Odgovor na to pitanje nam daje Artinov reciprocitet.

Navedimo još jedan motivirajući problem za CFT. Jedan od osnovnih razloga zbog koji je algebarska teorija brojeva izmišljena je rješavanja Diofantskih jednadžbi. Neka je $f(x, y) = 0$, gdje je $f \in \mathbb{Z}[x, y]$ neka polinomijalna jednadžba, za koje želimo naći cijelobrojna ili racionalna rješenja. U ATB se često promatra ta jendnžba u prstenu cijelih nekog PAB K u kojemu se f (ili dio od f) faktorizira. Ako je $h_K = 1$ (tj. $\mathcal{O}_K$ je domena jedinstvene faktoizacije), tada to značajno pomaže u riješavanju problema. Npr. da bi našli rješenje jednadžbe $y^2 = x^3 - 1$, faktorizira se $y^2 + 1$ nad $\mathbb{Z}[i]$, te se pokaže da $y + i$ i $y - i$ moraju biti kubovi u $\mathbb{Z}[i]$.

Međutim, što ako $h_K > 1$? Tada ono što prvo pada na pamet je naći neko veće polje L, $L \subseteq K$, takvo da je $L \supseteq K$, te da je $h_L = 1$. Međutim, postoji li takvo polje L? To je pitanje dugo bilo neriješeno, te su tek 1960. Šafarevič i Golod dokazali da ne postoji za svako PAB K. Međutim, nama je za riješavanje ove jednadžbe dosta puno slabije svojstvo: dosta nam je da svi ideali od $\mathcal{O}_K$ postaju glavni u $\mathcal{O}_L$. Uvijek postoji PAB L koje ima ovo svojstvo, te će nam ova tvrdnja biti *Teorem o glavnim idealima*.

Poglavlje 2

Kratki podsjetnik iz algebarske teorije brojeva

U kolegiju pretpostavljamo dobro poznavanje ATBa, te da je poznato sve iz [1, 1.1. Number Fields].

Sada ćemo se ukratko podsjetiti nekih činjenica. Neka je K/F konačno proširenje PAB. Tada se prosti ideal $\mathfrak{p}$ od $\mathcal{O}_F$ prosti ideal faktorizira kao

$$\mathfrak{p}O_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

gdje su svi $\mathfrak{P}_i$-ovi različiti prosti ideali od $\mathcal{O}_K$. Prirodni brojevi e_i se zovu indexi grananja (ili stupnjevi grananja) od $\mathfrak{P}_i/\mathfrak{p}$. Ako je K/F Galoisovo, tada je $e_1 = \cdots e_r = e$. Polja $\mathcal{O}_K/\mathfrak{P}_i$ i $\mathcal{O}_F/\mathfrak{p}$ su konačna polja, koja se nazivaju *polja ostataka* od $\mathfrak{P}$ i $\mathfrak{p}$, te je $\mathcal{O}_F/\mathfrak{p}$ izomorfno potpolju od $\mathcal{O}_K/\mathfrak{P}_i$. Stupanj inercije $f_i = f(\mathfrak{P}_i/\mathfrak{p})$ je

$$f(\mathfrak{P}_i/\mathfrak{p}) = [O_K/\mathfrak{P}_i : O_F/\mathfrak{p}]\,.$$

Ako je K/F Galoisovo, tada je $f_1 = \cdots f_r = f$, te vrijedi $efr = [K : F]$.

Kažemo da je $\mathfrak{p}$ *nerazgranat* ako je $e_i = 1$ za $i = 1, \ldots, r$, te da je *potpuno razgranat* ako je $r = 1$ i $e_1 = [K : F]$. Kažemo da je $\mathfrak{p}$ *inertan* ako je $r = 1$ i ako je $e_1 = 1$ (ili ekvivalentno $f_1 = [K : F]$), te kažemo da se $\mathfrak{p}$ *potpuno cijepa* ako je $r = [K : F]$.

Neka je F polje algebarskih brojeva, te neka je K/F konačno Galoisovo proširenje od F stupnja n. Neka je $\mathfrak{p}$ fiksan prost ideal od $\mathcal{O}_F$ i neka je njegova faktorizacija u $\mathcal{O}_K$

$$\mathfrak{p}\mathcal{O}_K = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e,$$

gdje svi $\mathfrak{P}_i$-ovi imaju isti stupanj inercije f. Grupa $\mathrm{Gal}(K/F)$ djeluje na skup $\{\mathfrak{P}_1, \cdots, \mathfrak{P}_r\}$. To djelovanje je tranzitivno, tj. za svaki $\mathfrak{P}_i$ i $\mathfrak{P}_j$ postoji $\sigma \in \mathrm{Gal}(K/F)$ takav da je $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$.

Kada grupa djeluje na skup, tada se često promatra stabilizatorska podgrupa nekog elementa, tj. podgrupa elemenata u grupi koji trivijalno djeluje na taj element skupa.

Definicija. Uz notaciju kao i prije, definiramo *dekompozicijsku grupu* $D(\mathfrak{P}_i/\mathfrak{p})$ elementa $\mathfrak{P}_i$

$$D(\mathfrak{P}_i/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(K/F) \mid \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\} \leq \mathrm{Gal}(K/F).$$

Primjetimo sljedeće neka su $\mathfrak{P}_i$ i $\mathfrak{P}_j$ takvi da je $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Tada se lako provjeri da je

$$D(\mathfrak{P}_j/\mathfrak{p}) = \sigma D(\mathfrak{P}_i/\mathfrak{p})\sigma^{-1}.$$

Dakle sve dekompozicijske grupe su konjugirane. Pošto je $D(\mathfrak{P}_i)$ po definiciji stabilizatorska podgrupa elementa $\mathfrak{P}_i$, te je djelovanje grupe tranzitivno (tj. orbita od $\mathfrak{P}_i$ je duljine r), po teoremu o Orbiti i stabilizatoru da je

$$\#D(\mathfrak{P}_i/\mathfrak{p}) = n/r = ef.$$

Primjer 1. Promotrimo proširenje $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$; to je proširenje stupnja $\phi(15) = 8$, vrijedi $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q}) \simeq (\mathbb{Z}/15\mathbb{Z})^\times$. Elemente $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q})$ prikazujemo kao $\sigma_i(\zeta_{15}) = \zeta_{15}^i$, gdje je $i \in (\mathbb{Z}/15\mathbb{Z})^\times$. Također, vrijedi da je prsten cijelih brojeva u $\mathbb{Q}(\zeta_{15})$ jednak $\mathbb{Z}[\zeta_{15}]$.

Promotrimo faktorizaciju elemenata $2, 3, 5$ i 31 u $\mathbb{Z}(\zeta_{15})$. Neka su

$$\begin{aligned}
\mathfrak{p}_2 &= (2, \zeta_{15}^4 + \zeta_{15} + 1),\\
\mathfrak{p}_3 &= (3, \zeta_{15}^4 + \zeta_{15}^3 + \zeta_{15}^2 + \zeta_{15} + 1),\\
\mathfrak{p}_5 &= (5, \zeta_{15}^2 + \zeta_{15} + 1)\\
\mathfrak{p}_{31} &= (31, \zeta_{15} + 3)
\end{aligned}$$

Prikažimo u sljedećoj tablici vrijednosti r, e i f za navedene proste brojeve.

	r	e	f
$\mathfrak{p}_2$	2	1	4
$\mathfrak{p}_3$	1	2	4
$\mathfrak{p}_5$	1	4	2
$\mathfrak{p}_{31}$	8	1	1

Izračunajmo sada dekompozicijsku grupu svakog od ovih prostih elemenata. Očito je $D(\mathfrak{p}_3/3) = D(\mathfrak{p}_5/5) = \mathrm{Gal}(L/K)$, pošto su $\mathfrak{p}_3$ i $\mathfrak{p}_5$ jedini prosti brojevi iznad 3 i 5. Također, očito vrijedi $\#D(\mathfrak{p}_{31}/31) = n/r = 1$.

Dakle jedini zanimljivi slučaj je $D(\mathfrak{p}_2/2)$. To je grupa reda $ef = 4$. Promotrimo preslikavanje

$$\mathbb{Z}[\zeta_{15}] \to \mathbb{Z}[\zeta_{15}]/\mathfrak{p}_2 = \mathbb{F}_2[x]/(x^4 + x + 1),$$

koji šalje ζ_{15} u x. Vrijedi

$$\sigma_i((2, \zeta_{15}^4 + \zeta_{15} + 1)) = (2, \sigma(\zeta_{15}^4 + \zeta_{15} + 1)) = (2, \zeta_{15}^{4i} + \zeta_{15}^i + 1).$$

Zaključujemo da će σ biti u $D(\mathfrak{p}_2/2)$ ako i samo ako je $\zeta_{15}^{4i} + \zeta_{15}^{i} + 1$ u $\mathfrak{p}_2$, ili ekvivalentno, da x^4+x+1 dijeli $x^{4i}+x^i+1$ u $\mathbb{F}_2[x]$. Sada eksplicitnim računom možemo provjeriti da je

$$D(\mathfrak{p}_2/2) = \{\sigma_1, \sigma_2, \sigma_4, \sigma_8\}.$$

Dekompozicijska grupa nam je važna jer fiksira polje ostataka. Neka je $\mathfrak{P}$ prost broj iznad $\mathfrak{p}$, te neka je $\sigma \in D(\mathfrak{P}/\mathfrak{p})$. Pošto je $\sigma(\mathfrak{P}) = \mathfrak{P}$, slijedi da σ inducira automorfizam polja $\mathcal{O}_K/\mathfrak{P}$. Ovaj automorfizham svakako fiksira $\mathcal{O}_F/\mathfrak{p}$, te slijedi da smo dobili preslikavanje

$$D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}((\mathcal{O}_K/\mathfrak{P})/(\mathcal{O}_F/\mathfrak{p})), \tag{2.1}$$

koje lako provjerimo da je homomorfizam.

Definicija. *Inercijska grupa* $I(\mathfrak{P}/\mathfrak{p})$ je jezgra preslikavanja (2.1), tj.

$$I(\mathfrak{P}/\mathfrak{p}) = \ker\left(D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}((\mathcal{O}_K/\mathfrak{P})/(\mathcal{O}_F/\mathfrak{p}))\right).$$

Eksplicitnije, vrijedi da je

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in D(\mathfrak{P}/\mathfrak{p}) | \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \text{ za sve } \alpha \in \mathcal{O}_K\}.$$

Po definiciji inercijske grupe i prvom teoremu o izomorfizmu grupa, slijedi da je

$$D(\mathfrak{P}/\mathfrak{p})/I(\mathfrak{P}/\mathfrak{p}) \simeq \mathrm{Gal}((\mathcal{O}_K/\mathfrak{P})/(\mathcal{O}_F/\mathfrak{p})).$$

Kao i za dekompozicijske grupe, inercijske grupe konjugiranih prostih idela su međusobno konjugirane, te se lako vidie da je $\#I(\mathfrak{P}/\mathfrak{p}) = e$. Drugim riječima, inercijska grupa $I(\mathfrak{P}/\mathfrak{p})$ je trivijalna ako i samo ako je $\mathfrak{P}/\mathfrak{p}$ nerazgranat.

Primjer 2. Izračunajmo inercijske grupe iz prethodnog primjera. Očito su $I(\mathfrak{p}_2/2)$ i $I(\mathfrak{p}_{31}/31)$ trivijalne. Grupa $I(\mathfrak{p}_3/3)$ je reda 2. Promotrimo preslikavanje

$$\mathbb{Z}[\zeta_{15}]/\mathfrak{p}_3 \simeq \mathbb{F}_3[x]/(x^4+x^3+x^2+x+1).$$

Element σ_i iz $D(\mathfrak{p}_3/3)$ će biti u $I(\mathfrak{p}_3/3)$ ako i samo ako je $\sigma_i(\zeta_{15}) = \zeta_{15}$ pošto je očito $\sigma_i(1) = 1$, a 1 i ζ_{15} su generatori od $\mathbb{Z}[\zeta_{15}]$, pa time i $\mathbb{Z}[\zeta_{15}]/\mathfrak{p}_3$. To je ekvivalentno tome da je

$$\sigma_i(x) = x^i \equiv x \pmod{x^4+x^3+x^2+x+1}$$

u $\mathbb{F}_3[x]$. Drugim rječima, pitamo se kada $x^4+x^3+x^2+x+1$ dijeli $x^i - x$. Vidimo da je to istina za $i = 11$, te onda pošto je $I(\mathfrak{p}_3/3)$ grupa reda 2, zaključujemo da je

$$I(\mathfrak{p}_3/3) = \{\sigma_1, \sigma_{11}\}.$$

Analogno možemo izračunati

$$I(\mathfrak{p}_5/5) = \{\sigma_1, \sigma_4, \sigma_7, \sigma_{13}\}.$$

Definicija. Pretpostavimo da je $\mathrm{Gal}(K/F)$ Abelova. Definiramo *inercijsko polje* K^I od $\mathfrak{P}/\mathfrak{p}$ kao fiksno polje od $I(\mathfrak{P}/\mathfrak{p})$, te *dekompozicijsko polje* K^D od $\mathfrak{P}/\mathfrak{p}$ kao fiksno polje od $D(\mathfrak{P}/\mathfrak{p})$.

Teorem 2 (Teorem o slojevima)**.** *Neka je $\mathfrak{p}$ netrivijalni ideal od $\mathcal{O}_F$, gdje je K/F Abelovo proširenje. Tada se $\mathfrak{p}$ poptuno cijepa u K^D, te ideali iznad $\mathfrak{p}$ ostaju inertni u K^I/K^D, te se potpuno granaju u K/K^D.*

Poglavlje 3

p-adski brojevi

3.1 Inverzni limes

Definicija. *Inverzni sistem* je niz objekata (npr. skupova/grupa/prstena) (A_n) skupa sa nizom morfizmama (npr. funkcija/homomorfizama) (f_n)

$$\cdots \to A_{n+1} \xrightarrow{f_n} A_n \to \cdots \xrightarrow{f_2} A_2 \xrightarrow{f_1} A_1.$$

Definicija. *Inverzni limes* $A = \varprojlim A_n$ inverznog sistema skupova (A_n), (f_n) definiranog kao gore je skup A čiji elementi su besklonačni nizovi (a_n), gdje je $a_n \in A_n$ za svaki $n \geq 0$, te koji zadovoljavaju $f_n(a_{n+1}) = a_n$ za svaki $n \geq 0$.

Napomena. Ako su A_n grupe i f_n su homomorfizmi grupa, tada je inverzni limes također grupa. Ako su A_n prsteni i f_n homomorfizmi prstenova, tada je A_n prsten.

3.2 Prsten cijelih p-adskih brojeva

Definicija. Neka je p fiksan prost broj. *Prsten cijelih p-adskih brojeva* $\mathbb{Z}_p$ je inverzni limes

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

inverznog sistema prstenova $(\mathbb{Z}/p^n\mathbb{Z})$ s homomorfizmima prstenova (f_n), gdje je f_n redukcija modulo p^n.

Napomena. Multiplikativna jedinica u prstenu je $1 = (\overline{1}, \overline{1}, \ldots)$, gdje je n-ta $\overline{1}$ označava $1 + p^n\mathbb{Z}$. Preslikavanje koje šalje $x \in \mathbb{Z}$ u $(\overline{x}, \overline{x}, \ldots)$, je homomorfizam prstenova koji očito ima trivijalnu jezgru. Dakle vidimo da se $\mathbb{Z}$ ulaže u $\mathbb{Z}_p$, pa vidimo da $\mathbb{Z}_p$ ima karakteristiku 0, te možemo smatrati $\mathbb{Z}$ potprstenom od $\mathbb{Z}_p$. Međutim, prsten $\mathbb{Z}_p$ je puno veći od $\mathbb{Z}$.

Elemente prstena $\mathbb{Z}_p$ ćemo neformalno pisati kao nizove $(a_1, a_2, \ldots)$, gdje cijeli broj $a_i \in [0, p^i - 1]$ reprezntira $1 + p^i\mathbb{Z}$.

Primjer 3. U $\mathbb{Z}_7$ imamo

$$\begin{aligned}
2 &= (2, 2, 2, 2, 2 \ldots), \\
2002 &= (0, 42, 287, 2002, 2002, \ldots), \\
-2 &= (5, 47, 341, 23999, 16805, \ldots), \\
\frac{1}{2} &= (4, 25, 172, 1201, 8304, \ldots), \\
\sqrt{2} &= \begin{cases} (3, 10, 108, 2166, 4567, \ldots) \\ (4, 39, 235, 235, 12240, \ldots) \end{cases} \\
\sqrt[5]{2} &= (4, 46, 95, 1124, 15530, \ldots)
\end{aligned}$$

Zadatak 1. Dokažite da postoji $\sqrt[p]{2}$ u $\mathbb{Z}_7$ za svaki $p > 7$.

Definicija. Sjetimo se da je niz homomorfizama grupa *egzaktan* ako je za svaku grupu u nizu slika ulaznog homomorfizma jednaka jezgri izlaznog homomorfizma. Za *kratki egzaktan niz*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0,$$

to znači da je f injektivan, g surjektivan, te da je $\operatorname{im} f = \ker g$. Po prvom teoremu o izomorfizmu grupa, također vrijedi $B/\operatorname{im} f \simeq C$.

Propozicija 3. *Za svaki cijeli broj m, niz*

$$0 \to \mathbb{Z}_p \xrightarrow{[p^m]} \mathbb{Z}_p \xrightarrow{\pi_m} \mathbb{Z}/p^m\mathbb{Z} \to 0$$

je egzaktan, gdje je $[p^m]$ množenje s p^m, te je π_m projekcija na $\mathbb{Z}/p^m\mathbb{Z}$, tj. preslikavanje koje šalje niz (a_n) u a_m.

Dokaz. Dokažimo prvo da je množenje s p u $\mathbb{Z}_p$ injektivno. Pretpostavimo suprotno, tj. da je $a = (a_n)$ u jezgri. Tada je $pa = 0$, pa je $pa_n = 0$ za svaki n. Posebno, $pa_{n+1} = 0$ u $\mathbb{Z}/p^{n+1}\mathbb{Z}$. To sada znači da je $a_{n+1} = p^n y_{n+1}$ u $\mathbb{Z}/p^{n+1}\mathbb{Z}$ za neki $y_{n+1} \in \mathbb{Z}/p^{n+1}\mathbb{Z}$. Sada slijedi da je $a_n = f(a_{n+1}) = p^n f(y_{n+1}) = 0$ u $\mathbb{Z}/p^n\mathbb{Z}$. Kako ovo vrijedi za sve n, slijedi $a = 0$.

Egzaktnost s lijeva: Pošto je množenje s p injektivno, vrijedi da je kompozicija tog preslikavanja sa samim sobom m puta (tj. množenje s p^m) injektivno.

Egzaktnost s desna: Zapišimo $\beta \in \mathbb{Z}/p^m\mathbb{Z}$ kao $b + p^m\mathbb{Z}$. Tada će π_m preslikati element $(b, b, b, b, \ldots)$ u β.

Egzaktnost u sredini: Ako je $a \in \mathbb{Z}_p$, tada je $\pi_m(p^m a) = p^m \pi_m(a) = 0$ u $\mathbb{Z}/p^m\mathbb{Z}$. Dakle slika ulaznog preslikavanja je u jezgri izlaznog preslikavanja. Dokažimo suprotnu inkluziju. Neka je $a = (a_n)$ u jezgri od π_m. Dakle vrijedi da je $a_m = 0$. Dakle za svaki $n \geq m$, imamo $a_n \in p^m\mathbb{Z}/p^n\mathbb{Z}$. Dakle postoji jedinstveni b_{n-m} koji se preslikava u a_n pod djelovanjem izomorfizma

$$\mathbb{Z}/p^{n-m}\mathbb{Z} \xrightarrow{p^m} p^m\mathbb{Z}/p^n\mathbb{Z}.$$

Niz tih b_{n-m}-ova je kompatibilan, pošto su a_n-ovi kompatibilni, te postoji element $b = (b_n)$ takav da je $p^m b = a$, dakle a je u slici od množenja s p^m.

□

Korolar 4. *Za svaki prirodan broj m vrijedi $\mathbb{Z}_p/p^m\mathbb{Z}_p \simeq \mathbb{Z}/p^m\mathbb{Z}$.*

Propozicija 5. *Element $x \in \mathbb{Z}_p$ je invertibilan ako i samo ako $x \notin p\mathbb{Z}_p$. Drugim riječima, $\mathbb{Z}_p^\times$ je $\mathbb{Z}_p \backslash p\mathbb{Z}_p$.*

Dokaz. Ako je $a = (a_n) \in \mathbb{Z}_p$ djeljiv s p, tada je $a_1 = 0$, pa a očito ne može biti invertibilan. Ako a nije djeljiv s p tada za svaki n vrijedi $a_n = b_n + p^n\mathbb{Z}$ za neki $b_n \in \mathbb{Z}$, te taj b_n nije djeljiv s p. Slijedi da a_n ima inverz c_n u $\mathbb{Z}/p^n\mathbb{Z}$ Također, niz (c_n) mora biti kompatibilan, te je $c = (c_n)$ inverz od a. □

Propozicija 6. *Svaki elemnt $x \in \mathbb{Z}_p$ se može na jedinstven način zapisati kao $p^n u$, gdje je $u \in \mathbb{Z}_p^\times$.*

Dokaz. Postojanje zapisa: Ako je $0 \neq a = (a_n)$, tada postoji najveći n takav da je $a_n = 0$. Za taj n, po Propoziciji 3 vrijedi $a = p^n u$ za neki $u \in \mathbb{Z}_p$. Štoviše, u ne može biti djeljiv s p, pošto bi tada bilo $u_{n+1} = 0$, pa je po prethodnoj propoziciji u invertibilan.

Jedinstvenost zapisa: Pretpostavimo $p^n u_1 = p^m u_2$. Ako je $m = n$, tada zbog injektivnosti množenja s p^m imamo $u_1 = u_2$. U suprotnom možemo BSO pretpostaviti da je $n > m$. Tada je $u_2 = p^{n-m}u_2$ invertibilan, što je kontradikcija s prethodnom propozicijom. □

Korolar 7. *Prsten $\mathbb{Z}_p$ je integralna domena.*

Dokaz. Množenjem dva ne-nul elementa $p^n u_1$ i $p_m u_2$ dobivamo $p^{n+m}u_1u_2$, čija je $(n+m+1)$-ta komponenta različita od nule. □

Definicija. Neka je $a = (a_n) \in \mathbb{Z}_p$, gdje je po običaju a_n cijeli broj iz $[0, p^n - 1]$. Niz $(b_0, b_1, \ldots)$ za kojeg vrijedi $b_0 = a_1$ i $b_n = (a_{n+1} - a_n)/p^n$ se zove p-adska ekspanzija od a.

Dakle svaki $a \in \mathbb{Z}_p$ se može zapisati kao formalni red

$$a = \sum_{i=0}^{\infty} b_i p^i.$$

Iz defincije odmah slijedi:

Propozicija 8. *Svaki element u $\mathbb{Z}_p$ ima jedinstvenu p-adsku ekspanziju i svaki niz $(b_0, b_1, \ldots)$, gdje je $b_i \in [0, p-1]$ je p-adska ekspanzija nekog elementa iz $\mathbb{Z}_p$.*

Dakle postoji bijekcija između $\mathbb{Z}_p$ i nizova cijelih brojeva s elementima iz $[0, p-1]$.

Definicija. Za svaki $0 \neq a \in \mathbb{Z}_p$, *p-adska valuacija* od a, s oznakom $v_p(a)$ je najveći cijeli broj m za koji je a u $p^m\mathbb{Z}_p$. Ekvivalentno $v_p(a)$ je za $a = \sum_{i=0}^{\infty} b_i p^i$ najmanji prirodan broj m takav da je $b_m \neq 0$. Također ekivivalentno, ako zapišemo $a = p^m u$, gdje je $u \in \mathbb{Z}_p^\times$ tada je $v_p(a) = m$. Definiramo $v_p(0) = +\infty$.

Propozicija 9. *Svaki ne-nul ideal u $\mathbb{Z}_p$ je oblika (p^m) za neki prirodan broj m.*

Dokaz. Neka je I ne-nul ideal u $\mathbb{Z}_p$ i neka je $m = inf\{v_p(a) : a \in I\}$. Pošto je $I \neq (0)$, tada je $m < \infty$, te za svaki $a \in I$ vrijedi $a \in p^m\mathbb{Z}_p = (p^m)$. S druge strane, postoji $a \in I$ takav da je $a = p^m u$. Slijedi da je $u^{-1}a = p^m \in I$, iz čega slijedi da je $(p^m) \subset I$. □

Korolar 10. *Prsten $\mathbb{Z}_p$ je domena glavnih ideala (a time i prsten jedinstvene faktorizacije) s jedinstvenim prostim idealom (p) (te jednim prostim elementom p).*

Propozicija 11. *Uz konvenciju da je $n + \infty = \infty$ za svaki cijeli broj n, p-adska valuacija zadovoljava sljedeća svojstva:*

1. $v_p(a) = \infty$ *ako i samo ako je* $a = 0$.
2. $v_p(ab) = v_p(a) + v_p(b)$.
3. $v_p(a + b) \geq \min(v_p(a), v_p(b))$.

Dokaz. Prvo svojstvo slijedi iz definicije. Drugo i treće svojstvo su očito zadovoljena ako su a ili b jednaki 0. Pretpostavimo $a, b \neq 0$. Neka je $v_p(a) = m$ i $v_p(b) = n$.

Da bi dokazali drugu tvrdnju zapišimo $a = p^m u_1$ i $b = p^n u_2$, gdje su $u_1, u_2 \in \mathbb{Z}_p^\times$. Tada je $ab = p^{m+n} u_1 u_2$, pa je $v_p(ab) = m + n$.

U trećoj tvrdnji možemo BSO pretpostaviti da je $m \leq n$. Slijedi da je $p^n\mathbb{Z}_p \subseteq p^m\mathbb{Z}_p$, pa su i $a, b \in p^m\mathbb{Z}_p$, iz čega slijedi da je $a + b \in p^m\mathbb{Z}_p$, te je $v_p(a + b) \geq \min(v_p(a), v_p(b))$.

□

p-adska valuacija je primjer *diskretne valuacije.*

Definicija. Neka je R komutativni prsten. *Diskretna valuacija* (na R) je funkcija $v : R \to \mathbb{Z} \cup \{\infty\}$ koja zadovoljava svojstva iz propozicije 11.

Definicija. *Prsten diskretne valuacije* je domena glavnih ideala koja sadrži jedinstveni maksimalan ideal, te nije polje.

Možda je ova definicija na prvi pogled neobična, pošto se ne spominje valuacija, međutim za svaki prsten diskretne valuacije se može na analogan način definirati diskretna valuacija.

Prsten diskretne valuacije je "najbliže" što komutativni prsten može biti polje, a bez da zaista je polje.

3.3 Polje p-adskih brojeva

Sjetimo da se polje razlomaka nekog prstena R definira kao skup uređenih parova $(a, b) \in R^2$, koji se obično zapisuje kao a/b gdje vrijedi da je $a/b \sim c/d$ kad god je $ad = bc$.

Definicija. *Polje p-adskih brojeva* $\mathbb{Q}_p$ je polje razlomaka od $\mathbb{Z}_p$.

Pošto je $a \in \mathbb{Q}_p$ po definiciji $a = (p^m u_1)/(p^n u_2) = p^{m-n} u_1 u_2^{-1}$, možemo svaki element iz $\mathbb{Q}_p$ zapisati kao up^k za $u \in \mathbb{Z}_p^\times,\ k \in \mathbb{Z}$. Sada možemo proširiti definiciju od v_p na $\mathbb{Q}_p$ tako da za $a = up^k$, $u \in \mathbb{Z}_p^\times,\ k \in \mathbb{Z}$ vrijedi $v_p(up^k) = k$, te je kao i prije $v_p(0) := +\infty$.

Napomena. Primjetimo da sada možemo $\mathbb{Z}_p$ identificirati kao podskup od $\mathbb{Q}_p$ sa elementima ne-negativne valuacije, te $\mathbb{Z}_p^\times$ možemo definirati kao podskup $\mathbb{Q}_p$ elemenata s valuacijom 0.

Vrijedi $\mathbb{Q} \subset \mathbb{Q}_p$, te vrijedi za svaki $x \in \mathbb{Q}_p$ je ili $x \in \mathbb{Z}_p$ ili je $x^{-1} \in \mathbb{Z}_p$.

Ovo je jedan od dva načina definiranja polja $\mathbb{Q}_p$. Promotrimo sada drugi način, preko apsolutnih vrijednosti.

3.4 Apsolutne vrijednosti

Definicija. Neka je k polje. *Apsolutna vrijednost* na k je funkcija $\|\| : k \to \mathbb{R}_{\geq 0}$ sa sljedećim svojstvima:

(1) $\|x\| = 0$ ako i samo ako je $x = 0$,

(2) $\|xy\| = \|x\| \cdot \|y\|$.

(3) $\|x + y\| \leq \|x\| + \|y\|$.

Absloutne vrijednosti se nekada nazivaju i "norme", ali mi 'cemo koristiti izraz norme za nešto drugo, te ćemo koristiti naziv "apsolutna vrijednost" kako bi izbjegli zabunu.

Neke norme zadovoljavaju jače svojstvno

(3') $\|x + y\| \leq \max\{\|x\|, \|y\|\}$.

se zovu *nearhimedske* apsolutne vrijednosti, a one koje ne zadovoljavaju se zovu *arhimedske.*

Definicija. Definiramo p-adsku apsolutnu vrijednost $|\ |_p$ na $\mathbb{Q}_p$ s

$$|x|_p = p^{-v_p(x)}.$$

Napomena. Primjetimo da pošto je $\mathbb{Q} \subset \mathbb{Q}_p$, ovo daje definiciju apsolutne vrijednosti $|\ |_p$ na $\mathbb{Q}$. Spomenuti alternativni način definicije od $\mathbb{Q}_p$ je da definiramo $\mathbb{Q}_p$ kao upotpunjenje od $\mathbb{Q}$ (tj. $\mathbb{Q}$ skupa s svim limesima nizova iz $\mathbb{Q}$) s obzirom na apsolutnu vrijednost $|\ |_p$. Dosta knjiga definira $\mathbb{Q}_p$ upravo na ovaj način. Tada se $\mathbb{Z}_p$ definira kao

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\},$$

ili kao upotpunjenje od $\mathbb{Z}$ s obzirom na $|\ |_p$.

Napomena. Naziv *prsten cijelih brojeva* u $\mathbb{Q}_p$ može biti zbunjujuć. Naime, $\mathbb{Z}_p$ *nije* integralno zatvorenje od $\mathbb{Z}$ u $\mathbb{Q}_p$. To možemo vidjeti promatranjem karidnaliteta tih skupova. Integralno zatvorenje od $\mathbb{Z}$ u $\mathbb{Q}_p$ je prebrojiv skup, (pošto postoj prebrojivo mnogo polinoma s cjelobrojnim koeficijentima) dok je $\mathbb{Z}_p$ očito neprebrojiv skup. Međutim, istina je da je $\mathbb{Z}_p$ integralno zatvoren u $\mathbb{Q}_p$, te $\mathbb{Z}_p$ sadrži integralno zatvorenje od $\mathbb{Z}$ u $\mathbb{Q}$.

Definicija. Dvije apsolutne vrijednosti $\|\ \|$ i $\|\ \|'$ na polju k su ekvivalentne ako postoji $\alpha \in \mathbb{R}$ takav da je

$$\|x\|' = \|x\|^\alpha$$

za svaki $x \in k$.

Sljedeći teorem, koji nećemo dokazivati, nam govori koje su sve apsolutne vrijednosti, do na ekvivalenciju, na $\mathbb{Q}$. Označimo s $|\ |_\infty$ uobičajenu apsolutnu vrijednost.

Općenito u p-adskoj apsolutnoj vriejdnosti, "mali" su brojevi koji su djeljivi velikim potencijama broja p.

Teorem 12 (Ostrowski)**.** *Svaka ne-trivijalna apsolutna vrijednost na $\mathbb{Q}$ je ekvivalentna s $|\ |_p$ za neki prost broj p ili $|\ |_\infty$.*

Na $\mathbb{Z}_p$ i $\mathbb{Q}_p$ se može definirati *p-adska topologija* preko apsolutne vrijednosti. U p-adskim brojevima su $a, b \in \mathbb{Q}$, promatrani kao elementi od $\mathbb{Q}_p$ "blizu", ako je u brojniku od $a - b$ velika potencija od p. Na primjer niz brojeva (2^n) konvergira u 0 u $\mathbb{Z}_2$.

p-adska analiza nam je često vrlo korisna, međutim trebamo biti vrlo pažljivi s intuicijom kada radimo s p-adskim brojevima.

Primjer 4. Neka su $b, c \in \mathbb{Q}$, te neka je p prost broj. Tada postoji niz racionalnih brojeva a_i koji konvergira u b s obzirom na standardnu normu, te konvergira u c s obzirom na p-adsku normu. Dokažimo ovu tvrdnju. Neka je

$$d_n = \frac{p^n}{p^n + 1} \quad e_n = \frac{1}{p^n + 1}.$$

U standardnoj normi d_n konvergira u 1, a e_n konvergira u 0, dok u p-adskoj normi d_n konvergira u 0, a $e_n = 1 - \frac{p^n}{p^n+1}$ kovergira u 1. Dakle vidimo da će niz $(a_n) = (bd_n + ce_n)$ konvergirati u b s obzirom na standardnu normu, te u c s obzirom na p-adsku.

Prikažimo sada jednu primjenu p-adskih brojeva i jednostavne p-adske analize.

Primjer 5. Promtrimo razvoj ;

$$(1+t)^{\frac{1}{6}} = 1 + \frac{1}{6}t - \frac{5}{2^2 3^2}t^2 + \frac{55}{2^4 3^4}t^3 - \frac{935}{2^7 3^5}t^4 + \dots .$$

Vidimo da se u nazivnicima nalaze samo potencije od 2 i 3, tj. prostih djelitelja od 6. Tvrdimo da, za $a \in \mathbb{Q}$, $k \in \mathbb{N}$, se u nazivniku od

$$\binom{a}{k} = \frac{a(a-1)(a-2)\dots(a-k+1)}{k!}$$

nalaze samo potencije prostih projeva koje dijele nazivnik od a.

Dokažimo tvrdnju obratom po kontrapoziciji: ako p ne dijeli nazivnik od a, tada p ne dijeli nazivnik od $\binom{a}{k}$. Pošto a nema faktore od p u nazivniku, tada je $a \in \mathbb{Z}_p$. Dakle, zaključujemo da je $a = (a_n)$ limes niza (b_n), gdje je $b_n \in \mathbb{Z}$, npr. uzmimo da je b_i i-ti član p-adske ekspanzije $b_i = \sum_{k=0}^{i} a_k p^k$. Općenitije $\mathbb{Z}_p$ je upotpunjenje od $\mathbb{Z}$ s obzirom na p-adsku normu, pa ova tvrdnja vrijedi za svaki $r \in \mathbb{Z}_p$.

S druge strane, polinomijalna funkcija $x \mapsto \binom{x}{k} \in \mathbb{Q}[x]$ je neprekidna u p-adskoj metrici, pa zbog $a = \lim_{i\to\infty} b_i$, imamo

$$\binom{a}{k} = \lim_{i\to\infty} \binom{b_i}{k}.$$

Pošto je $b_i \in \mathbb{Z}$, slijedi da je $\binom{b_i}{k} \in \mathbb{Z}$. Pošto je $\binom{a}{k}$ limes elemenata iz $\mathbb{Z}$, slijedi da je $\binom{a}{k} \in \mathbb{Z}_p$, tj. p ne dijeli nazivnik od $\binom{a}{k}$.

3.5 Rješenja polinomijalnih jednadžbi

Lema 13. *Neka je (S_n) inverzni sistem konačnih nepraznih skupova s kompatibilnim preslikavanjem $f_n : S_{n+1} \to S_n$. Tada je $\varprojlim S_n$ neprazan.*

Dokaz. Ako su svi f_n surjektivni, tada lako konstuiramo element (s_n): izaberemo bilo koji $s_1 \in S_1$, te za $n \geq 1$ izaberemo $s_{n+1} \in f_n^{-1}(s_n)$. sada nam je cilj opći slučaj reducirati na ovaj.

Neka je $T_{n,n} = S_n$ i za $m > n$ neka je $T_{m,n}$ slika od S_m u S_n, tj.

$$T_{m,n} = f_n(f_{n+1}(\cdots f_{m-1}(S_m)\cdots)).$$

Tada za svaki n imamo niz inkluzija

$$\cdots, \subseteq T_{m,n} \subseteq T_{m-1,n} \subseteq \cdots T_{n,n} \subseteq S_n.$$

Svaki $T_{m,n}$ je končan neprazan skup, pa slijedi da je za sve osim konačno mnogo inkluzija, ta inkluzija zapravo jednakost. Dakle za svaki n, je $E_n = \cap_m T_{m,n}$ neprazan podskup od S_n. Restringirajući prselikavanje f_n tako da definira preslikavanje $E_{n+1} \to E_n$ dobivamo inverzni sistem (E_n) nepraznih skupova takvih da su sva preslikavanja surjekcija, kao što smo i htjeli. $\square$

Propozicija 14. *Neka je $f \in \mathbb{Z}_p[x]$. Tada su sljedeće tvrdnje ekvivalentne:*

(1) Jednadžba $f(x) = 0$ ima rješenja u $\mathbb{Z}_p$.

(2) Jednadžba $f(x) = 0$ ima rješenja u $\mathbb{Z}/p^n\mathbb{Z}$ za svaki $n \in \mathbb{N}$

Dokaz. Neka je S_n skup rješenja u $\mathbb{Z}/p^n\mathbb{Z}$. Tada je $\varprojlim S_n \subseteq \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$ skup rješenja u $\mathbb{Z}_p$. Sada imamo $\varprojlim S_n \neq \emptyset$ ako i samo ako su svi S_n neprazni po Lemi 13. $\square$

Henselova lema će nam reći da je nešto što je "blizu" rješenja polinomijalne jednadžbe može "popraviti" do egzaktnog rješenja.

Teorem 15 (Henselova lema)**.** *Neka je $f_p \in \mathbb{Z}_p[x]$. Pretpostavimo da je $f(a) \equiv 0 \pmod p$ i $f'(a) \not\equiv 0 \pmod p$. Tada postoji jedinstveni $b \in \mathbb{Z}_p$, $b \equiv a \pmod b$ takav da je $f(b) = 0$.*

Dokaz. Neka $a_1 = a$ i definiramo za $n \geq 1$

$$a_{n+1} = a_n - f(a_n)/f'(a_n).$$

Dokazujemo indukcijom da za svaki $n \geq 1$ vrijedi

$$f'(a_n) \not\equiv 0 \pmod p, \tag{3.1}$$

$$f(a_n) \equiv 0 \pmod{p^n}. \tag{3.2}$$

Primjetimo da (3.1) osigurava da je $f'(a_n) \in \mathbb{Z}_p^\times$, pa je a_{n+1} dobro definiran element iz $\mathbb{Z}_p$. Definicija od a_{n+1} skupa s (3.1) i (3.2) osiguravaju da je $a_{n+1} \equiv a_n \pmod{p^n}$, što znači da niz ($a_n \mod p^n$) definira element $b \in \mathbb{Z}_p$ za koji vrijedi $f(b) = 0$ i $b \equiv a_1 \equiv a \pmod p$.

Za $n = 1$ tvrdnja očito vrijedi, pa pretpostavimo da (3.1) i (3.2) vrijede za a_n. Tada $a_{n+1} \equiv a_n \pmod{p^n}$, pa je $f'(a_{n+1}) \equiv f'(a_n) \not\equiv 0 \pmod p$. Dakle (3.1) je zadovoljen za sve $n \in \mathbb{N}$. Da bi pokazali (3.2), napravimo Taylorov razvoj od f oko a_n:

$$f(x) = f(a_n) + f'(a_n)(x - a_n) + (x - a_n)^2 g(x),$$

za neki $g(x) \in \mathbb{Z}_p[x]$. Uvrštavajući $x = a_{n+1}$, dobivamo

$$f(a_{n+1}) = f(a_n) + f'(a_n)(a_{n+1} - a_n) + (a_{n+1} - a_n)^2 g(a_n + 1).$$

Iz definicije a_{n+1} imamo $f'(a_n)(a_{n+1} - a_n) = -f(a_n)$, pa je

$$f(a_{n+1}) = (a_{n+1} - a_n)^2 g(a_{n+1}).$$

Pošto je $a_{n+1} \equiv a_n \pmod{p^n}$, slijedi da je $f(a_{n+1}) \equiv 0 \pmod{p^{n+1}}$, pa (3.2) vrijedi za a_{n+1}.

Pošto $f(x) = 0$ ima jedinstveno rješenje u $\mathbb{Z}/p^n\mathbb{Z}$ konguentno s a modulo p (jer (3.1) povlači da je $f'(a_n) \not\equiv 0 \pmod{p^n}$), pa je a_n jednostruka nul-točka od $f \pmod p)^n$.), slijedi da niz (a_n) definira jedinstveno rješenje u $\mathbb{Z}_p$. $\square$

3.6 Stuktura od $\mathbb{Z}_p^\times$

Restrikcija projekcije $\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ na $\mathbb{Z}_p^\times$ definira surjektivni homomorfizam

$$\mathbb{Z}_p^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Jezgra ovog preslikavanja je $U_n := 1 + p^n\mathbb{Z}_p$. Dakle vrijedi

$$\mathbb{Z}_p^\times / U_n \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times,$$

pa je

$$\mathbb{Z}_p^\times \simeq \varprojlim(\mathbb{Z}_p^\times / U_n) \simeq \varprojlim(\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Primjetimo da je (U_n) padajući niz podgrupa od $\mathbb{Z}_p^\times$:

$$\cdots \subset U_3 \subset U_2 \subset U_1 \subset \mathbb{Z}_p^\times.$$

Lema 16. *Vrijedi:*

(1) $\mathbb{Z}_p^\times / U_1 \simeq (\mathbb{Z}/p\mathbb{Z})^\times$.

(2) $U_n / U_{n+1} \simeq \mathbb{Z}/p\mathbb{Z}$.

Dokaz. Prvu tvrdnju smo već dokazali. Za drugu, promotrimo preslikavanje

$$U_n \to \mathbb{Z}/p\mathbb{Z},$$
$$1 + p^n z \mapsto (z \bmod p).$$

To preslikavanje je surjekcija, te je jezgra U_{n+1}. □

Korolar 17. *Grupa U_1/U_n ima p^{n-1} elemenata.*

Propozicija 18. *Neka je μ_{p-1} skup rješenja jednadžbe $x^{p-1} = 1$ u $\mathbb{Z}_p^\times$. Tada je μ_{p-1} s opercaijom množenja grupa izomorfna s $(\mathbb{Z}/p\mathbb{Z})^\times$, te je $\mathbb{Z}_p^\times = U_1 \times \mu_{p-1}$.*

Dokaz. Skup μ_{p-1} je jezgra homomorfizam potenciranja na $(p-1)$-vu potenciju sa $\mathbb{Z}_p^\times$ u $\mathbb{Z}_p^\times$, pa je grupa. Neka je $f(x) = x^{p-1} - 1$. Po Malom Fermatovom teoremu, svaki element $\neq 0$ iz $\mathbb{Z}/p\mathbb{Z}$ je korijen ovog polinoma, te vrijedi $f'(x) \not\equiv 0 \pmod p$ za sve $x \in \{1, 2, \ldots, p-1\}$. Sada po Henselovoj lemi, za svaki $x \in \{1, 2, \ldots, p-1\}$ postoji jedinstveni $a \in \mathbb{Z}_p$ takav da je $f(a) = 0$. Također, ne postoji element is μ_{p-1} koji je kongruentan 0 modulo p. Slijedi da je redukcija modulo p izomorfizam $\mu_{p-1} \to (\mathbb{Z}/p\mathbb{Z})^\times$.

Primjetimo sada da je $U_1 \cap \mu_{p-1} = \{1\}$, pošto je 1 očito rješenje, a po Henselovoj lemi, rješenje kongruentno 1 mod p je jedinstveno. Također, vrijedi da je $U_1 \cdot \mu_{p-1} = \mathbb{Z}_p^\times$, pošto se bilo koji element $a \in \mathbb{Z}_p^\times$ može podijeliti s elementom iz μ_{p-1} koji je kongruentan s a modulo p da bi dobio element iz U_1. Slijedi da je direktan produkt $U_1 \times \mu_{p-1}$ izomorfan $\mathbb{Z}_p^\times$. □

Lema 19. *Neka je p prost broj. Ako je $p \neq 2$, neka je $n \geq 1$, a ako je $p = 2$, neka je $n \geq 2$. Ako je $x \in U_n \backslash U_{n+1}$, tada je $x^p = U_{n+1} \backslash U_{n+2}$.*

Dokaz. Neka je $x \in U_n \backslash U_{n+1}$, dakle $x = 1 + p^n k$, za neki k koji nije djeliv s p. Tada je

$$x^p = 1 + \binom{p}{1} kp^n + \binom{p}{2} k^2 p^{2n} + \cdots k^p p^{np} \equiv 1 + kp^{n+1} \pmod{p^{n+2}}.$$

Slijedi da je $x^p \in U_{n+1} \backslash U_{n+2}$. □

Propozicija 20. *Ako je $p \neq 2$, tada je $U_1 \simeq \mathbb{Z}_p$. Ako je $p = 2$, tada je $U_1 = \{\pm 1\} \times U_2$, te je $U_2 \simeq \mathbb{Z}_2$.*

Dokaz. Neka je prvo $p \neq 2$, te neka je $\alpha = 1 + p \in U_1 \backslash U_2$. Koristeći prethodnu lemu, zaključujemo da je $\alpha^{p^i} \in U_{i+1} \backslash U_{i+2}$. Neka je α_n slika od α u U_1/U_n. Tada je $\alpha_n^{p^{n-2}} \neq 1$, ali je $\alpha_n^{p^{n-1}} = 1$, pa onda α ima red točno p^{n-1}. Dakle U_1/U_n je ciklička grupa generirana s α. Slijedi da imamo izomorfizam inverznih sistema

$$\begin{array}{ccccccc} \cdots & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^{n-1}\mathbb{Z} & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & U_1/U_{n+1} & \longrightarrow & U_1/U_n & \longrightarrow & \cdots \end{array}$$

Nakon što primjetimo da je $\varprojlim(U_1/U_n) = U_1$, slijedi da je $U_1 \simeq \mathbb{Z}_p$.

Za $p = 2$, isti argument s izborom $\alpha = 1 + 4$ dokazuje da je $U_2 \simeq \mathbb{Z}_2$. Koristeći da $\{\pm 1\}$ i U_2 imaju trivijalan presjek (tj. $-1 \notin U_2$, te pošto njihov produkt generira U_1 (jer je $[U_1 : U_2] = 2$), slijedi da je $\{\pm 1\} \times U_2$. □

Teorem 21. *Vrijedi:*

(1) Grupa $\mathbb{Z}_p^\times$ je izomorfna s $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ za $p \neq 2$, te s $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ za $p = 2$.

(2) Grupa $\mathbb{Q}_p^\times$ je izomorfna s $\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ ako je $p \neq 2$, te s $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ ako je $p = 2$.

Dokaz. Tvrdnja (1) slijedi iz Propozicija 18 i 20.
Da bi dokazali (2), promotimo preslikavanje

$$\begin{aligned} \mathbb{Z} \times \mathbb{Z}_p^\times &\to \mathbb{Q}_p^\times \\ (n, u) &\mapsto p^n u, \end{aligned}$$

te primjetimo da je to izomorfizam grupa. Korištnjem (1), tvrdnja slijedi. □

Propozicija 22. *Za $p \neq 2$ i prirodan broj m postoji primtivni m-ti korijen iz jedinice u $\mathbb{Q}_p^\times$ (tj. element reda m) ako i samo ako $m|p-1$, te su u $\mathbb{Q}_2^\times$ elementi -1 i 1 jedini korijeni iz jedinice.*

Dokaz. Neka je prvo $p \neq 2$. Da postoje m-ti korijeni iz jedinice kada $m|p-1$ smo vidjeli u korolaru 18. S druge strane kada bi za $m \not| p-1$ postojao m-ti korijen iz jedinice ζ_m, tada bi $\mu_m = \{1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{n-1} q\}$ činili podgrupu reda m od $\mathbb{Z}_p^\times$, što je u kontradikciji s Teoremom 21, (2).

U $\mathbb{Z}_2$ je očito da su ± 1 korijeni iz jedinice. Iz strukture od $\mathbb{Z}_2^\times$ opisane u Teoremom 21, vidimo da su to jedini elementi konačnog reda u $\mathbb{Q}_2^\times$.

□

Korolar 23. *Neka su p i q različiti prosti brojevi. Tada polja $\mathbb{Q}_p$ i $\mathbb{Q}_q$ nisu izomorfna.*

Dokaz. Tvrdnja direktno slijedi iz prošle propozicije, pošto polja imaju korijene jedinice različitog reda. □

Napomena. Neka je p neparan. Tada će se element -1 nalaziti u podgrupi μ_{p-1}, koja je ciklička reda $p-1$, te je -1 reda 2. Element -1 će dakle biti kvadrat u $\mathbb{Q}_p^\times$ ako i samo ako u μ_{p-1} postoji element reda 4, tj. kada je $p \equiv 1 \pmod 4$.

3.7 Kvadrati u $\mathbb{Q}_p^\times$

3.7.1 Slučaj $p \neq 2$

Teorem 24. *Vrijedi:*

(1) *Element $p^n u \in \mathbb{Q}_p^\times$ (s $n \in \mathbb{Z}$ i $u \in \mathbb{Z}_p^\times$) je kvadrat ako i samo ako je n paran i $u \mod p$ je kvadrat u $\mathbb{F}_p^\times$.*

(2) *Vrijedi $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$.*

(3) *Za svaki $c \in \mathbb{Z}_p^\times$ s $c \mod p \notin (\mathbb{F}_p^\times)$, slike od p i c generiraju $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.*

Dokaz. (1) Zapisujući $\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{F}_p^\times \times \mathbb{Z}_p$. Primjetimo da je $2\mathbb{Z}_p = \mathbb{Z}_p$, pa je

$$(\mathbb{Q}_p^\times)^2 = p^{2\mathbb{Z}} \times (\mathbb{F}_p^\times)^2 \times \mathbb{Z}_p.$$

Dakle elemnt $p^n u$ je kvadrat ako i samo ako je n paran u $u \mod p \in (\mathbb{F}_p^\times)^2$.

(2) Koristeći sti zapisa kao u (1), imamo

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \times \{0\} \simeq (\mathbb{Z}/2\mathbb{Z})^2,$$

pošto je $[\mathbb{F}_p^\times : (\mathbb{F}_p^\times)^2] = 2$.

(3) Očito je da je slika od p generator od $p^{\mathbb{Z}}/p^{2\mathbb{Z}}$, te da je slika od c generator od $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$.

□

3.7.2 Slučaj $p = 2$

Teorem 25. *Vrijedi:*

(1) Element $2^n u \in \mathbb{Q}_2^\times$ (s $n \in \mathbb{Z}$ i $u \in \mathbb{Z}_2^\times$) je kvadrat ako i samo ako je n paran i $u \equiv 1 \mod 8$.

(2) Vrijedi $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^3$.

(3) Slike od $2, -1$ i 5 generiraju $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$.

Dokaz. (1) Zapišimo

$$\mathbb{Q}_2^\times \simeq 2^{\mathbb{Z}} \times \mathbb{Z}_2^\times \simeq 2^{\mathbb{Z}} \times U_1.$$

Dokažimo sada da je $U_1^2 \simeq U_3$. Da bi dokazali $U_1^2 \supseteq U_3$, moramo pokazati da za svaki $t \in \mathbb{Z}_2$ postoji $x \in \mathbb{Z}_2$ takav da je $(1+2x)^2 = 1 + 4x + 4x^2 = 8t + 1$, tj. da jednadžba $f(x) = x + x^2 - 2t = 0$ ima rješenje u $\mathbb{Z}_2$. Lako se vidi da je $f(1) \equiv 0 \pmod 2$, te da je $f'(1) \equiv 1 \pmod 2$, pa po Henselovoj lemi, ta jednadžba ima rješenje u $\mathbb{Z}_2$. S druge strane, vidimo da za $1 + 2x \in U_1$, $x \in \mathbb{Z}_2$ vrijedi da je $(1+2x)^2 = 1 + 4x + 4x^2$, a pošto je $x + x^2 \equiv 0 \pmod 2$ za sve $x \in \mathbb{Z}_2$, slijedi da je $x + x^2 \in 2\mathbb{Z}_2$, pa je i $(1+2x)^2 \in 1 + 8\mathbb{Z}_2 = U_3$.

Sada imamo da je $\mathbb{Q}_2^\times \simeq 2^{2\mathbb{Z}} \times U_3$, te slijedi da je element $2^n u \in \mathbb{Q}_2^\times$ kvadrat ako i samo ako je n paran i $u \equiv 1 \pmod 8$.

(2) Koristći (1) dobivamo

$$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times U_1/U_3.$$

Po korolaru 17 vrijedi da je U_1/U_3 grupa reda 4, te se lako provjeri da je svaki element u njoj reda 2.

(3) Očito je da je slika od 2 generator od $2^{\mathbb{Z}}/2^{2\mathbb{Z}}$, te se lako provjeri da slike od -1 i 5 generiraju U_1/U_3.

□

3.8 Proširenja od $\mathbb{Q}_p$

Vratimo se sada na lokalna polja.

Definicija. Neka je $K/\mathbb{Q}_p$ konačno proširenje polja $\mathbb{Q}_p$. Definiramo *prsten cijelih brojeva* $\mathcal{O}_K$ od K kao integralno zatvorneje od $\mathbb{Z}_p$ u K.

Sljedeća propozicije (koju ostavljamo bez dokaza), nam govore da postoji jedinstveno proširenje apsolutne vrijednosti i izgledaju takvi prsteni cijelih brojeva.

Propozicija 26. *Neka je K konačno proširenje od $\mathbb{Q}_p$. Tada postoji jedinstveno ne-arhimedska apsolutna vrijednost na K, koja proširuje p-adsku apsolutnu vrijednost na $\mathbb{Q}_p$.*

Tu apsolutnu vrijednost ćemo također označavati sa $|\cdot|_p$.

Propozicija 27. *Neka je K konačno proširenje od $\mathbb{Q}_p$. Tada je*

$$\mathcal{O}_K = \{x \in K : |x|_p \leq 1\}.$$

Za proširenja od $\mathbb{Q}_p$, kao i za $\mathbb{Q}_p$ vrijedi da imaju jedinstveni maksimalni ideal u svom prstenu cijelih.

Propozicija 28. *Neka je K konačno proširenje od $\mathbb{Q}_p$. Tada $\mathcal{O}_K$ ima jedinstveni maksimalni ideal M,*

$$M = \{x \in K : |x|_p < 1\}.$$

Dokaz. Tvrdnja slijedi odmah iz činjenice da se svaki neinvertibilni element iz $\mathcal{O}_K$ nalazi u M. □

Neka je sada L/K Galoisovo proširenje, $\sigma \in \mathrm{Gal}(L/K)$, gdje su L i K konačna proširenja od $\mathbb{Q}_p$, dakle L je polje cijepanja nekog polinoma iz $K[x]$. Neka je $\mathfrak{p}$ maksimalni ideal od K, a $\mathfrak{P}$ maksimalni ideal od L. Tada je očito $\sigma(\mathfrak{P}) = \mathfrak{P}$. Dakle σ inducira automorfizam od $\mathcal{O}_L/\mathfrak{P}$ koji fiksira $\mathcal{O}_K/\mathfrak{p}$ (lako se dokaže da je $\mathcal{O}_K/\mathfrak{p}$ izomorfno potpolju od $\mathcal{O}_L/\mathfrak{P}$), te nam time daje homomorfizam

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})). \tag{3.3}$$

Propozicija 29. *Preslikavanje* (3.3) *je surjekcija.*

Dokaz. Pošto je $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ konačno proširenje polja, slijedi da postoji primitivni element, tj. da je $\mathcal{O}_L/\mathfrak{P} \simeq (\mathcal{O}_K/\mathfrak{p})[a]$. Neka je $f(x)$ njegov minimalni polinom; slijedi da je minimalni polinom proširenja $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ jednak

$$f(x) = \prod_{s \in \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))} (x - s(a)).$$

Izaberimo $\alpha \in \mathcal{O}_L$ takvog da se preslikava u a pri redukciji $\mod \mathfrak{P}$. Neka je S podskup od $\mathrm{Gal}(L/K)$ takv da se svi konjugati od α pojavljuju točno jednom u skupu $\{\sigma(\alpha) | \alpha \in S\}$. Tada je minimalni polinom od α jednak

$$g(x) = \prod_{\sigma \in S} (x - \sigma(\alpha)).$$

Promotrimo redukciju $\overline{g}(x)$ od $g(x)$. Pošto je α korijen od $g(x)$, tada je i a korijen od $\overline{g}(x)$. Zaključujemo da $f(x)$, pošto je minimalni polinom od a, dijeli $\overline{g}(x)$ u $(\mathcal{O}_K/\mathfrak{p})[x]$. Isto vrijedi i za sve konjugate od a. To znači da za svaki $s \in \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ postoji $\sigma \in \mathrm{Gal}(L/K)$ takav da je $s(a) \equiv \sigma(a) \pmod{\mathfrak{P}}$. Pošto je a primitivni element proširenja, djelovanje $s : \mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}$ je u potpunosti određeno djelovanjem na a. Dakle, vidimo da σ inducira s, tj. s je slika od σ s obzirom na preslikavanje (3.3), te slijedi da je preslikavanje surjektivno. □

Definicija. *Inercijska podgrupa* $I(L/K)$ od $\mathrm{Gal}(L/K)$ je jezgra preslikavanja (3.3).

Drugim riječima, $I(L/K)$ je normalna podgrupa od $\mathrm{Gal}(L/K)$ koju možemo zapisati kao

$$I(L/K) = \{\sigma \in \mathrm{Gal}(L/K) | \sigma(\alpha) \equiv \alpha \text{ za sve } \alpha \in \mathcal{O}_L\}.$$

Iz definicije slijedi da je

$$\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})) \simeq \mathrm{Gal}(L/K)/I(L/K).$$

Definicija. Kažemo da je L/K *nerazgranato* proširenje ako je $I(L/K) = \{1\}$. Kažemo da je L/K *potpuno razgranato* ako je $I(L/K) = \mathrm{Gal}(L/K)$.

Vidimo da je po definiciji proširenje nerazgranato ako i samo ako je

$$\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})) \simeq \mathrm{Gal}(L/K).$$

Primjetimo da će nerazgranato proširenje onda biti uvijek cikličko, pošto je proširenje konačnih polja cikličko (generirano Frobeniusom). U takvoj situaciji ćemo generator od $\mathrm{Gal}(L/K)$ koji odgovara Frobeniusu u $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ također zvati Frobeniusom. Dakle, to je preslikavanje koje zadovoljava

$$\phi(\alpha) = \alpha^q \pmod{\mathfrak{P}},$$

za $q = \#(\mathcal{O}_L/\mathfrak{P})$ i za sve $\alpha \in \mathcal{O}_L$.

Sljedeću činjenicu nećemo dokazivati.

Teorem 30. *Neka je K konačno proširenje od $\mathbb{Q}_p$, neka je k polje ostataka od K, te neka je l/k neko konačno proširenje. Tada postoji jedinstveno nerazgranato proširenje L/K, takvo da je l polje ostataka od L.*

Sada pogledajmo kako primijeniti teoriju p-adskih polja na proširenja polja algebarskih brojeva. Na isti način na koji smo konstruirali $\mathbb{Z}_p$ i $\mathbb{Q}_p$ možemo za polje algebarskih brojeva i prosti ideal $\mathfrak{p}$ u $\mathcal{O}_K$ konstruirati

$$\mathcal{O}_{K,\mathfrak{p}} = \varprojlim \mathcal{O}_K/\mathfrak{p}^n,$$

te $K_{\mathfrak{p}}$ kao polje razlomaka od $\mathcal{O}_{K,\mathfrak{p}}$.

Definicija. Neka je $\mathfrak{p}$ jedinstveni maksimalni ideal u $\mathcal{O}_{K,\mathfrak{p}}$. Generator od π od $\mathfrak{p}$ se zove *uniformizator*.

Neka je L/K Galoisovo proširenja polja algebarskih brojeva, te neka je $\mathfrak{P}$ prost ideal u $\mathcal{O}_L$ iznad prostog ideala $\mathfrak{p}$ u $\mathcal{O}_K$. Može se dokazati da postoji prirodno ulaganje $\mathcal{O}_{K,\mathfrak{p}} \hookrightarrow \mathcal{O}_{L,\mathfrak{P}}$. Slijedi da postoji i ulaganje $K_{\mathfrak{p}} \hookrightarrow L_{\mathfrak{P}}$. Zapravo iz ove činjenice možemo vidjeti da su $K_{\mathfrak{p}}$ i $L_{\mathfrak{P}}$ porširenja od $\mathbb{Q}_p$. Vrijedi također da je $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ također Galoisovo proširenje.

Odredimo sada $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. Očito za svaki $\sigma \in \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, možemo restringirati σ na L, te će σ fiksirati K, pa smo dobili element u $\mathrm{Gal}(L/K)$. Dakle dobili smo preslikavanje $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(L/K)$ za koje lako vidimo da je homomorfizam. Nadalje, pošto je $\sigma(\mathfrak{P}\mathcal{O}_{L,\mathfrak{P}}) = \mathfrak{P}\mathcal{O}_{L,\mathfrak{P}}$ (jer je $\mathfrak{P}\mathcal{O}_{L,\mathfrak{P}}$ jedini prost ideal u $\mathcal{O}_{L,\mathfrak{P}}$), vidimo da je slika takve σ zapravo u dekompozicijskokj grupi $D(\mathfrak{P}/\mathfrak{p})$. S druge strane za svaki $\sigma \in \mathrm{Gal}(L/K)$ koji je u $D(\mathfrak{P}/\mathfrak{p})$, vrijedi da je $\sigma(\mathfrak{P}^i) = \mathfrak{P}^i$. Zaključujemo da je σ automorfizam od $\mathcal{O}_L/\mathfrak{P}^i$, pa time i automorfizam od $\mathcal{O}_{L,\mathfrak{P}}$. Dakle, sada imamo homomorfizam $D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$.

Komponiranjem navedena dva preslikavanja

$$D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(L/K),$$

iz njihovih definicija vidimo da je $D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(L/K)$ prirodno ulaganje (identiteta), te iz toga slijedi da je

$$\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(L/K)$$

također injekcija sa slikom $D(\mathfrak{P}/\mathfrak{p})$. Dakle,

$$\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \simeq D(\mathfrak{P}/\mathfrak{p}).$$

Primjer 6. Neka je $L = \mathbb{Q}(i)$, $K = \mathbb{Q}$, $\mathfrak{p} = 5\mathbb{Z}$. Imamo da se $\mathfrak{p}$ cijepa u $\mathfrak{P}_1\mathfrak{P}_2$, gdje je $\mathfrak{P}_1 = (2-i)$, $\mathfrak{P}_2 = (2+i)$. Pošto je $e = f = 1$, $D(\mathfrak{P}_i/\mathfrak{p})$ je trivijalna, dakle $K_{\mathfrak{P}_i} \simeq \mathbb{Q}_5$.

Poglavlje 4

Dirichletovi karakteri

Definicija. Za konačnu abelovu grupu G, *karakter* od G je homomorfizam $G \to \mathbb{C}^\times$. S $\hat{G}$ označavamo skup svih karaktera od G.

Ako su χ, ψ karakteri od G, tada definiramo umnožak od χ i ψ kao funkciju definiranu s $\chi\psi(g) := \chi(g)\psi(g)$. Uz tu operaciju, $\hat{G}$ postaje grupa, koja se zove *grupa karaktera*. Karakter χ_0 koji šalje svaki $g \in G$ u 1 se zove *trivijalni karakter*, te je on neutralni element u $\hat{G}$.

Propozicija 31. *Ako je G konačna abelova grupa , tada je $\hat{G} \simeq G$.*

Dokaz. [1, Proposition 1.1. p.18] $\square$

Očito slijedi da je $\hat{\hat{G}} \simeq G$. Opišimo eksplicitno ovaj izomorfizam. Neka je $g \in G$. Definirajmo s $\tilde{g} : \hat{G} \to \mathbb{C}^\times$ funkciji koja šalje χ u $\chi(g)$; dakle $\tilde{g} \in \hat{\hat{G}}$.

Propozicija 32. *Preslikavanje $g \mapsto \tilde{g}$ je izomorfizam s G u $\hat{\hat{G}}$.*

Dokaz. [1, Proposition 1.2. p.18] $\square$

Propozicija 33. *(Relacije ortogonalnosti) Neka je G konačna abelova grupa. Za $H \leq G$, neka je*

$$H^\perp := \{\chi \in \hat{G} : \chi(h) = 1 \text{ za sve } h \in H\}.$$

Tada vrijedi:

- $H^\perp \simeq \widehat{G/H}$,
- $\hat{H} \simeq \hat{G}/H^\perp$,
- $(H^\perp)^\perp \simeq H$.

Dokaz. [1, Proposition 1.3. p.18-19] $\square$

Propozicija 34. *a) Neka je χ karakter konačne abelove grupe G. Tada je*

$$\sum_{g\in G}\chi(G) = \begin{cases} 0 \ \textit{ako}\ \chi \neq \chi_0, \\ |G| \ \textit{ako}\ \chi = \chi_0 \end{cases}$$

b) Neka je $g \in G$, gd je G konačna abelova grupa. Tada je

$$\sum_{\chi\in\hat{G}}\chi(G) = \begin{cases} 0 \ \textit{ako}\ g \neq 1, \\ |G| \ \textit{ako}\ g = 1 \end{cases} \quad .$$

Dirichletovi karakteri su vrsta karaktera, te su uvedeni prije općenitijeg pojma karaktera konačne abelove grupe.

Definicija. *Dirichletov karakter modulo n* je karakter χ abelove grupe $(\mathbb{Z}/n\mathbb{Z})^\times$. Vrijednost n nazivamo modulus od χ.

Često se Dirichletovi karakteri modulo n χ proširuju na funkcije $\mathbb{Z} \to C$ tako da se definira da je $\chi(a) = 0$ ako je $(a, n) > 1$. Primjetite da ovo onda više nije homomorfitam grupa.

Primjer 7.
- Neka je $p > 2$ prost. Tada je $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ Legendreov symbol mod p, tj. $\chi(a) = \left(\frac{a}{p}\right)$.
- Neka je $\chi : (\mathbb{Z}/5\mathbb{Z})^\times \to \mathbb{C}^\times$ definiran s $\chi(1) = 1$ $\chi(2) = i$, $\chi(3) = -i$ i $\chi(4) = -1$. Tada je χ karakter.

Lako vidimo da ako je χ karakter modulusa n i $m|n$, i ako je $\phi : (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ prirodni homomorfizam , možemo definirati Dirichletov karakter $\chi' := \chi \circ \phi$ modulusa m. Kažemo da je χ' induciran s χ. Neka je f_χ najmnaji modulus Dirichletovog karaktera, tj. χ nije induciran nekim karakterom manjeg modulusa; tada se f_χ naziva ***konduktor*** od χ. Dirichletov karakter definiran modulo svoj konduktor se naziuva *primitivan*.

Primjer 8.
- Neka je $\chi : (\mathbb{Z}/12\mathbb{Z})^\times \to \mathbb{C}^\times$ definrano s $\chi(1) = 1, \chi(5) = -1, \chi(7) = 1, \chi(11) = -1$. Modulus od χ je 12, konduktor je 3, pošto je χ induciran s karakterom $\psi : (\mathbb{Z}/3\mathbb{Z})^\times \to \mathbb{C}^\times$ definiranog s $\psi(1) = 1, \psi(2) = -1$. Karakter ψ je primitivan, dok χ nije.
- Neka je $\chi : (\mathbb{Z}/12\mathbb{Z})^\times \to \mathbb{C}^\times$ definrano s $\chi(1) = 1, \chi(5) = -1, \chi(7) = -1, \chi(11) = 1$. Tada je χ primitvan karakter.

Ako su χ i ψ primitvni karakteri konduktora f_χ i f_ψ i neka je $n = NZV(f_\chi, f_\psi)$. Tada je funkcija

$$\eta : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times,$$

$$\eta(a) = \chi(c)\psi(a)$$

Dirichletov karakter modulusa n. Konduktor od η je djelitelj od n, te η ne mora biti primitvan. Ovako definirano množenje karaktera je asocijativno i komutatuivno.

Primjer 9. Neka je $\chi : (\mathbb{Z}/12\mathbb{Z})^\times \to \mathbb{C}^\times$ definiran s $\chi(1) = 1, \chi(5) = -1, \chi(7) = -1, \chi(11) = 1$, $\chi : (\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}^\times$ definiran s $\chi(1) = 1, \chi(3) = -1$, tada je $\eta = \chi\psi : (\mathbb{Z}/12\mathbb{Z})^\times \to \mathbb{C}^\times$ definiran s $\chi(1) = 1, \chi(5) = -1, \chi(7) = 1, \chi(11) = -1$, te η nije primitavan, tj. konduktor mu je 3.

Za Dirichletov karakter $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ možemo definirati $\overline{\chi} : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ s $\chi(a) = \overline{\chi(a)} = \chi(a)^{-1}$. Lako vidimo da je $\overline{\chi}$ također karakter istog konduktora kao i χ, te da je $\chi\overline{\chi} = \chi_0$. Zaključujemo da Dirichletovi karaktreri modulo n čine grupu. *Red* Dirichletovog karaktera je njegov red u toj grupi. Pošto je slika Dirichletovog karaktera modulo n sadržana u μ_n, tzaključujemo da red karaktera dijeli μ_n, dakle dijeli $\phi(n)$. Dirichletov karakter reda 2 se naziva kvadratni karakter.

Primjetimo da vrijedi da je $\chi(-1) = \pm 1$. Karakter za kojeg vrijedi da je $\chi(-1) = 1$ kažemo da je paran, a inače kažemo da je neparan.

Napomena. Parni Dirichletovi karakteri modulo n čine podgrupu svih Dirichletovih karaktera modulo n.

Pošto je $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, možemo Dirichletove karaktere smatrati karakterima na $G := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Definicija. Neka je χ karakter od $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, te neka je $H = \ker\chi$, vrijedi da je $H \leq G$. Neka je $K = \mathbb{Q}(\zeta_n)^H$. Tada K nazivamo *polje asocirano s* χ.

Primjer 10. Neka je $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) \to \mathbb{C}^\times$ definiran s $\chi(\sigma_1) = 1, \chi(\sigma_5) = -1, \chi(\sigma_7) = 1, \chi(\sigma_{11}) = -1$, gdje je $\sigma_i(\zeta_{12}) = \zeta_{12}^i$. Tada je očito $\ker\chi = \{\sigma_1, \sigma_7\}$. Primjetimo da je $\sigma_7(\zeta_{12}^4) = \zeta_{12}^4$, pa je $\mathbb{Q}(\zeta_{12}^4) = \mathbb{Q}(\zeta_3)$ sadržano u fiksnom polju od χ. Promatrajući stupnjeve, zaključujemo da je $\mathbb{Q}(\zeta_3)$ polje asocirano s χ.

Općenitije, možemo promatrati konačnu podgrupu X Dirichletovih karaktera. Neka je n NZV konduktora svih karaktera u X. Tada je X podgrupa od $\hat{G}$, gdje je $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Neka je H presjek jezgara svih $\chi \in X$. Tada se fiksno polje K od H naziva polje asocirano s X.

Primjer 11. Neka je $\chi : (\mathbb{Z}/15\mathbb{Z})^\times \to \mathbb{C}^\times$ definiran s $\chi(1) = 1, \chi(2) = -1, \chi(4) = 1, \chi(7) = -1, \chi(8) = -1, \chi(11) = 1, \chi(13) = -1, \chi(14) = 1$. Možemo, kao i prije, smatrati χ karakterom od $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q})$. Vidimo da je $\ker\chi$ reda 4, dakle fiksno polje od jezgre je kvadratno polje. Također vidimo da to fiksno polje mora bit realno jer ga fiksira σ_{14} koje je kompleksno konjugiranje. Dakle, to mora bit realno potpolje od $\mathbb{Q}(\zeta_{15})$. Polje $\mathbb{Q}(\zeta_{15})$ ima 3 kvadratna potpolja, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{5})$ i $\mathbb{Q}(\sqrt{-15})$. Zaključujemo da je to fiksno polje $\mathbb{Q}(\sqrt{5})$.

Neka je $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ i neka je X podgrupa od $\hat{G}$ svih parnih karaktera . Lako vidimo da je $\hat{G}/X$ grupa reda 2 (pošto je produkt 2 neparna karaktera paran), te vidimo po definiciji da je $\chi(\sigma_{-1}) = 1$ za svaki $\chi \in X$. Pošto je σ_{-1} kompleksno konjugiranje, zaključujemo da polje asocirano s X mora biti realno. Općenitije, polje asocirano nekom karakteru χ je realno ako i samo ako je χ paran. Može se pokazati da je polje asocirano s X maksimalno realno potpolje $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ od $\mathbb{Q}(\zeta_n)$.

Sljedeći rezultat ostavljamo bez dokaza

Teorem 35 (Teorem o konduktoru i diskriminanti)**.** *Neka je X konačna grupa Dirichletovih karaktera i K njegovo asocirano polje. Tada je*

$$d_{K/\mathbb{Q}} = (-1)^r \prod_{\chi \in X} f_\chi,$$

gdje je r broj parova kompleksnih ulaganja K u $\mathbb{C}$.

Za primjenu ovog teorema vidi [1, Example 8, p. 23].

4.1 Dirichletov teorem o prostim brojevima u aritimetičkim nizovima

Definicija. *Riemannova zeta fukcija* $\zeta(s)$ se definira s

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prost}} \frac{1}{1-p^{-s}}.$$

Pokažimo sada Eulerov dokaz da postoji beskonačno mnogo prostih brojeva. Tada bi očito limes u 1 izraza s desne strane postojao i bio konačan. Dakle,

$$\lim_{s \to 1} \zeta(s) = \prod_{p \text{ prost}} \frac{1}{1-p}.$$

Međutim, jasno je da lijeva strana divergira, po definiciji, dakle ima beskonačno mnogo prostih brojeva.

Teorem 36 (Dirichletov teorem o prostim brojevima u aritimetičkim nizovima)**.** *Neka je m prirodan broj i a neki prirodan broj relativno prost s m. Tada postoji beskonačno mnogo prostih brojeva takvih da je $p \equiv a \pmod{m}$.*

Skicirajmo dokaz ovog teorema.

Definicija. Neka je χ Dirichletov karakter. Tada je *Dirichletova L-funkcija pridružena* χ

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Ključna tvrdnja koja se pokaže za dokaz Dirichletovog teorema o prostim brojevima je da je

$$\sum_{\chi} \chi(a)^{-1} \log L(s,\chi) = \phi(m) \sum_{p \equiv a(m)} p^{-s} + \text{ nešto abs. konv. za } \mathrm{Re}(s) > 1/2,$$

te se zatim dokaže da lijeva strana divergira. Prvi, analitički, dokaz je dao Dirichlet 1840., a Kummer je 1850. našao aritmetički dokaz.

4.2 Dirichletova gustoća

Definicija. Neka je S neki skup prostih brojeva. Tada kažemo da S ima Dirichletovu gustoću $\delta(S)$ ako postoji

$$\delta(S) = \lim_{s\to 1^+} \frac{\sum_{p\in S} p^{-s}}{\sum_{p\in \mathcal{P}} p^{-s}}.$$

Ekvivalentno je

$$\frac{\lim_{s\to 1^+} \sum_{p\in S}}{\log \frac{1}{1-s}} p^{-s} = \delta.$$

Vrijedi:

a) Ako je S konačan, tada je $\delta(S) = 0$.

b) Ako je S skup prostih brojeva takvih da je $p \equiv a \pmod{m}$, tada je $\delta(S) = 1/\phi(m)$.

c) Ako je S skup prostih brojeva koji počinju s 1 u dekadskom zapisu, tada je $\delta(S) = \log_2 10$.

Napomena. Vriednost

$$\lim_{x\to\infty} \frac{|\{p \in S : p \leq x\}|}{|\{p \in \mathcal{P} : p \leq x\}|},$$

ako spostoji, se naziva *prirodna gustoća.* Vrijedi da ko postoji prirodna gustoća, tada postoji i Dirichletova gustoća, i one su jednake. Međutim, može se dogoditi da postoji Dirichletova gustoća nekog skupa, a da ne postoji prirodna gustoća. Na primjer, skup iz c) gore nema prirodnu gustoću. Vidi [6, Proposition 4.1. p.158]

Promotrimo sljedeći problem: neka je $f(x) \in \mathbb{Z}[x]$, te nas zanima koliki je prosječan broj n_p korijena od $f \pmod{p}$ kada p varira. Na primjer, za $f(x) = x^2 + 1$, vrijedi da f ima 1 nultočku kada je $p = 2$, 2 nultočke ako je $p \equiv 1 \pmod{4}$, i 0 ako je $p \equiv 3 \pmod{4}$. Dakle u prosjeku je $n_p = 1$.

Definicija. Neka je K/F Galoisovo proširenje i neka je

$$\mathcal{S}_{K/F} := \{\mathfrak{p} \in \mathcal{O}_F : \text{ koji se potpuno cijepaju u } K/F\}.$$

Teorem 37 (Kronecker, 1880.)**.** *Ako $f(X)$ ima r ireducibilnih faktora u $\mathbb{Z}[x]$, tada je prosječna vrijednost n_p jednaka r, tj.*

$$\lim_{s\to 1^+} \frac{\sum_p n_p p^{-s}}{\sum_p p^{-s}} = r.$$

Korolar 38. *Neka je $K/\mathbb{Q}$ Galoisovo proširenje. Tada je $\delta(\mathcal{S}_{K/\mathbb{Q}}) = 1/[K : \mathbb{Q}]$.*

Dokaz. Neka je $K = \mathbb{Q}(\alpha)$, za neki $\alpha \in \mathcal{O}_K$; takav postoji po teoremu o primitivnom elementu. Neka je $f \in \mathbb{Z}[x]$ njegov minimalni polinom. Tada su svi korijeni od f polinomi u α. Dakle ako f ima korijen $\pmod p$, tada su svi korijeni definirani nad $\mathbb{F}_p$, te se se p cijepa u K (ova tvrdnja vrijedi za sve osim konačno mnogo p-ova). Dakle $n_p = \deg f = [K : \mathbb{Q}]$, osim ako je $n_p = 0$.

Sada Kroneckerov teorem kaže da je

$$\delta(S_{K/F}) = \lim_{s\to 1^+} \frac{\sum_{p\in S_{K/F}} [K:\mathbb{Q}]p^{-s}}{\sum_{p\in\mathcal{P}} p^{-s}} = 1,$$

to jest,

$$\delta(S) = \lim_{s\to 1^+} \frac{\sum_{p\in A} p^{-s}}{\sum_{p\in\mathcal{P}} p^{-s}} = \frac{1}{[K:\mathbb{Q}]}.$$

Pošto vrijedi da se $f(x) \pmod p$ cijepa ako i samo ako se p cijepa u K osim za konačno mnogo iznimaka (pogledati na wikipediji), tvrdnja je dokazana. $\square$

Kronecker je u svom radu napisao dva važna problema. Jedna je slutila gustoću prostih brojeva tavih da $f(x) \pmod p$ ima neki fiksan broj faktora (Kronecker je to dokazao za slučaj da se F potpuno cijepa). Postojanje ovih gustoća je dokazao Frobenius krajem 19. stoljeća (1896.), te je on dao točnu slutnju, koja će kasnije postati Čebotarev teorem o gustoći, kojeg ćemo kasnije spomenuti.

Drugo pitanje je bila slutnja da je Galoisovo proširenje K od $\mathbb{Q}$ karakterizirano prostim brojevima koji se u potpunosti cijepaju u K. Na primjer $\mathbb{Q}(i)$ je u potpunosti određeno s tim da se potpuno cijepaju prosti brojevi $p \equiv 1 \pmod 4$. Slutnju je dokazao Bauer 1903.

Dirichletovu gustoću se može definirati i općenitije, gdje se promatra neki skup prostih ideala nekog PAB.

Definicija. Neka je F PAB i S neki skup prostih ideala od F. Tada kažemo da S ima Dirichletovu gustoću $\delta_F(S)$ ako postoji

$$\delta_F(S) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} N(p)^{-s}}{\log \frac{1}{1-s}}.$$

Tada se na isti način kao i Kroneckerov teorem dokazuje da je $\delta_F(\mathcal{S}_{K/F}) = 1/[K:F]$.

Teorem 39 (Bauer)**.** *Neka su L_1 i L_2 konačna Galoisova proširenja od K Tada je $L_1 \subseteq L_2$ ako i samo ako je $\mathcal{S}_{L_2/K} \subseteq \mathcal{S}_{L_1/K}$. Posebno, $L_1 = L_2$ ako i samo ako je $\mathcal{S}_{L_2/K} \subseteq \mathcal{S}_{L_1/K}$.*

Dokaz. Ako je $L_1 \subseteq L_2$, tada se lako vidi da je $\mathcal{S}_{L_2/K} \subseteq \mathcal{S}_{L_1/K}$. Obrnuto, ako je $\mathcal{S}_{L_2/K} \subseteq \mathcal{S}_{L_1/K}$, promotrimo proširenje L_1L_2/K. Ono je Galoisovo i $\mathcal{S}_{L_1L_2/K} = \mathcal{S}_{L_2/K} \cap \mathcal{S}_{L_1/K} = \mathcal{S}_{L_2/K}$. Uspoređujući Dirichletovu gustoću prostih brojeva koji se cijepaju u L_1L_2 i L_2 dobijemo da je $1/[L_1L_2 : K] = 1/[L_2 : K]$, tj. $L_1L_2 = L_2$, odnosno $L_1 \subseteq L_2$. $\square$

U gornjem dokazu smo koristili tvrdnju da je $\mathcal{S}_{L_1L_2/K} = \mathcal{S}_{L_2/K} \cap \mathcal{S}_{L_1/K}$. Dokažimo tu tvrdnju.

Propozicija 40. *Neka su L_1/K i L_2/K proširenja PAB. Tada se $\mathfrak{p}$, prost ideal od $\mathcal{O}_K$ u potpunosti cijepa (u kojima je nerazgranat) ako i samo ako se $\mathfrak{p}$ poptuno cijepa (nerazgranat je) u L_1L_2/K.*

Dokaz. Očito je da ako se $\mathfrak{p}$ potpuno cijepa u L_1L_2/K, tada se potpuno cijepa u L_1/K i L_2/K. Pretpostavimo sada da se $\mathfrak{p}$ poptuno cijepa u L_1/K i L_2/K. Neka je F Galoisovo zatvorenje od L_1L_2 nad K, neka je $\mathfrak{P}$ prost ideal od F nad $\mathfrak{p}$, te neka je $D := D(\mathfrak{P}/\mathfrak{p})$. Neka je $K \subseteq M \subseteq F$ bilo koje međupolje, te neka je $\mathfrak{p}_M$ prost ideal ispod $\mathfrak{P}$. Tada je $e(\mathfrak{p}_M/\mathfrak{p}) = f(\mathfrak{p}_M/\mathfrak{p}) = 1$ (tj. $\mathfrak{p}$ se potpuno cijepa u M) ako i samo je $M \subseteq F^D$. Neka je $G_i := \mathrm{Gal}(F/L_i)$. Tada je po pretpostavci $L_i \subseteq F^D$, tj. drugim riječima $F^{G_i} \subseteq F^D$, odnosno $D \leq G_i$. Pa slijedi da je $D \leq G_1 \cap G_2 = \mathrm{Gal}(F/L_1L_2)$, dakle $L_1L_2 \subseteq F^D$, pa se $\mathfrak{p}$ potpuno cijepa u L_1L_2.

Tvrdnaj za nerazgranatost se dokazuje potpuno ekvivalenetno, osim što se koristi inercijska podgrupa umjesto dekompozicijske. $\square$

Primjetimo da mijenjanje skupa prostih brojeva za neki konačan skup, Bauerov teorem ostaje isti, pošto se ne mijenjaju gustoće.

Poglavlje 5

Grupe klasa zraka

Prirodno je pitanje je li možemo generalizirati Dirichletov teorem o prostim brojevima: postoji li beskonačno mnogo prostih ideal u $\mathcal{O}_K$ u nekakvoj "aritmetičkoj progresiji".

Definicija. Kažemo da je $a \in K$ *potpuno pozitivan* ako je $\sigma(\alpha/\beta) > 0$ za sva realna ulaganja $K \hookrightarrow \mathbb{C}$, te označavamo to s $a >> 0$.

Definicija. Neka je $\mathfrak{m}$ neki netrivijalni ideal u PAB $\mathcal{O}_K$ i neka jhe $I_\mathfrak{m}$ grupa razlomljenih ideala u K koji su relativno prosti s $\mathfrak{m}$ i neka je $P_\mathfrak{m}^+$ grupa glavnih razlomljenih ideala u K oblika (α/β) takvih da je

- (α) i (β) su relativno prosti s $\mathfrak{m}$,
- $\alpha \equiv \beta \pmod{\mathfrak{m}}$,
- α/β je potpuno pozitivan.

Ako je $\gamma = \alpha/\beta$ takav da zadovoljava gornja svojstva, pišemo $\gamma \equiv 1 \pmod{^*\mathfrak{m}}$. Grupu $P_\mathfrak{m}^+$ nazivamo *zraka modulo* $\mathfrak{m}$.

Dakle, $P_\mathfrak{m}^+$ je skup (γ) takvih da je $\gamma \equiv 1 \pmod{^*\mathfrak{m}}$.

Primjer 12. Ideal je u $P_{(1)}^+$ ako i samo ako je generiran nekim potpuno pozitivnim generatorom. Na primjer, u $\mathbb{Q}(\sqrt{2})$ ideal $\sqrt{2}$ je u $P_{(1)}^+$ iako $\sqrt{2}$ nije potpuno pozitivan. To možemo vidjeti jer $\sqrt{2}(1+\sqrt{2})$ generira isti ideal, a potpuno je pozitivan.

S druge strane $(\sqrt{3})$ nije u u $P_{(1)}^+$ jer $\sqrt{3}u$ nije potpuno pozitivan ni za jednu vrijednost $u \in \mathbb{Z}[\sqrt{-3}]$, to vidimo pošto sve jedinice u u $\mathbb{Z}[\sqrt{-3}]$ imaju normu 1 (grupa je generirana s -1 i $2+\sqrt{3}$), pa $\sqrt{3}u$ ima normu -3.

Primjetimo da uvijek vrijedi $P_{(1)}^+ \leq P \leq I_{(1)}$ gdje je P skup svih galvnih razlomljenih ideala od K. Također, vrijedi da je $I_{(1)}/P$ grupa klasa ideala.

Definicija. Svaku grupu $P_{\mathfrak{m}}^{+} \leq H \leq I_{\mathfrak{m}}$ nazivamo *grupu ideala s modulusom* $\mathfrak{m}$, te kvocijent $I_{\mathfrak{m}}/H$ nazivamo *generaliziranom grupom klasa ideala.*

Definicija. *Grupa klasa zraka* je

$$\mathcal{R}_{\mathfrak{m}}^{+} = I_{\mathfrak{m}}/P_{\mathfrak{m}}^{+}.$$

Definicija. Grupa

$$\mathcal{R}_{K}^{+} := I_{(1)}/P_{(1)}^{+}$$

se naziva *stroga (uska) grupa klasa ideala od K.*

Primjer 13. Neka je $K = \mathbb{Q}$ i $\mathfrak{m} = m\mathbb{Z}$. Tada za $(r) \in I_{\mathfrak{m}}$ vrijedi $r = a/b$, gdje su $r > 0$, $(a, m) = (b, m) = 1$. Tada je preslikavanje

$$I_{\mathfrak{m}} \to (\mathbb{Z}/m\mathbb{Z})^{\times},$$

$$(r) \mapsto ab^{-1} \pmod m$$

dobro definirano. Lako vidimo da je to preslikavanje surjektivno s jezgrom $P_{(\mathfrak{m})}^{+}$, te slijedi da je

$$I_{\mathfrak{m}}/P_{(\mathfrak{m})}^{+} \simeq (\mathbb{Z}/m\mathbb{Z})^{\times}.$$

Propozicija 41. *Za modulus $\mathfrak{m}$ polja K je $R_{\mathfrak{m}}^{+}$ je konačna grupa i vrijedi*

$$|R_{\mathfrak{m}}^{+}| = \frac{h_K \cdot 2^{r_1}\phi(\mathfrak{m})}{[\mathcal{O}_K^{\times} : (\mathcal{O}_K^{\times})^{+}]},$$

gdje su

$$h_K = \text{ broj klasa od } K, \tag{5.1}$$
$$r_1 = \text{ broj realnih ulaganja } K \hookrightarrow \mathbb{C}, \tag{5.2}$$
$$\phi(m) = |\mathcal{O}_K/\mathfrak{m}|, \tag{5.3}$$
$$(\mathcal{O}_K^{\times})^{+} = \left\{\epsilon \in \mathcal{O}_K^{\times} : \epsilon \equiv 1 \pmod{{}^{*}\mathfrak{m}}\right\}. \tag{5.4}$$

Dokaz. [1, Proposition 2.1. p.50-52]. □

Za dva skupa A, B označimo da $A \approx B$ ako se A i B razlikuju za skup Dirichletove gustoće 0.

Definicija. Neka je K/F Galoisovo proširenje i neka je $\mathfrak{m}$ ideal u $\mathcal{O}_F$. Kažemo da je K *polje klasa* od H (gdje je H generalizirana grupa ideala) nad F ako je

$$S_{K/F} = \{\text{prosti ideali } \mathfrak{p} \text{ u } \mathcal{O}_F : \mathfrak{p} \text{ se potpuno cijepa u } K/F\}$$

$$\approx \{\text{prosti ideali } \mathfrak{p} \text{ u } \mathcal{O}_F : \mathfrak{p} \in H\}.$$

Primjer 14. Neka je $F = \mathbb{Q}$ i $\mathfrak{m} = m\mathbb{Z}$. Tada je

$$\{p\mathbb{Z} : p\mathbb{Z} \in P_{\mathfrak{m}}^{+}\} = \{p\mathbb{Z} : p \equiv 1 \pmod m, p > 0\}$$

$$= \{p\mathbb{Z} : p \text{ se potpuno cijepa u } \mathbb{Q}(\zeta_m)/\mathbb{Q}\} = S_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}.$$

Dakle $\mathbb{Q}(\zeta_m)$ je polje klasa od $P_{\mathfrak{m}}^{+}$ nad $\mathbb{Q}$.

Primjer 15. Proširenje $\mathbb{Q}(i)/\mathbb{Q}$ je polje klasa za $P^+_{(4)}$, pošto se $p > 0$ cijepa u $\mathbb{Q}(i)$ ako i samo ako je $p \equiv 1 \pmod 4$.

Primjer 16. Proširenje $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ je polje klasa za $\{P^+_{(8)}, -P^+_{(8)}\}$, pošto se $p > 0$ cijepa u $\mathbb{Q}(\sqrt{2})$ ako i samo ako je $p \equiv \pm 1 \pmod 8$.

Logično se nameće pitanje je li postoje polje klasa za svaku generaliziranu grupu klasa ideala i je li jedinstveno. Jedinstvenost nije teško pokazati.

Teorem 42 (Weber)**.** *Ako polje klasa K od H nad F postoji, tada je jedinstveno.*

Dokaz. Sjetimo se da smo pokazali da je $\delta(S_{K/F}) = 1/[K : F]$. Ako su K_1 i K_2 dva polja klasa od H i neka je $K = K_1K_2$. Imamo da je

$$S_{K/F} = S_{K_1/F} \cap S_{K_2/F} \approx \{\mathfrak{p} \in \mathcal{O}_F : \mathfrak{p} \in H\}.$$

Očito slijedi da je

$$S_{K/F} \approx S_{K_1/F} \approx S_{K_2/F}.$$

Dakle vrijedi

$$\frac{1}{[K : F]} = \frac{1}{[K_1 : F]} = \frac{1}{[K_2 : F]},$$

pa vrijedi $K = K_1 = K_2$. □

Možemo se pitati je li postoji generalizacija Dirichletovog teorema o aritmetičkim progresijama za PAB? Zapravo se pitamo za neki modulus $\mathfrak{m}$, postoji li beskonačno prostih ideala u svakoj klasi modulo H. Vrijedi sljedeće

Teorem 43 (Weber)**.** *Neka je K/F Galoisovo i $P^+_{\mathfrak{m}} \leq H \leq I_{\mathfrak{m}}$. Pretpostavimo da postoji skup prostih $T \subseteq H$ takav da je $S_{K/F} \approx T$. Tada je*

$$[I_{\mathfrak{m}} : H] \leq [K : F].$$

Dokaz. [1, Theorem 2.4, p.57-58.] □

Primjetimo da $I_{\mathfrak{m}}/H$ možemo smatrati generalizacijom od $(\mathbb{Z}/m\mathbb{Z})^{\times}$, kao što smo ranije vidjeli u primjeru. Tako da bi generalizacija Dirichletovog teorema zapravo pitala postoji li beskonačno mnogo prostih ideala u svakoj klasi od $I_{\mathfrak{m}}/H$.

Korolar 44. *Neka je K/F Galoisovo i neka je K polje klasa od H, gdje je $P^+_{\mathfrak{m}} \leq H \leq I_{\mathfrak{m}}$. Tada je*

$$[I_{\mathfrak{m}} : H] = [K : F]$$

i postoji beskonačno mnogo prostih ideala u svakoj klasi od $I_{\mathfrak{m}}/H$.

Dokaz. [1, Corollary 2.5]. □

Ovdje vidimo prvu primjenu polja klasa - njihovo postojanje je nužnost u dokazu generaliziranog Dirichletovog teorema.

Ulogu koje je u dokazu od Dirichletovog teorema o aritmetičkim progresijama imala Dirichletova L-funcija ovdje zauzima funkcija koju je uveo Weber:

$$L(s,\psi)=\prod_{\mathfrak{p}\nmid\mathfrak{m}}\frac{1}{1-\psi(\mathfrak{p})N(\mathfrak{p})^{-s}}=\sum_{(a,\mathfrak{m})=1}\frac{\psi(a)}{N(a)^s},$$

gdje je ψ karatker od I_m/H.

Poglavlje 6

Mjesta

Definicija. *Mjesto* od K je klasa ekvivalenncije netrivijalnih apsolutniuh vrijednosti na K. Skup svih mjesta od PAB F označavamos V_F.

Definicija. Za svaki prosti ideal od $\mathcal{O}_K$ postoji točno jedno mjesto (koje se naziva *konačno ili ne-Arhimedsko ili diskretno mjesto*) u K, te po jedno mjesto za svako ulaganje $K \hookrightarrow \mathbb{R}$ (koje se naziva *realno mjesto*), te po jedno za svaki par konjugiranih kompleksnih ulaganja $K \hookrightarrow \mathbb{C}$ (koje se naziva *kompleksno mjesto*).

Preciznije, imamo sljedeće 3 vrste mjesta na PAB F

- Konačna mjesta, za svaki prost ideal $\mathfrak{p}$ imamo $|\alpha|_{\mathfrak{p}} = N(\mathfrak{p})^{-v_{\mathfrak{p}}(\alpha)}$.
- Beskonačna realna, za ulaganje $\sigma : F \to \mathbb{R}$, imamo $|\alpha|_\sigma = |\sigma(\alpha)|_{\mathbb{R}} = |\sigma(\alpha)|_\infty$.
- Beskonačna kompleksna, za ulaganje $\sigma : F \to \mathbb{C}$, imamo $|\alpha|_\sigma = |\sigma(\alpha)|_{\mathbb{C}}^2$.

Činjenica. Neka su mjesta nekog PAB defgfinirana kao gore. Tada vrijedi *produktana formula*, koja kaže da je

$$\prod_{v \in V_F} |x|_v = 1 \text{ za svaki } x \in F^\times.$$

Za ilustraciju, vidjeti [1, p.65-66].

Primjetimo da različita prosti ideali daju različita mjesta, te da različita realna (i kompleksna) ulaganja također daju različite absolutne vrijednosti (osim ako su konjugirana).

Konačna mjesta poistovjećujemo s idealima $\mathfrak{p}$ od $\mathcal{O}_K$, dok za realno mjesto pridruženo realnom ulaganju σ često pišemo $\mathfrak{p}_\sigma$, te definiramo

$$\alpha \equiv \beta \pmod{\mathfrak{p}}_\sigma \text{ ako i samo ako je } \sigma(\alpha/\beta) > 0.$$

Definicija. Kažemo da se realno mjesto od K cijepa u L/K ako su sva njegova proširenja na $L \hookrightarrow \mathbb{C}$ relana. U suprotnom kažemo da se to mjesto grana.

Definicija. *Modulus* $\mathfrak{m}$ (od K) je preslikavanje

$$m : \{\text{mjesta od } K\} \to \mathbb{Z}$$

takvo da

- $m(\mathfrak{p}) \geq 0$ za sva mjesta $\mathfrak{p}$ i $m(\mathfrak{p}) = 0$ za sve osim konačno mnogo $\mathfrak{p}$.
- Ako je $\mathfrak{p}$ realno mjesto, ta da je $m(\mathfrak{p}) = 0$ ili 1, te ako je $\mathfrak{p}$ kompleksan, tada je $m(\mathfrak{p}) = 0$.

Definicija.

Pišemo
$$\mathfrak{m} = \prod \mathfrak{p}^{m(\mathfrak{p})}.$$

Također, modulus $\mathfrak{m}$ možemo zapisati kao $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, gdje je $\mathfrak{m}_\infty$ product realnih mjesta, dok je $\mathfrak{m}_0$ produkt konačnih mjesta (prostih ideala). Primjetimo da sa da $P_\mathfrak{m}^+$ možemo reinterpretirati s skupom svih $a \in K^\times$ takvih da je

- $v_\mathfrak{p}(a-1) \geq m(\mathfrak{p})$ za sva konačna mjesta $\mathfrak{p}$ koja dijele $\mathfrak{m}$.
- $v_\mathfrak{p}(a) > 0$ za sve realna mjesta $\mathfrak{p}$.

Poglavlje 7

Artinovo preslikavanje

Označimo polje ostataka $\mathcal{O}_K/\mathfrak{P}$ od $\mathfrak{P}$ s $k(\mathfrak{P})$, te polje ostataka $\mathcal{O}_F/\mathfrak{p}$ od $\mathfrak{p}$ s $k(\mathfrak{p})$. Pretpostavimo da je $e(\mathfrak{P}/\mathfrak{p}) = 1$, tada imamo da je preslikavanje

$$I(\mathfrak{P}/\mathfrak{p}) = \ker\left(D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})\right)$$

izomorfizam, te je tada $D(\mathfrak{P}/\mathfrak{p}) \simeq \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ ciklička grupa reda f. Pošto je $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ generirana s elementom $\phi_\mathfrak{p}$ (koji djeluje kao $x \mapsto x^{N(\mathfrak{p})}$) koji se naziva *Frobenius*, mora postojati jedinstveni $\sigma \in D(\mathfrak{P}/\mathfrak{p})$ takav da se on preslika (s kanonskim izomorfizmom $D(\mathfrak{P}/\mathfrak{p}) \simeq \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$) u $\phi_\mathfrak{p}$. Dakle, imamo da je $\langle\sigma\rangle = D(\mathfrak{P}/\mathfrak{p})$. Ovaj element σ se naziva Frobenius u $\mathfrak{P}$. Označavamo ga i s $\sigma = \left(\frac{\mathfrak{P}}{K/F}\right) = (\mathfrak{P}, K/F)$.

Propozicija 45. *Neka je K/F Galoisovo proširenje PAB, $\mathfrak{p}$ ne-nul prosti ideal od $\mathcal{O}_F$ koji je nerazgranat u K, te neka je $\mathfrak{P}$ prost ideal od $\mathcal{O}_K$ koji dijeli $\mathfrak{p}\mathcal{O}_F$. Tada je Frobenius od $\mathfrak{P}$ jedinstveni $\sigma \in \mathrm{Gal}(K/F)$ koji zadovoljava $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})}$ $\pmod{\mathfrak{P}}$ za svaki $\alpha \in \mathcal{O}_K$.*

Dokaz. Neka je $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$ za sve $\alpha \in \mathcal{O}_K$. Tada vidimo da ako je $\alpha \in \mathfrak{P}$, tada je $\sigma(\alpha) \in \mathfrak{P}$, pa je $\sigma(\mathfrak{P}) \subseteq \mathfrak{P}$. Očito vrijedi da je $\sigma(\mathfrak{P}) = \mathfrak{P}$, pošto σ šalje proste ideale u proste ideale. Dakle $\sigma \in D(\mathfrak{P}/\mathfrak{P})$. Očito je da prirodni izomorfizam $D(\mathfrak{P}/\mathfrak{P}) \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ šalje σ u $\phi_\mathfrak{p}$. $\square$

Lema 46. *Neka je K/F Galoisovo proširenje PAB, $\mathfrak{p}$ ne-nul prosti ideal od $\mathcal{O}_F$ koji je nerazgranat u K, te neka je $\mathfrak{P}$ prost ideal od $\mathcal{O}_K$ koji dijeli $\mathfrak{p}\mathcal{O}_F$, te neka je $\mathfrak{P}_2 = \tau\mathfrak{P}$ drugi takava ideal, za neki $\tau \in \mathrm{Gal}(K/F)$. Tada je $D(\tau\mathfrak{P}/\mathfrak{p}) = \tau D(\mathfrak{P}/fp)\tau^{-1}$ i $(\tau\mathfrak{P}, K/F) = \tau(\mathfrak{P}, K/F)\tau^{-1}$.*

Dokaz. Neka je $\sigma \in D(\mathfrak{P}/\mathfrak{p})$; tada vrijedi

$$\tau\sigma\tau^{-1}(\tau\mathfrak{P}) = \tau\sigma(\mathfrak{P}) = \tau\mathfrak{P},$$

pa je $\tau\sigma\tau^{-1} \in D(\tau\mathfrak{P}/\mathfrak{p})$. Dakle imamo da je $\tau D(\mathfrak{p})\tau^{-1} \subseteq D(\tau\mathfrak{P}/\mathfrak{p})$, a pošto su ovmi grupama redovi jednaki ($= ef$), te grupe su jednake.

Dokažimo sada drugu tvrdnju: neka je $\alpha \in \mathcal{O}_K$ i neka je $\sigma = (\mathfrak{P}, K/F)$, dakle $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{p}}$ za svaki $\alpha \in \mathcal{O}_K$. Tada vrijedi

$$\tau\sigma\tau^{-1}(\alpha) = \tau((\tau^{-1}\alpha)^{N(\mathfrak{p})} + a) \text{ za neki } a \in \mathfrak{P}.$$

Nadalje imamo

$$\tau((\tau^{-1}\alpha)^{N(\mathfrak{p})} + a) = \alpha^{N(\mathfrak{p})} + \tau a \equiv \alpha^{N(\mathfrak{p})} \pmod{\tau\mathfrak{P}}.$$

□

Pretpostavimo od sada nadalje da je $G = \mathrm{Gal}(K/F)$ Abelova. Po prethodnoj lemi $D(\mathfrak{P}/\mathfrak{p})$ i $D(\tau\mathfrak{P}/\mathfrak{p})$ su konjugirane, tj. jednake pošto je G Abelova. Dakle dekompozicijska grupa ovisi samo o $\mathfrak{p}$ te ju možemo označiti s $D(\mathfrak{p})$ (uvijek ćemo znati o kojem se proširenju radi). Također, dokazali smo i sljedeću propoziciju.

Propozicija 47. *Neka je K/F Abelovo proširenje PAB, $\mathfrak{p}$ ne-nul prosti ideal od $\mathcal{O}_F$ koji je nerazgranat u K, te neka je $\mathfrak{P}$ prost ideal od $\mathcal{O}_K$ koji dijeli $\mathfrak{p}\mathcal{O}_F$. Tada $\sigma = \left(\frac{\mathfrak{P}}{K/F}\right)$ ne ovisi o izboru $\mathfrak{P}$ nad $\mathfrak{p}$*

Dokaz. Prema prethodnoj lemi, Frobeniusi različitih prostih ideala koji leže nad istim prostim idealom su konjugirani u $\mathrm{Gal}(K/F)$, dakle jednaki, pošto je $\mathrm{Gal}(K/F)$ Abelova. □

Dakle i Frobenius ovisi samo o $\mathfrak{p}$, a ne o izboru $\mathfrak{P}$. U tom slučaju taj automorfizam zovemo *Artinov automorfizam.* Dakle, možemo definirati preslikavanje koje za nerazgranati ideal $\mathfrak{p}$ šalje $\mathfrak{p} \to \sigma_\mathfrak{p} = (\mathfrak{p}, K/F)$.

Definiramo *Artinovo preslikavanje* kao preslikavanje koje neki prosti ideal $\mathfrak{p}$ preslikava u Frobenius u $\mathfrak{p}$. Možemo ga proširiti na sljedeći način.

Primjer 17. Neka je $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{m})$. Gdje je m kvadratno slobodan. Tada se skup prostih brojeva takvih da se p grana u K satoji od svih $p|m$ i od 2 ako je $m \not\equiv 1 \pmod 4$.

Definicija. Neka je K/F Abelovo proširenje PAB, te $\mathfrak{m}$ produkt svih ideala u F koji se granaju u K. Preslikavanje

$$\theta_{K/F} : I_m \to \mathrm{Gal}(K/F), \quad \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_t^{n_t} \mapsto \prod_{i=1}^{t} (\mathfrak{p}_i, K/F)^{n_i}.$$

se zove *globalno Artinovo preslikavanje.*

Primjer 18. Neka je $F = \mathbb{Q}$, $K = \mathbb{Q}(\zeta_m)$, gdje je m neparan broj, te neka je p neaparan prost broj koji ne dijeli m. Tada se p ne grana u K.

Odredimo $(p, K/\mathbb{Q})$. Neka je $\alpha = \sum_i a_i\zeta_m^i \in \mathcal{O}_K = \mathbb{Z}[\zeta_m]$. Imamo da je

$$\alpha^p = (\sum_i a_i\zeta_m^i)^p \equiv \sum_i a_i\zeta_m^{ip} = \sigma_p(\alpha) \pmod{\mathfrak{p}},$$

za svaki $\mathfrak{p}$ nad p, pošto je $\mathcal{O}_K/\mathfrak{p}$ karakteristike p. Dakle $\sigma_p = (p, K/\mathbb{Q})$.

Neka je p nerazgranat. Što je $(p, K/\mathbb{Q})$? Imamo dva slučaja: kada se p cijepa i kada je p inertan u K. Ako se p cijepa, tada je $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, te je $D(p) = \{id\}$. U ovom slučaju nemamo puno izbora, dakle $(p, K/\mathbb{Q}) = id$. Ako je p inertan tada je $D(p) = \mathrm{Gal}(K/\mathbb{Q})$, te tražimo $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ takav da je $\alpha^p \equiv \sigma(\alpha) \pmod{p\mathcal{O}_K}$ za sve $\alpha \in \mathcal{O}_K$. Primjetimo da je ovdje $k(p\mathcal{O}_K) \simeq \mathbb{F}_{p^2}$, te da je $\mathrm{Gal}(k(p\mathcal{O}_K)/\mathbb{F}_p) = \langle \phi^p \rangle$, tj. $x \mapsto x^p$ je genrator od $\mathrm{Gal}(k(p\mathcal{O}_K)/\mathbb{F}_p)$. To preslikavanje ne djeluje trivijalo na sve elemente od $\mathbb{F}_{p^2}$ (djeluje trivijalno samo na elemente od $\mathbb{F}_p$), dakle $(p, K/\mathbb{Q})$ ne može biti identita, pa mora biti generator od $\mathrm{Gal}(K/\mathbb{Q})$.

Neka je $\mathfrak{m}'$ produkt svih prostih brojevarazgranatih u K/F. Ako poistovjetimo $\mathrm{Gal}(K/\mathbb{Q})$ s $\{\pm 1\}$, u ovom slučju je Artinovo preslikavanje definirano s

$$I_{m'} \to \{\pm 1\} \quad p \mapsto \left(\frac{m}{p}\right)$$

Lema 48. *Neka je $F \subseteq L \subseteq K$ proširenja PAB (ne nužno Galoisova), te neka je $\mathfrak{p}$ prost ideal od $\mathcal{O}_F$, $\mathfrak{P}_1$ prost ideal od L nad $\mathfrak{p}$, te $\mathfrak{P}_2$ prost ideal od K nad $\mathfrak{P}_1$, te pretpostavimo da je $\mathfrak{P}_2$ nerazgranat nad $\mathfrak{p}$. Tada je $(\mathfrak{P}_2, K/L) = (\mathfrak{P}_2, K/F)^{f(\mathfrak{P}_1/\mathfrak{p})}$.*

Dokaz. Neka je $k(\mathfrak{P}_2) \supseteq k(\mathfrak{P}_1) \supseteq k(\mathfrak{p})$ odgovarajući toranj proširenja konačnih polja. Tada je po definiciji, $f(\mathfrak{P}_1/\mathfrak{p}) = [k(\mathfrak{P}_1) : k(\mathfrak{p})]$, te je Frobenius u $\mathrm{Gal}(k(\mathfrak{P}_2)/k(\mathfrak{P}_1))$ je $f(\mathfrak{P}_1/\mathfrak{p})$-ta potencija Frobeniusa u $\mathrm{Gal}(k(\mathfrak{P}_2)/k(\mathfrak{p}))$. Sada tvrdnja slijedi iz činjenice da je $\mathrm{Gal}(k(\mathfrak{P}_2)/k(\mathfrak{p})) \simeq D(\mathfrak{P}_2/\mathfrak{p})$. □

Lema 49. *Neka su pretpostavke iste kao u prethodnoj lemi, te neka je L Galoisovo nad F. Tada je $(\mathfrak{P}_2, K/F)|_L = (\mathfrak{P}_1, L/F)$.*

Dokaz. Automorfizam $\sigma = (\mathfrak{P}_2, K/F)$ zadovoljava $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}_2}$ za svaki $\alpha \in \mathcal{O}_K$. Restrikcijom na L, vrijedi $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}_2}$ za svaki $\alpha \in \mathcal{O}_L$, pa svakako vrijedi i $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}_1 = \mathfrak{P}_2 \cap \mathcal{O}_L}$. □

Propozicija 50. *Za proizvoljno Abelovo proširenje PAB K/F, neka je m produkt svih razgranatih ideala. Vrijedi*

$$N_{K/F}(I_m) \leq Ker(\theta_{K/F} : I_m \to \mathrm{Gal}(K/F)).$$

Dokaz. Vidi [6, Proposition 3.3. i Corolary 3.4. i njihove dokaze]. □

Poglavlje 8

Produktna formula

Hilbert je krajem 19. stoljeća gledao kako poopćiti Gaussov zakon kvadratnog reciprociteta.

Definicija. Neka je K PAB i v mjesto od K. Za $a, b \in K^\times$ definiramo Hilbertov simbol $(a, b)_v$

$$(a,b)_v = \begin{cases} 1, & \text{ako je } a = x^2 - by^2 \text{ rješivo u } K_v \\ -1, & \text{inače.} \end{cases}$$

Dobio je sljedeće poopćenje.

Teorem 51 (Produktna formula)**.** *Vrijedi*

$$\prod_{v \in V_F} (a,b)_v = 1.$$

Napomena. Primjetimo da je ovo poiopćenje Gaussovog zakona o reciprocitetu. Naime, neka su p i q pozitivni neparni prosti brojevi; imamo

- $(p,q)_\infty = 1$,
- $(p,q)_r = 1$ za svaki neparni prost broj $r \neq p, q$,
- $(p,q)_q = \left(\frac{p}{q}\right)$,
- $(p,q)_p = \left(\frac{q}{p}\right)$,
- $(p,q)_2 = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Poglavlje 9

Iskazi teorema (globalne) teorije polja klasa

Sada imamo definicije koje nam omogućuju da iskažemo dokaze teorma teorije polja klasa. U ovom poglavlju ćemo slijediti [3].

Otkada smo uveli pojam modulusa možemo proširiti definiciju zraka modulo $\mathfrak{m}$.

Definicija. Neka je $\mathfrak{m}$ modulus nekog polja K. Tada je $P_\mathfrak{m}$ grupa glavnih razlomljenih ideala u K oblika (α/β) takvih da je

- (α) i (β) su relativno prosti s $\mathfrak{m}$,
- $\alpha \equiv \beta \pmod{\mathfrak{m}}$,
- $\sigma(\alpha/\beta) > 0$ za svako realno mjesto σ koje dijeli $\mathfrak{m}$.

Ako je $\gamma = \alpha/\beta$ takav da zadovoljava gornja svojstva, pišemo $\gamma \equiv 1 \pmod{\mathfrak{m}}$. Grupu $P_\mathfrak{m}$ nazivamo *zraka modulo* $\mathfrak{m}$.

Proširimo definicije grupa ideala s modulusom $\mathfrak{m}$, grupa klasa ideala s modulusom $\mathfrak{m}$, te grupe klasa zraka.

Definicija. Svaku grupu $P_\mathfrak{m} \leq H \leq I_\mathfrak{m}$ nazivamo *grupu ideala s modulusom* $\mathfrak{m}$, te kvocijent $I_\mathfrak{m}/H$ nazivamo *generaliziranom grupom klasa ideala.*

Definicija. *Grupa klasa zraka od* $\mathfrak{m}$ je

$$\mathcal{R}_\mathfrak{m} = I_\mathfrak{m}/P_\mathfrak{m}.$$

Prvo proširujemo definiciju Artinovog preslikavanja.

Definicija. Neka je L/K Abelovo proširenje PAB, te $\mathfrak{m}$ modulus djeljiv sa svim prostim idealima u K koji se granaju u L. Preslikavanje

$$\theta_{L/K,\mathfrak{m}} : I_m \to \mathrm{Gal}(L/K), \quad \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_t^{n_t} \mapsto \prod_{i=1}^{t} (\mathfrak{p}_i, L/K)^{n_i}.$$

se zove *Artinovo preslikavanje*.

Napomena. Napomenimo činjenicu koja je možda očita ali je nismo eksplicitno spomenuli: neki prost ideal je u jezgri Artinovog preslikavanja $\theta_{L/K,\mathfrak{m}}$ ako i samo ako se u potpunosti cijepa u L/K.

Teorem 52 (Artinov teorem reciprociteta)**.** *Neka je L/K Abelovo proširenje PAB, te neka je $\mathfrak{m}$ modulus djeljiv s svim prostim idealima, konačnim ili beskonačnim, koji se granaju u L. Tada je*

1) *Artinovo preslikavanje $\theta_{L/K,\mathfrak{m}}$ surjektivno,*

2) *Ako su potencije konačnih prostih ideala u $\mathfrak{m}$ dovoljno velike, imamo da je $\ker\theta_{L/K,\mathfrak{m}}$ grupa klasa idela za modulus $\mathfrak{m}$, tj.*

$$P_{\mathfrak{m}} \leq \ker\theta_{L/K,\mathfrak{m}} \leq I_{\mathfrak{m}}.$$

Dokaz. [4, Chapter V, Theorem 5.7.] □

Direktna posljedica Artinovog teorema reciprociteta je da je

$$I_{\mathfrak{m}}/\ker\theta_{L/K,\mathfrak{m}} \simeq \mathrm{Gal}(L/K).$$

Dakle svako Abelovo proširenje L od K ima Galoisovu grupu koja je generaliziranu grupa klasa ideala za neki $\mathfrak{m}$.

Očiti nedostatak Artinovog teorema reciprociteta je da modulus $\mathfrak{m}$ za koji je $\ker\theta_{L/K}$ nije jedinstven. Neka je $P_{\mathfrak{m}} \leq \ker\theta_{L/K,\mathfrak{m}}$ i neka je $\mathfrak{n}$ neki modulus djeljiv s $\mathfrak{m}$. Po definiciji je $P_{\mathfrak{m}}$ skup svih α takvih da je $\alpha \equiv 1 \pmod{\mathfrak{m}}$, te je očito je $P_{\mathfrak{n}} \subseteq P_{\mathfrak{m}}$, te iz $P_{\mathfrak{m}} \leq \ker\theta_{L/K,\mathfrak{m}}$ slijedi da je $P_{\mathfrak{n}} \leq \ker\theta_{L/K,\mathfrak{n}}$, pa vrijedi $P_{\mathfrak{n}} \leq \ker\theta_{L/K,\mathfrak{n}}$, pa je $\mathrm{Gal}(L/K)$ generalizirana grupa klasa idela i za modulus $\mathfrak{n}$. Dakle slijedi da ima beskonačno mnogo modulusa koji zadovoljavaju Artinov teorem reciprociteta.

Međutim, postoji "najbolji" modulus, što vidimo iz sljedećeg teorema.

Teorem 53 (Teorem o konduktoru)**.** *Neka je L/K Abelovo proširenje. Postoji modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ takav da je*

1) *Prost ideal od K, konačan ili beskonačan, se grana u L ako i samo ako dijeli $\mathfrak{f}$.*

2) *Neka je $\mathfrak{m}$ modulus djeljiv s svim prostim idealima (konačnim i beskončnim) koji se granaju u L. Tada je $\ker\theta_{L/K,\mathfrak{m}}$ generalizirana grupa ideala za $\mathfrak{m}$ ako i samo ako $\mathfrak{f}$ dijeli $\mathfrak{m}$.*

Modulus $\mathfrak{f}$ se naziva konduktor od L/K.

Dokaz. [4, Chapter V, Theorem 12.7] □

Zadnji od glavnih teorema teorije polja klasa nam kaže da je svaka generalizirana grupa ideala od K zapravo izomorfna Galoisovoj grupi nekog proširenja L/K.

Teorem 54 (Teorem o egzistenciji). *Neka je $\mathfrak{m}$ modulus od K, te neka je H generalizirana grupa ideala, tj. $P_{\mathfrak{m}} \leq H \leq I_{\mathfrak{m}}$. Tada postoji jedinstveno Abelovo proširenje L od K, čiji svi razgranati prosti ideali (konačni i beskonačni) dijele $\mathfrak{m}$, takvo da ako je*

$$\theta_{L/K,\mathfrak{m}} : I_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$$

Artinovo preslikavanje, tada je $H = \ker \theta_{L/K,\mathfrak{m}}$.

Definicija. Za polje iz teorema o egzistenciji kažemo da je L *polje klasa* od H.

Napomena. Ova definicija polja klasa proširuje prethodnu. Povijesno, ovo je Takagijeva definicija polja klasa, dok je ona prethodna Weberova.

Napomena. Artinov teorem reciprociteta nam kaže da je svako Abelovo proširenje polje klasa neke generalizirane grupe ideala.

Ovaj teorem nam dopušta dokaz egzistencije Abelovih proširenja s točno određenom Galoisovom grupom, te s restrikcijama na grananje prostih ideala.

Pokažimo sada neke posljedice ovih važnih teorema. Prvo ćemo trebati sljedeći korolar teorema o egzistenciji.

Korolar 55. *Neka su L i M Abelova proširenja od K. Tada je $L \subseteq M$ ako i samo ako postoji modulus $\mathfrak{m}$, djeljiv s svim prostim idealima od K koji se granaju ili u L ili u M takav da*

$$P_{\mathfrak{m}} \leq \ker \theta_{M/K,\mathfrak{m}} \leq \ker \theta_{L/K,\mathfrak{m}}.$$

Dokaz. Mi ćemo dokazati samo jedan smjer. Pretpostavimo da je $L \subseteq M$ i neka je $r : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ restrikcija. Po Artinovom teroemu o reciprocitetu postoji modulus $\mathfrak{m}$ takav da su i $\ker \theta_{M/K,\mathfrak{m}}$ i $\ker \theta_{L/K,\mathfrak{m}}$ generalizirane grupe ideala. Prema Lemi 49, $r \circ \theta_{M/K,\mathfrak{m}} = \theta_{L/K,\mathfrak{m}}$, te je tada $\ker \theta_{M/K,\mathfrak{m}} \leq \ker \theta_{L/K,\mathfrak{m}}$. Dokaz drugog smjera se može naći u [3, Corollary 8.7., p. 147.]

□

Sada možemo dokazati Kronecker-Weberov teorem pomoću teorije polja klasa.

Teorem 56 (Kronecker-Weber). *Neka je L Abelovo proširenje od $\mathbb{Q}$. Tada postoji $m \in \mathbb{N}$ takav da je $L \subseteq \mathbb{Q}(\zeta_m)$.*

Dokaz. Po Artinovom teoremu reciprociteta, postoji modulus $\mathfrak{m}$ takav da je $P_{\mathfrak{m}} \subseteq \ker \theta_{L/\mathbb{Q},m}$. Neka je m konačan dio od $\mathfrak{m}$. tj. $\mathfrak{m} = m$ ili $\mathfrak{m} = m\infty$. Međutim, znamo da je $P_{\mathfrak{m}} = \ker \theta_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}$, pa je $P_{\mathfrak{m}} = \ker \theta_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}} \subseteq \ker \theta_{L/\mathbb{Q},m}$. Tada po prethodnom korolaru vrijedi $L \subseteq \mathbb{Q}(\zeta_m)$. □

Napomena. Ako uzmemo $K = \mathbb{Q}$, tada će konduktor $\mathfrak{f}(L/\mathbb{Q})$ biti najmanji m takava da je $L \subseteq \mathbb{Q}(\zeta_m)$.

Napomena. Primjetimo da teoremi TPK daju generalizaciju Kronecker-Weberovog teorema. Postoji sljedeća generalizacija Kronecker-Weberovog teorema: za svaki modulus $\mathfrak{m}$, postoji konačno Abelovo proširenje $K_{\mathfrak{m}}$ takva da je svako konačno Abelovo proširenje sadržano u nekom $K_{\mathfrak{m}}$. Ova polja su definirana kroz teroemu o egzistenciji - definiramo da je $K_{\mathfrak{m}}$ polje klasa od $P_{\mathfrak{m}}$. Ovdje polja $K_{\mathfrak{m}}$ igraju ulogu koju imaju $\mathbb{Q}(\zeta_m)$ za $\mathbb{Q}$.

Primjetimo da međutim teoremi TPK ne govore kako konstruirati, tj. kako eksplicitno izgledaju polja $K_{\mathfrak{m}}$.

Definicija. Polje klasa $K_{\mathfrak{m}}$ od $P_{\mathfrak{m}}$ se naziva *polje klasa zrake modulo* $\mathfrak{m}$.

Napomena. Neka je $K \neq \mathbb{Q}$ PAB. Pokažimo da postoje abelova proširenja L/K koja nisu sadržana u $K(\zeta_n)$ ni za jedan n. Neka je $p \in \mathbb{Z}$ neki prost broj koji se potpuno cijepa u K, te $\mathfrak{p}$ neki ideal od K nad $(p) \subseteq \mathbb{Z}$. Iskoristit ćemo sljedeću činjenicu (koju ostavljamo za vježbu): Ako se $\mathfrak{p}$ grana u $K(\zeta_m)/K$, tada se svaki ideal od K nad (p) grana u $K(\zeta)/K$. Konstuirajmo L takav da nije sadržan ni u jednom ciklotomskom proširenju od K. Neka je $\alpha \in \mathfrak{p}$, takav da $\alpha \notin \mathfrak{p}^2$, te takav da je $\alpha \equiv 1 \pmod{\mathfrak{q}}$ za sve $\mathfrak{q} \neq \mathfrak{p}$ nad p. Uzmimo da je $L = K(\sqrt{\alpha})$. Tada promatrajući $\Delta_{L/K}$ vidimo da se $\mathfrak{p}$ grana u L/K, dok se $\mathfrak{q}$ ne granaju, dakle zaključujemo da $L \not\subseteq K(\zeta_m)$.

Sažmimo glavne teoreme globalne teorije polja klasa u jednom teoremu (uz malo reformulacije).

Teorem 57 (Teoremi teorije polja klasa)**.** *Neka je K polje algebarskih brojeva.*

(1) (Egzistencija) Za svaku grupi idela H postoji polje klasa K.

(2) (Izomorfizam) Za grupu ideala H s modulusom $\mathfrak{m}$ i poljem klasa L, vrijedi $\mathrm{Gal}(L/K) \simeq I_{\mathfrak{m}}/H$*.*

(3) (Potpunost) Za svako konačno Abelovo proširenje K je polje klasa.

(4) (Usporedivost) Ako su H_1 i H_2 grupe ideala s istim modulusom $\mathfrak{m}$ i imaju polja klasa L_1 i L_2 (unutar istog algebarskog zatvorenja $\overline{K}$), tada je $L_1 \subseteq L_2 \iff H_2 \subseteq H_1$.

(5) (Konduktor) Za svaku konačno Abelovo proširenje L/K, mjesta od K koja se pojavljuju u konduktoru od $\mathfrak{f}(L/K)$ su točno ona koja se granaju u L/K.

(6) (Dekompozicija) Ako je H grupa ideala s modulusom $\mathfrak{m}$ i poljem klasa L/K tada je svaki $\mathfrak{p} \nmid \mathfrak{m}$ nerazgranat u L i stupanj inercije $\mathfrak{f}(\mathfrak{P}/\mathfrak{p})$ za neki (tj. svaki) ideal $\mathfrak{P}$ nad $\mathfrak{p}$ je jednak redu od $\mathfrak{p}$ u $I_{\mathfrak{m}}/H$.

9.1 Hilbertovo polje klasa

Hilbert je znao dokazati produktnu formulu za $\mathbb{Q}$, ali nije za općenita PAB. Problem su mu predstavljala PAB koja imaju svugdje nerazgranata kvadratna proširenja, te je tada počeo promatrati svugdje nerazgranata abelova proširenja. Napomenimo da je jedan od razloga zašto je Hilbertov dokaz Kronecker-Weberovog teorema "radio" je zato što nema svugdje nerazgranatih Abelovih proširenja od $\mathbb{Q}$.

Teorem 58 (Hilbert 1898. izrekao kao slutnju). *Za svako PAB K postoji jedinstveno konačno proširenje K'/K takvo da je*

1. *K'/K je Galoisovo i $\mathrm{Gal}(K'/K) \simeq Cl_K$,*
2. *K'/K je nerazgranato (u konačnim i beskonačnim mjestima) i svako Abelovo proširenje s ovim svojstvom je potpolje od K',*
3. *Za svaki prost ideal $\mathfrak{p}$ od K, stupanj inercije $f(\mathfrak{P}/\mathfrak{p})$ za svaki ideal $\mathfrak{P}$ od K' nad $\mathfrak{p}$ je red klase od $\mathfrak{p}$ u Cl_K,*
4. *svaki ideal od K je glavni u K'*

Hilbert je dokazao slutnu za $h(K) = 2$, a Furtwangler općenito 1907 (1. i 2.), 1911 (3.) i 1930. (4.).

Definicija. Polje iz Slutnje 58 se zove *Hilbertovo polje klasa.*

Napomena. Alternativna definicija Hilbertovog polja klasa je da je to polje klasa zrake modulo $\mathfrak{m} = 1$.

Primjer 19. Promotrimo $K = \mathbb{Q}(\sqrt{3})$, $L = K(i)$. Promtorimo grananje prostih ideala u L/K. Jedini koji dolaze u obzir da se granaju (po Propoziciji 40) su ideali od K nad 2 i 3, tj. $(1+\sqrt{3})$ i $(\sqrt{3})$. Možemo zaključiti da se $(\sqrt{3})$ ne grana u L, pošto bi u suprotnom 3 bio potpuno razgranat u L, te bi se tada morao granati u $\mathbb{Q}(i)/\mathbb{Q}$, što nije istina. Da bi dokazali da je $(1+\sqrt{3})$ ne razgranat u L, primjetimo sljedeće: kad bi bio, tada bi se 2 potpuno granao u L, a time i u svim potpoljima. Međutim 2 se ne grana u $\mathbb{Q}(\sqrt{-3})$. Dakle ni jedan prost ideal od K se ne grana u L. Međutim realna mjesta od K se granaju u L, pa L/K nije nerazgranato.

Primjer 20. Nađimo Hilbertovo polje klasa L od $K = \mathbb{Q}(\sqrt{-5})$. Primjetimo sljedeće: $h_K = 2$, dakle Hilbertovo polje klasa od K je kvadratno proširenje od K, dakle oblika $L = K(\sqrt{\delta})$. Također, primjetimo da $\mathbb{Q}$ nema nerazgranato proširenje, tako da svi prosti brojevi iz $\mathbb{Q}$ koji se granaju u L se moraju već granati u K, dakle to su 2 i 5. Dakle, probamo s $L = K(i)$, vidimo koristeći argumentaciju kao i prije da su ideali nad 2 i 5 nerazgranati u L, te zaključujemo da je L Hilbertovo polje klasa.

Primjer 21. Vidi [2, Example 4.2].

Dokažimo postojanje Hilbertovog polja klasa karakteriziranog sa svojstvom (1) iz Slutnje 58 korištenjem teorije polja klasa. Uzmimo modulus $\mathfrak{m} = 1$ i grupu ideala $H = P_K$, tj podgrupu glavnih ideala. Sada teorem o egzistenciji kaže da postoji jedinstveno Abelovo proširenje L od K, za koje vrijedi (pošto je $P_{\mathfrak{m}} = P_K$, i $I_m = I_K$, skup svih razlomljenih ideala),

$$P_K = \ker \theta_{L/K,1}.$$

Primjetimo da je po teoremu o egzistenciji, polje L s tim svojstvom jedinstveno, te da je to polje svugdje nerazgranato pošto je $\mathfrak{m} = 1$. Pošto je Artinovo preslikavanje surjektivno, po Artinovom teoremu reciprociteta, vrijedi

$$Cl_K = I_K/P_K \simeq \mathrm{Gal}(L/K).$$

Dokažimo sada da je to i maksimalno nerazgranto Abelovo proširenje od K.

Teorem 59. *Polje L iz prethodne diskusije je maksimalno nerazgranto Abelovo proširenje od K.*

Dokaz. Već smo vidjeli da je L nerazgranato. Neka je M bilo koje drugo nerazgranato Abelovo proširenje. Po teoremu o konduktoru, imamo da je konduktor $\mathfrak{f}(M/K) = 1$, pošto se prost ideal grana ako i samo ako dijeli konduktor. Također po teoremu o konduktoru imamo da je $\ker \theta_{M/K,1}$ generalizirana grupa ideala za modulus 1, tj.

$$P_K \subseteq \ker \theta_{M/K,1}.$$

Dakle,

$$\ker \theta_{L/K,1} = P_K \subseteq \ker \theta_{M/K,1},$$

pa je po Korolaru 55, $M \subseteq L$. □

9.2 Neke posljedice teorema teorije polja klasa

Primjetimo da nam teorem o konduktoru govori o povezanosti konduktora i diskriminante, tj. da ih isti prosti ideali dijele. Točnije imamo sljedeći teorem (vidite sličnost sa poglavljem o karakterima).

Teorem 60. *Neka je L/K Abelovo proširenje PAB i neka je $\mathfrak{m}$ neki modulus za kojeg je L polje klasa nad K (za neku generalizirranu grupu ideala H). Za svaki karakter χ od $I_\mathfrak{m}/H$, neka je L_χ polje klasa asocirano s $\ker \chi$ i neka je $\mathfrak{f}_\chi$ konduktor od L_χ/K. Tada je diskriminanta od L/K jednaka*

$$|\Delta_{L/K}| = \prod_\chi \mathfrak{f}_\chi^k,$$

gdje je $\mathfrak{f}_\chi^k$ konačan dio od $\mathfrak{f}_\chi$.

Koristeći terminologiju iz poglavlja o Dirichletovim karakterima, polje asocirano L_χ nekom karakteru χ (ili podgrupi karaktera H) će biti polje klasa od $\ker \chi$ (tj. od H).

Primjer 22. Odredimo $\Delta_{\mathbb{Q}(\zeta_5)/\mathbb{Q}}$. Znamo i da je $\mathbb{Q}(\zeta_5)$ polje zraka klasa za modulus $\mathfrak{m} = 5\infty$, tj. polje klasa za podgrupu ideala $P_\mathfrak{m}$ koja se sastoji od (α), gdje je $\alpha \equiv 1 \pmod 5$. Očito je $I_\mathfrak{m}/P_\mathfrak{m} \simeq (\mathbb{Z}/5\mathbb{Z})^\times$. Za karaktere od $I_\mathfrak{m}/H \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ se lako vidi: trivijalni karakter ima $\ker_\chi = I_\mathfrak{m}$, pa je njegov konduktor 1 (ovdje je $L_\chi = \mathbb{Q}$), karakter χ reda 2 ima $L_\chi = \mathbb{Q}(\sqrt{5})$, pa je njegov $\mathfrak{f}_\chi^k = 5$, dok za karaktere reda 4 vrijedi $L_\chi = \mathbb{Q}(\zeta_5)$, te je $\mathfrak{f}_\chi^k = 5$. Dakle $\Delta_{\mathbb{Q}(\zeta_5)/\mathbb{Q}} = 1 \cdot 5 \cdot 5 \cdot 5 = 5^3$.

Primjetimo još jednu posljedicu dekompozicijskog teorema za $\mathbb{Q}$. Grupe $I_{\mathfrak{m}}/H$ su podgrupe od $(\mathbb{Z}/m\mathbb{Z})^{\times}$. Sada nam dekompozicijski teorem zapravo govori da je cijepanje prostih u nekom proširenju $K/\mathbb{Q}$ zadano kongruencijskim uvjetima ako je K Abelovo proširenje (ili ekvivalentno je potpolje od $\mathbb{Q}(\zeta_m)$ za neki $\mathfrak{m}$.)

Primjer 23. Odredimo koji se ideali cijepaju u $\mathbb{Q}(\sqrt{6})$ pomoću TPK. Prvo izračunamo da je konduktor od $K = \mathbb{Q}(\sqrt{6})$ jednak diskriminanti (ovo vrijedi za sva kvadratna polja) $\mathfrak{f} = 24$. Dakle $\mathbb{Q}(\sqrt{6}) \subseteq \mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\sqrt{-3}, \sqrt{2}, i)$. Tražimo $H \leq I_{\mathfrak{f}}$ takav da he $\mathbb{Q}(\sqrt{6})$ njegovo polje klasa. Očito je $I_{\mathfrak{f}}/H \simeq \mathrm{Gal}(K/\mathbb{Q})$ grupa reda 2, dakle $I_{\mathfrak{f}}/H$ je kvocijenta grupa reda 2 u $I_{\mathfrak{f}}/P_{\mathfrak{f}} \simeq (\mathbb{Z}/24\mathbb{Z})^{\times}$. Koriteći rezultate iz poglavlja o karakterima, možemo vidjeti da je $\mathbb{Q}(\sqrt{6})$ fiksno polje od $\{\sigma_1, \sigma_5, \sigma_{19}, \sigma_{23}\}$. Zaključujemo da je $\ker \chi = H = \{1, 5, 19, 23\} \leq (\mathbb{Z}/24\mathbb{Z})^{\times}$, a $H = \ker \theta_{K/\mathbb{Q},\mathfrak{f}}$, dakle skup svih idela koji se cijepaju u K. Dakle, p se cijepa u $\mathbb{Q}(\sqrt{6})$ ako i samo ako je $p \equiv 1, 5, 19, 23 \pmod{24}$.

Mogli smo i doći do vrijednosti kada se p cijepa i koristeći da je kopnduktor točno 24. Dakle, cijepanje se mora dogoditi u pola klasa $(\mathbb{Z}/24\mathbb{Z})^{\times}$, te mora taj uvjet biti zadan modulo 24, i nijednim manjim modulom. Analogno možemo vidjeti:

$$p \text{ se cijepa u } \mathbb{Q}(\sqrt{-3}) \iff p \equiv 1 \pmod{3},$$
$$p \text{ se cijepa u } \mathbb{Q}(\sqrt{-1}) \iff p \equiv 1 \pmod{4},$$
$$p \text{ se cijepa u } \mathbb{Q}(\sqrt{2}) \iff p \equiv \pm 1 \pmod{8},$$
$$p \text{ se cijepa u } \mathbb{Q}(\sqrt{3}) \iff p \equiv \pm 1 \pmod{12}.$$
$$p \text{ se cijepa u } \mathbb{Q}(\sqrt{-2}) \iff p \equiv 1, 3 \pmod{8},$$
$$p \text{ se cijepa u } \mathbb{Q}(\sqrt{-6}) \iff p \equiv 1, 5, 7, 11 \pmod{24}.$$

Tvrdnja da ako je cijepanje zadano "kongruencijskim uvjetima", da je tada proširenje Abelovo, vrijedi i općenito, ne samo kada je bazno polje $K = \mathbb{Q}$. Da bi to dokazali, dokažimo prvo poopćenje Bauerovog teorema.

Teorem 61 (Bauer). *Neka su L_1 i L_2 proširenja PAB od K, gdje je L_2/K Galosiovo. Tada je $L_1 \subseteq L_2$ ako i samo ako je $S_{L_2/K} \subseteq S_{L_1/K}$ osim za konačno mnogo iznimaka.*

Dokaz. Prvo dokažimo sljedeću tvrdnju: ako je $\widetilde{L}_1$ Galoisovo zatvorenje od L_1 nad K tada je $S_{L_1/K} = S_{\widetilde{L}_1/K}$. Možemo to vidjeti iz činjenice da se prost ideal $\mathfrak{p}$ od K cijepa u L_1 na isti način na koji se cijepa i u $\sigma(L_1)$ za svaki $\sigma \in \mathrm{Gal}(\widetilde{L}_1/K)$. S druge strane, $\widetilde{L}_1$ je kompozit svih $\sigma(L_1)$, pa vidimo da će se $\mathfrak{p}$ potpuno cijepati u $L_1 \iff \mathfrak{p}$ se potpuno cijepa u svim $\sigma(L_1) \iff \mathfrak{p}$ se potpuno cijepa u $\widetilde{L}_1$. Dakle, $S_{L_1/K} = S_{\widetilde{L}_1/K}$.

Sada imamo, pošto je L_2 Galoisovo nad K, imamo da je $L_1 \subseteq L_2$ ako i samo ako je $\widetilde{L}_1 \subseteq L_2$, pa po Bauerovom teoremu, to vrijedi ako i samo ako $S_{L_1/K} = S_{\widetilde{L}_1/K} \supseteq S_{L_2/K}$. $\square$

Teorem 62. *Neka je L/K proširenje PAB, te neka je $\mathfrak{m}$ modulus od K, te S konačan skup prostih ideala od K koji sadrži sve $\mathfrak{p}|\mathfrak{m}$. Neka za svaki $\mathfrak{p} \notin S$ vrijedi da se $\mathfrak{p}$ potpuno cijepa u L ovisno o tome u kojoj je klasi od $I_\mathfrak{m}/P_\mathfrak{m}$. Tada je L/K Abelovo.*

Dokaz. Neka je $\mathfrak{m}$ kao u pretpostavci i neka je $K_\mathfrak{m}$ polje klasa zraka od $\mathfrak{m}$, tj. polje klasa od $P_\mathfrak{m}$. Dakle imamo da se $\mathfrak{p} \nmid \mathfrak{m}$ potpuno cijepa u $K_\mathfrak{m}$ ako i samo ako je $\mathfrak{p}$ u $P_\mathfrak{m}$. Pogledajmo kompozit $LK_\mathfrak{m}/K$. Uzmimo $\mathfrak{q} \notin S$ prost ideal od K takava da se $\mathfrak{q}$ potpuno cijepa u $LK_\mathfrak{m}/K$ (takvih očito postoji beskonačno mnogo). Pošto se $\mathfrak{q}$ potpuno cijepa u $K_\mathfrak{m}/K$, imamo da je $\mathfrak{q} \in P_\mathfrak{m}$. Ideal $\mathfrak{q}$ se cijepa i u L, a pošto je cijepanje u L određeno time u kojoj je klasi u $I_\mathfrak{m}/P_\mathfrak{m}$ ideal $\mathfrak{q}$, imamo da se ideali iz $P_\mathfrak{m}$ cijepaju u L.

Dakle $S_{K_\mathfrak{m}/K} \subseteq S_{L/K}$, osim za konačno mnogo $\mathfrak{p}$ koji dijele $\mathfrak{m}$. Dakle po prethodnom teoremu imamo da je $L \subseteq K_\mathfrak{m}$, pa je L Abelovo. □

9.3 Čebotarevljev teorem o gustoći

Čebotarevljev teorem će biti najmanji zajednički višekratnik Dirichletovog teorema o aritmetičkim progresijama i Frobeniusovog teroema kojeg ćemo opisati. Pitamo se kako će se asimptotski neki ireducibilni polinom $f(x)$ faktorizirati modulo p? Na primjer, možemo promotriti polinom $x^4 - x^3 + x^2 - x + 2$, te kako se on faktorizira modulo sve proste brojeve do 1000. Dobijemo da se faktorzira kao produkt linearnih polinoma u 4% slučajeva, produkta faktora stupanja $1, 1, 2$ u $25,5\%$, $2, 2$ u $12,5\%$, $1, 3$ u 31%, te ostaje ireducibilan u 27%.

Odgovor na ovo pitanje daje Frobeniusov teorem. Označimo s $\mathrm{Gal}(f)$ Galiosovu grupu polja cijepanja od f nad $\mathbb{Q}$. Grupu $\mathrm{Gal}(f)$ možemo promatrati kao podgrupu od S_n koja djeluje na korijene od f.

Teorem 63 (Frobenius). *Gustoća skupa prostih brojeva p za koji se polinom $f \in \mathbb{Z}[x]$ faktorizira modulo p kao produkt ireducibilnih faktora stupnja $n_1, n_2, \dots n_i$ postoji i jednak je $1/\mathrm{Gal}(f)$, pomonoženo s brojem elemenata $\sigma \in \mathrm{Gal}(f)$ koji imaju dekompoziciju u disjunktne cikluse reda $n_1, \dots n_i$.*

Sjetimo se Dedekindovog teorema o faktorizaciji:

Teorem 64 (Dedekind). *Neka je K PAB i $\alpha \in \mathcal{O}_K$ takav da je $K = \mathbb{Q}(\alpha)$. Neka je $f(t) \in \mathbb{Z}[t]$ minimalni polinom od α. Tada za svaki prost p koji ne dijeli $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, zapišimo*

$$f(t) \equiv \pi_1(t)^{e_1} \cdots \pi_g(t) \pmod p,$$

gdje su $\pi_i(t)$ različiti ireducibilni elementi od $\mathbb{F}_p[t]$. Tada se $(p) = p\mathcal{O}_K$ faktorizira kao

$$(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g},$$

te vrijedi da je $f(\mathfrak{p}_i/p) = \deg(\pi_i)$.

Pri promatranju gustoće nekog tipa cijepanja, možemo zanemariti one p koji dijele $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, pošto je njih konačno mnogo. Dakle Frobeniusov teorem nam govori i nešto o cijepanju prostih u proširenjima PAB.

Sjetimo se da smo za Galoisovo proširenje L/K, za $\mathfrak{P}/\mathfrak{p}$ definirali Frobenius $(\mathfrak{P}, L/K)$ kao prasaliku od $x \mapsto x^p$ pri prirodnom izomorfizmu

$$\mathrm{Gal}(L/K)/I(\mathfrak{P}/\mathfrak{p}) \simeq D(\mathfrak{P}/\mathfrak{p}).$$

Do sada smo gledali samo slučaj kada je $Gal(L/K)$ Abelova.

Sjetimo se da je za $(\tau\mathfrak{P}, L/K) = \tau(\mathfrak{P}, L/K)\tau^{-1}$ za $\tau \in \mathrm{Gal}(L/K)$. Primjetimo da je tada

$$\{(\tau\mathfrak{P}, L/K) : \tau \in \mathrm{Gal}(L/K)\} = \{(\mathfrak{P}, L/K) : \mathfrak{P}|\mathfrak{p}\} =: (\mathfrak{p}, L/K)$$

klasa konjugacije od $\mathrm{Gal}(L/K)$.

Teorem 65. *(Čebotrevov teorem o gustoći) Neka je L/K Galoisovo proširenje PAB i neka je C klasa konjugacije grupe G. Tada je Dirichletova gustoća prostih ideala $\mathfrak{p}$ od K takvih da je $(\mathfrak{p}, L/K) = C$ jednaka $\frac{|C|}{|\mathrm{Gal}(L/K)|}$.*

Napomena. Primjetimo da je Dirichletov teorem o Aritmetičkim progresijama direktno slijedi iz Čeborarevljevog teroema o gustoći: neka su $a, n \in \mathbb{N}$, $(a, n) = 1$. Kao i uvijek, poistovjetimo elemente od $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ s $(\mathbb{Z}/n\mathbb{Z})^\times$, dakle a odgovoara σ_a. Pitamo se za koje proste brojeve p je Frobenius $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q}) = a$? Frobenius u $p \nmid n$ je preslikavanje takvo da je $\sigma(\alpha) = \alpha^p \pmod{\mathfrak{p}}$ za $\mathfrak{p}|p$ i sve $\alpha \in \mathbb{Z}[\zeta_n]$. Dakle, Frobenius mora zadovoljavati da je $\sigma(\zeta_n^k) = \sigma(\zeta_n^{pk}) \pmod{\mathfrak{p}}$ za sve k. Dakle, imamo da je Frobenius u p jednak σ_p. Dakle $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q}) = \sigma_a$ ako i samo ako je $p \equiv a \pmod{n}$. Čebotarevljev teorem nam kaže da takvih p-ova ima beskonačno mnogo.

Napomena. Po čemu je jači Čebotarevljev teorem od Frobeniusovog? Frobeniusov teorem nam govori o tome koliko često će Frobenius biti u nekom *podijeljenju* $G := \mathrm{Gal}(f)$. Kažemo da su dva elementa grupe G u istom podijeljenju, ako su cikličke grupe koje generiraju konjugirane u G. Pogledajmo primjer cikličke grupe $\mathbb{Z}/4\mathbb{Z}$ s 4 elementa. Tada su $1, 3$ u istom podijeljenju, dok nisu u istoj klasi konjugacije.

Promotrimo proširenje $\mathbb{Q}(\zeta_5)/\mathbb{Q}$; znamo da je $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$. Frobeniusov teorem nam kaže da će u 50% slučajeva Frobenius biti σ_2 ili σ_4 (ali ne znamo koji), tj. da će p biti inertan, tj. polinom f će biti ireducibilan. Ostali slučajevi se pojavljuju asimptotski za $1/4$ prostih brojeva. S druge strane Čebotarevljev teorem nam kaže da se svi Frobeniusi pojavljuju u $1/4$ slučajeva.

Primjer 24. Pogledajmo što nam kaže Čebotarevljev teorem o gustoći za $L/\mathbb{Q}$, gdje je $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$. Ima tri klase konjugacije od S_3 : $\{id\}, \{(12), (13), (23)\}$ i $\{(123), (132)\}$. Ako je $(p, L/\mathbb{Q}) = \{id\}$, imamo pošto se id preslikava u generator of $[\mathbb{F}_{p^f} : \mathbb{F}_p]$, da je $f = 1$. Pošto pričamo o gustoći i $e = 1$ osim za konačno mnogo p-ova, možemo ignorirati one za koje je $e \neq 1$. Dakle $f = 1$, tj. p se potpuno cijepa za $1/6$ prostih brojeva. Za $\{(12), (13), (23)\}$ vidimo da će Frobenius biti reda 2, pa je $f = 2, r = 3$, takvih će prostih brojeva biti $3/6 = 1/2$. Prostih brojeva takvih da je $f = 3$ i $r = 2$ će biti $1/3$. Od prvih 1000 prostih brojeva vrijdei da je $r = 2$ za 334, $r = 3$ za 508 i $r = 6$ za 156, tako da vidimo da dobivamo jako dobru aproximaciju.

Definicija. Neka je L/K proširenje PAB, $\mathfrak{p}$ prost idela u K koji se ne grana u L. Neka je $\mathfrak{p}_L = \mathfrak{P}_1 \dots \mathfrak{P}_r$, gdje proste ideal poredamo tako da je $f(\mathfrak{P}_{i+1}/\mathfrak{p}) \leq (\mathfrak{P}_i/\mathfrak{p})$. Kažemo da je *tip faktorizacije od* $\mathfrak{p}$ *u* L jednak $(f(\mathfrak{P}_1/\mathfrak{p}), \dots f(\mathfrak{P}_r/\mathfrak{p}))$.

Konačno, Čebotarevljev teorem nam govori o cijepanju u Galoisovim proširenjima. Što je sa ne-Galoisovim proširenjima? Tu zapravo dobijemo Frobeniusov teorem.

Propozicija 66. *Neka je $\widetilde{L}$ Galoisovo zatvorenje od L nad K. Pretpostavimo da je $\mathfrak{p}$, ideal od K nerazgranat u L (a time i u $\widetilde{L}$), pošto takvih ima konačno mnogo, te ih možemo zanemariti. Neka je $G := \mathrm{Gal}(\widetilde{L}/K)$, te $H := \mathrm{Gal}(\widetilde{L}/L)$. Neka je $\phi = (\mathfrak{p}, \widetilde{L}/K)$. Tada je tip faktorizacije od $\mathfrak{p}$ jednak duljini ciklusa od ϕ, prikazanog kroz djelovanje na G/H.*

Dokaz. Neka je $L = K(\alpha)$, f minimalni polinom od α i neka je $\mathfrak{p}$ iz K nerazgranat u L. Prvo primjetimo da je $[G : H] = [L : K]$, te da G prirodno djeluje na G/H translacijom, tj. $x \cdot gH = (xg)H$. Dakle ϕ djeluje na skup G/H, te možemo ϕ zapisati kao produkt disjunktnih ciklusa, s obzirom na djelovanje na taj skup. Primjetimo da djelovanje od ϕ na ovaj skup ovisi samo o klasi konjugacije u S_n (to je elementarna činjenica o simetričnim grupama). Faktorizacija od $\mathfrak{p}$ u L je jednaka faktorizaciji od f u $(\mathcal{O}_K/\mathfrak{p})[x]$. Reducirajući sve modulo (ideali nad) $\mathfrak{p}$, dobijemo da su stupnjevi faktora polinoma f mod p jednaki duljini orbita nultočaka od f pri djelovaju od $D(\mathfrak{P}/p)$, tj. kako ϕ djeluje na nultočke of $f \pmod{\mathfrak{p}}$.

S druge strane, pošto α generira L nad K, vidimo da za svaki $\tau \in G$ vrijedi $\tau\alpha = \alpha$ ako i samo ako je $\tau \in H$, pa slijedi da je $\tau_1\alpha = \tau_2\alpha$ ako i samo ako je $\tau_1 H = \tau_2 H$. Dakle vidimo da je djelovanje od ϕ na G/H potpuno identično kao djelovanje od ϕ na konjugate od α. □

Primjer 25. Pogledajmo sljedeći primjer: neka je $\alpha = \sqrt[3]{2}$, $L = \mathbb{Q}(\alpha)$. Tada je $H = \{1, \tau\}$, gdje je τ kompleksno konjugiranje. Neka je σ automorfizam od $\widetilde{L}$ koji šalje α u $\zeta_3\alpha$. Ako numeriramo $\alpha_1 = \alpha, \alpha_2 = \zeta_3\alpha, \alpha_3 = \zeta_3^2\alpha$, σ djeluje kao (123), a τ kao (23). Imamo da je

$$G/H = \{H = \{1, \tau\}, \sigma H = \{\sigma, (12)\}, \sigma^2 H = \{(132), (13)\}.$$

Elementi iz iste klase djeluju jednako na α.

Grupa S_3 ima tri klase konjugacije:

$$C_1 := \{1\}, C_2 = \{(12), (23), (13)\}, C_3 = \{(123), (132)\}.$$

Frobenius je jedna od tih tri klasa konjugacije. Pogledajmo što ako je Frobenius od p jednak C_1. Tada C_1 djeluje trivijalno na G/H, pa svaka orbita ima jedan element, pa se p potpuno cijepa u L (i također u $\widetilde{L}$). Ako je Frobenius C_3, tada Frobenius (tj. svaki element iz C_3) djeluje na G/H tranzitivno, dakle G/H je jedna orbita. Taj prosti ideal dakle ostaje inertan u L. Međutim, redovi elemenata u C_3 su 3, što je jednako redu stupnju inertnosti od prostih ideala u faktorizaciji od $p\mathcal{O}_{\widetilde{L}}$. Dakle p je inertan u $L/\mathbb{Q}$, te se cijepa u $\widetilde{L}/L$.

Ako je Frobenius C_2, tada svaki element iz C_2 djeluje na G/H tako da sui orbite duljina 1 i 2. Dakle imamo $p\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$, gdje je jedan od $\mathfrak{p}$-ova stupnja inertnosti 1, a drugi 2. U $\widetilde{L}_2$ se p cijepa u tri ideala stupnja inertnosti 2.

Primjer 26. Vidi kako se cijepa u poljima stupnja 4 [5, p.11].

9.4 Primjena teorije polja klasa na prste brojeve oblika $p = x^2 + ny^2$

Pogledajmo sljedeće pitanje: za fiksan n, koji se prosti brojevi p mogu zapisati kao $p = x^2 + ny^2$ za cijele brojeve x, y. Tim problemom se bavi sjajna knjga [3].

Prije nego iskažemo rješenje ovog problema, recimo par komentara. Neka je $K = \mathbb{Q}(\sqrt{-n})$, tada je *konduktor* nekog reda $\mathcal{O}$ (to je potprsten konačnog indeksa od $\mathcal{O}_K$) jednak $\mathfrak{f} = [\mathcal{O}_K : \mathcal{O}]$. Primjer takvog reda je $\mathbb{Z}[\sqrt{-n}]$. Primjetimo da je $P_\mathfrak{f}$ generalizirana grupa ideala za modulus $\mathfrak{f}$.

Mi ćemo iskazati rješenje ovog problema.

Teorem 67. *Neka je $n \in \mathbb{N}$ Tada postoji normirani ireducibilni polinom $f_n \in \mathbb{Z}[x]$ takava da za svaki prosti broj $p > 2$ koji ne dijeli ni n ni diskriminantu od f_n, vrijedi*

$$\exists x, y \in \mathbb{Z} \text{ takvi da } p = x^2 + ny^2 \iff \left(\frac{-n}{p}\right) = 1 \text{ i } f_n(x) \text{ mod } p \text{ ima nultočku.}$$

Nadalje, za f_n možemo uzeti minimalni polinom realnog algebarskog broja α za kojeg je $L = K(\alpha)$, gdje je $K = \mathbb{Q}(\sqrt{-n})$, L polje klasa od generalizirane grupe ideala $P_\mathfrak{f}$ s modulusom $\mathfrak{f}$, gdje je $\mathfrak{f}$ konduktor od $\mathbb{Z}[\sqrt{-n}]$. Polinom f_n je stupnja $|I_\mathfrak{f}/P_\mathfrak{f}|$.

Primjetimo da ako je n kvadratno slobodan, te $\mathfrak{n} \not\equiv 3 \pmod 4$, tada je $\mathbb{Z}[\sqrt{-n}] = \mathcal{O}_K$, $\mathfrak{f} = 1$, te je L Hilbertovo polje klasa.

Primjer 27. Neka je $n = 2$. Imamo da je $h_K = 1$, te tada vrijedi da je K Hilbertovo polje klasa samo sebi, dakle

$$p = x^2 + 2y^2 \iff \left(\frac{-2}{p}\right) = 1,$$

to jest

$$p = x^2 + 2y^2 \iff p \equiv 1, 3 \pmod 8.$$

Ovu činjenicu, bez korištenja TPK, je dokazao još Fermat.

Primjer 28. Uzmimo $n = 14$. Vrijedi da je $K = \mathbb{Q}(\sqrt{-14})$ i da $h_K = 4$, te da je Hilbertovo polje klasa od K jednako $K(\alpha)$ gdje je $\alpha = \sqrt{2\sqrt{2} - 1}$. Zaključujemo da je

$$p = x^2 + 14y^2 \iff \left(\frac{-14}{p}\right) = 1 \text{ i postoji } x \text{ takav da } (x^2 + 1)^2 \equiv 8 \pmod{p}.$$

Poglavlje 10

Lokalni Artinov simbol

Mi na kolegiju nećemo raditi lokalnu teoriju polja klasa, ali ćemo napraviti lokalni Artinov simbol, koji se dalje koristi u lokalnoj teoriji polja klasa. On će generalizirati Hilbertov simbol.

Definicija. Neka je L/K Abelovo proširenje, $\alpha \in K^\times$, i v mjesto od K. Definirajmo $(\alpha, L/K)_v \in \mathrm{Gal}(L/K)$ na sljedeći način. Neka je $\mathfrak{m}$ modulus takav da je $\mathrm{Gal}(L/K) \simeq I_\mathfrak{m}/H$ za neku generaliziranu grupu ideala H. Kada je v konačan, izaberimo α_0 koji je "blizu" α u v i takav da je α_0 blizu 1 u mjestima koja dijele $\mathfrak{m}$ (s iznimkom ako v dijeli $\mathfrak{m}$):

$$v_v\left(\frac{\alpha_0}{\alpha} - 1\right) \geq v_v(\mathfrak{m}), \quad v_w(\alpha_0 - 1) \geq v_w(\mathfrak{m}), \quad \sigma(\alpha_0) > 0,$$

gdje w ide po svim konačnim mjestima različitima od v, te σ ide po svim realnim mjestima koja dijele $\mathfrak{m}$. Ako v ne dijeli $\mathfrak{m}$, tada uključimo i dodatan uvjet da

$$((\alpha_0/\alpha), v) = 1.$$

Faktorizirajući ideal (α_0) u produkt prostih ideala, neka je I produkt faktora od (α_0) koji nisu djeljivi s v. Dakle imamo da je $(I, \mathfrak{m}) = 1$ po definiciji. Definiramo

$$(\alpha, L/K)_v = \theta_{L/K,\mathfrak{m}}(I)^{-1}$$

za konačna mjesta v. Za beskonačna mjesta v u kojima je K_v realno, a L_v kompleksno i za koje je $\alpha < 0$ u K_v definiramo da je $(\alpha, L/K)_v$ kompleksno konjugiranje u $\mathrm{Gal}(L_v/K_v) \lesssim \mathrm{Gal}(L/K)$, a u svim drugim slučajevima definirajmo da je $(\alpha, L/K)_v$ identiteta.

Primjetimo da izbor od α_0 ovisi o izboru mjesta v, tj. za svako mjesto v biramo drugi α_0.

Prvo što možemo primjetiti u definiciji iznad je da izbor od α_0 nije jedinstven, štoviše postoji beskonačno mnogo α_0 koji zadvoljavaju uvjete. Pokažimo da vrijednost $(\alpha, L/K)_v$ ne ovisi o izboru α_0. Neka je β_0 neka druga vrijednost koja zadovoljava uvjete definicje. Tada imamo da je $(\alpha_0/\beta_0) \equiv 1 \pmod{\mathfrak{m}}$, tj.

$(\alpha_0/\beta_0) \in P_{\mathfrak{m}}$, tj. $\theta_{L/K,\mathfrak{m}}(\alpha_0/\beta_0) = 1$. Dakle $(\alpha, L/K)_v$ je dobro definiran, tj. ne ovisi o izboru od α_0.

Primjetimo da ovdje implicitno koristimo globalnu teoriju polja klasa kako bi definirali $(\alpha, L/K)_v$.

Definicija. Neka je L/K proširenje PAB. Kažemo da je modulus $\mathfrak{m}$ *prihvatljiv* ako potoji generalizirana grupa ideala $P_{\mathfrak{m}} \leq H \leq I_{\mathfrak{m}}$ takav da je L polje klasa od H.

Primjer 29. Iračunajmo $(-1, \mathbb{Q}(i)/\mathbb{Q})_v$. Znamo da je $\mathfrak{m} = 4\infty$ prihvatljiv modulus za $\mathbb{Q}(i)/\mathbb{Q}$. Poistovjetimo $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ s $\{\pm 1\}$. Pošto je $-1 < 0$ imamo da je $(-1, \mathbb{Q}(i)/\mathbb{Q})_\infty = -1$. Za $v = 2$, možemo uzeti $\alpha_0 = 3$, pa je $(-1, \mathbb{Q}(i)/\mathbb{Q})_2 = (3, \mathbb{Q}(i)/\mathbb{Q}) = \left(\frac{-1}{3}\right)$. Za bilo koji neparan prost broj p možemo uzeti $\alpha_0 = 1$, pa je $(-1, \mathbb{Q}(i)/\mathbb{Q})_\infty = \theta_{L/K,\mathfrak{m}}(1)^{-1} = 1$.

Avalogno, imamo da je $(3, \mathbb{Q}(i)/\mathbb{Q})_v = 1$ za $v \neq 2, 3$. Za $v = 2$, imamo $(3, \mathbb{Q}(i)/\mathbb{Q})_v = -1$ koristeći istu argumentaciju kao i gore. Za $v = 3$, tražimo α_0 takav da je $(\alpha_0/\alpha, v) = 1$, pa vidmo da možemo izabrati $\alpha_0 = 3$, pa dobijemo $(3, \mathbb{Q}(i)/\mathbb{Q})_3 = (3, \mathbb{Q}(i)/\mathbb{Q}) = -1$.

Primjer 30. Neka je $\mathfrak{p}$ prost ideal koji ne dijeli prihvatljiv modulus $\mathfrak{m}$ za L/K. Za $\alpha \in K^\times$, neka je $k = v_p(\alpha)$. Izaberite α_0 takav da je $v_w(\alpha_0 - 1) \geq v_w(\mathfrak{m})$ za sve konačne $w|\mathfrak{m}$, te $w(\alpha_0) > 0$ za sve beskonačne w koji dijele $\mathfrak{m}$ i $v_{\mathfrak{p}}(\alpha_0/\alpha - 1) \geq 1$. Tada je $(\alpha_0) = \mathfrak{p}^k I$, za neki I relativno prost s $\mathfrak{p}$ i s $\mathfrak{m}$.

Sada imamo da je $(\alpha, L/K)_{\mathfrak{p}} = \theta_{L/K,\mathfrak{m}}(I)^{-1} = \theta_{L/K,\mathfrak{m}}((\alpha_0)\mathfrak{p}^{-k})^{-1}$. Pošto smo izabrali $\alpha_0 \in P_{\mathfrak{m}}$, imamo da je $\theta_{L/K,\mathfrak{m}}(\alpha_0) = 1$, pa je

$$(\alpha, L/K)_{\mathfrak{p}} = \theta_{L/K,\mathfrak{m}}(\mathfrak{p})^k = (\mathfrak{p}, L/K)^{v_{\mathfrak{p}}(\alpha)}.$$

Vidimo da za $\mathfrak{p} \nmid \mathfrak{m}$, $(\alpha, L/K)_{\mathfrak{p}} = 1$ ima jednostavnu definiciju pomoću Frobeniusa. Štoviše, odmah vidimo da je $(\alpha, L/K)_{\mathfrak{p}}$ za sve osim konačno mnogo $\mathfrak{p}$, pošto samo konačno mnogo $\mathfrak{p}$ dijeli $\mathfrak{m}$ i $v_{\mathfrak{p}}(\alpha) = 0$ za sve osim konačno mnogo $\mathfrak{p}$.

Ranije smo bili definirali Hilbertov simbol $(\alpha, \beta)_v$. Pokažimo da naš novi simbol generalizira Hilbertov simbol: neka je $L = K(\sqrt{\beta})$, te poistovjetimo $\mathrm{Gal}(L/K)$ s $\{\pm 1\}$. Lako vidimo da je tada $(\alpha, L/K)_v = (\alpha, \beta)_v$.

U gornjim primjerima nam je produkt po svim mjestima $(\alpha, L/K)_{\mathfrak{p}}$ bio 1. To naravno nije slučajno, što nam govori sljedeći teorem.

Teorem 68 (Hasse). *Za sva konačna Abelova proširenja PAB L/K i $\alpha \in K^\times$, vrijedi*

$$\prod_{v \in V_K} (\alpha, L/K)_v = 1.$$

Napomenimo da je Hasse u dokazu prethodnog teorema koristio globalnu teoriju polja klasa.

Poglavlje 11

Eliptičke krivulje

Definicija. **Eliptička krivulja** nad poljem k je glatka, projektivna krivulja genusa 1 sa specificiranom točkom $\mathcal{O} \in k$.

Objasnimo ovu definiciju. **Afini pravac** je $\mathbb{A}^1(k) = k$. **Afina ravnina** je $\mathbb{A}^2(k) = k \times k$.

Definicija. **Projektivni pravac** $\mathbb{P}^1(k)$ je

$$\mathbb{P}^1(k) = \{(a,b) \in k^2 | (a,b) \neq (0,0)\}/\sim$$

gdje je $(a,b) \sim (c,d)$ ako i samo ako postoji $0 \neq \lambda \in k$ takav da je $a = \lambda c$ i $b = \lambda d$.

Analogno, **projektivna ravnina** $\mathbb{P}^2(k)$ je

$$\mathbb{P}^2(k) = \{(a,b,c) \in k^3 | (a,b,c) \neq (0,0,0)\}/\sim$$

gdje je $(a,b,c) \sim (d,e,f)$ ako i samo ako postoji $0 \neq \lambda \in k$ takav da je $a = \lambda d$ i $b = \lambda e$ i $c = \lambda f$. Klasu ekvivalencije čije je (a,b,c) reprezent, označavamo s $(a : b : c)$.

Točke projektivnog pravca $\mathbb{P}^1(k)$ možemo zamišljati kao nagib nekog pravca u ravnini ili alternativno kao $A^1(k) \cup \{\infty\}$, gdje ∞ "predstavlja" okomiti pravac. Pošto je preslikavanje

$$(a : b : c) \to \begin{cases} (a/c, b/c) & \text{ako je } c \neq 0 \\ (a : b) & \text{ako je } c \neq 0 \end{cases}$$

bijekcija, vrijedi da je $\mathbb{P}^2(k) = A^2(k) \cup \mathbb{P}^1(k)$.

Definicija. Neka je k savršeno polje, $f \in k[x,y]$ polinom, te $\overline{k}$ algebarsko zatvorneje od k. Tada je **afina krivulja** C_f skup točaka

$$C_f = \{P \in A^2(\overline{k}) | f(P) = 0\}.$$

Definicija. Neka je $F \in k[X,Y,Z]$ homogeni polinom. Tada je **projektivna krivulja** C_F skup točaka

$$C_F = \{P \in \mathbb{P}^2(\overline{k}) | F(P) = 0\}.$$

Stupanj od krivulje C_F je stupanj od F.

S $C_f(k)$ i $C_F(k)$ označavamo skupove k-racionalnih točaka od C_f i C_F.

Ako je krivulja C definirana nad k (tj. $F \in k[X,Y,Z]$ za projektivnu krivulju, ili $f \in k[x,y]$), tada pišemo C/k.

Definicija. Projektivna krivulja C_F/k je nesingularna ako ne postoji $P \in C_F(k)$ takva da je

$$\frac{dF}{dX}(P) = \frac{dF}{dY}(P) = \frac{dF}{dZ}(P) = 0.$$

Na primjer, krivulja

$$Y^2Z = X^3 + X^2Z$$

ima sve parcijalne derivacije jednake 0 u $P = (0:0:1)$, dakle nije glatka.

Bitno je i da eliptička krivulja ima k-racionalnu točku. Npr. krivulja

$$S : 3X^3 + 4Y^3 + 5Z^3 = 0$$

nema točaka nad $\mathbb{Q}$ (sjetimo se da $(0:0:0)$ nije točka!), tako da S nije eliptička krivulja nad $\mathbb{Q}$, iako je glatka projektivna krivulja genusa 1.

Svaka afina krivulja se može upotpuniti do projektivne krivulje dodavanjem odgovarajuće potencije od z u svakom sumandu. Na primjer,

$$x^4 + xy = y^3 + 2x$$

se može upotpuniti tako da se napiše kao

$$x^4 + xyz^2 = y^3z + 2xz^3.$$

Projektivne krivulje se često pretvaraju u afine krivulje (između ostalog zbog lakše notacije) tako da se uzme $z = 1$. Mi ćemo često, zbog lakše notacije pisati (eliptičke) krivulje kao da su afine krivulje, iako ćemo ih zapravo zauvijek smatrati projektivnim krivuljama.

Prije nego što krenemo promatrati svojstva eliptičkih krivulja, uvest ćemo standardni oblik zapisivanja krivulja.

Lema 69. *Svaka eliptička krivulja E nad poljem k se može zapisati u* ***Weierstrassovoj formi***

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_2x + a_6. \tag{11.1}$$

Eliptička krivulja E, zapisana u projektivnom obliku je zapravo

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

ali mi možemo zbog jednostovanosti $E(k)$ zamišljati kao skup točaka koje zadovoljavaju jednadžbu (11.1) plus "točka u beskonačnosti $\mathcal{O}$", koja je $(0 : 1 : 0)$ u projektivnim koordinatama.

Ako je karakteristika polja k, $char\ k \neq 2, 3$, tada se eliptička krivulja može zapisati u **kratkoj Weierstrassovoj formi**

$$y^2 = x^3 + ax + b.$$

Neka je

$$E : y^2 = x^3 + ax + b$$

eliptička krivulja u kratkoj Weierstrassovoj formi. Tada je **diskriminata eliptičke krivulje**

$$\Delta(E) = \Delta = -16(4a^3 + 27b^2).$$

Primjetimo da je $\Delta(E) = 16\times$diskriminanta od $x^3 + ax + b$, te vrijedi da je $\Delta \neq 0$ ekvivalentno tome da je E glatka. Zaista ako je $F = y^2 - x^3 - ax - b$, tada je

$$\frac{dF}{dy}(P) = 0 \Longleftrightarrow y(P) = 0,$$

te je

$$\frac{dF}{dy}(P) = 0 \text{ i } \frac{dF}{dx}(P) = 0 \Longleftrightarrow x^3 + ax + b \text{ ima višestruke nultočke}$$

$$\Longleftrightarrow \text{diskriminanta od } x^3 + ax + b \text{ je } 0 \Longleftrightarrow \Delta(E) = 0.$$

11.1 Funkcijska polja (afinih) krivulja

U ovom i sljedećem poglavlju ćemo navoditi mnoge tvrdnje bez dokaza. Dokazi se mogu naći u [7].

Definicija. Neka je R integralna domena. Tada je $\mathrm{Frac}(R) = \{\frac{a}{b}, a, b \in R, b \neq 0\}/\sim$, gdje je $\sim$ standardna relacija ekvivalencije, **polje razlomaka** od R.

Primjer 31. $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q},\ \mathrm{Frac}(k[x]) = k(x)$.

Definicija. Racionalna funkcija na $\mathbb{A}^n(k)$ je $f \in k(x_1, \ldots, x_n) =: k(A^n)$.

Mi ćemo promatrati samo slučaj $n = 2$.

Definicija. Neka je C/k afina krivulja, te $f = \frac{g}{h} \in k(\mathbb{A}^2)$, gdje je $h \neq 0$ na $C(k)$. Restrikcija od f na C

$$f : C - \{\text{konačan skup gdje je } h = 0\} \to \overline{k}$$

je **racionalna funkcija na** C. Skup svih racionalnih funkcija na C čini polje, koje označavamo s $k(C)$.

Činjenica. Neka je C afina krivulja definirana s $f \in k[x, y]$. Tada je

$$k(C) \simeq \mathrm{Frac}\left(\frac{k[x,y]}{(f)}\right).$$

Također, $k[C] \simeq \left(\frac{k[x,y]}{(f)}\right)$ se zove **koordinatni prsten** od C.

Primjer 32. Neka je $D : y = 0$ u afinoj ravnini.

$$k(C) \simeq \mathrm{Frac}\left(\frac{k[x,y]}{(y)}\right) \simeq \mathrm{Frac}(k[x]) = k(x).$$

Primjer 33. Neka je $C : y^2 = x^3 + 1$ u afinoj ravnini. Tada je

$$k(C) \simeq \mathrm{Frac}\left(\frac{k[x,y]}{(y^2 - x^3 - 1)}\right) \simeq k(x, \sqrt{x^3 + 1}).$$

Definirajmo sada glatkoću da algebarski način.

Definicija. Neka je C/K neka krivulja, te neka je $\overline{K}(C)$ njeno funkcijsko polje (nad algebarskim zatvorenjem). Neka je $P \in C(\overline{K})$, te definiramo

$$\overline{K}[C]_P = \{f/g \in \overline{K}(V), f, g \in \overline{K}[V], g(P) \neq 0\}.$$

$$\mathfrak{m}_P = \{f \in \overline{K}[C]_P : f(P) = 0\}.$$

Prsten $\overline{K}[C]_P$ se naziva lokalni prsten od C u P. To je lokalni prsten s maksimalnim idealom $\mathfrak{m}_p$. Za funkciju $f \in \overline{K}(V)$, koja je u $K[C]_P$, kažemo da je *regularna*.

Činjenica. Krivulja C je regularna u $P \in C$ ako i samo ako je $\dim_{\overline{K}} \mathfrak{m}_P/\mathfrak{m}_P^2 = 1$.

Primjer 34. Pogledajmo krivulje

$$C_1 : y^2 = x^3 + x,$$

$$C_2 : y^2 = x^3 + x^2.$$

Točka $P = (0,0)$ se nalazi na obje te krivulje.

Pogledajmo prvo C_1. Tu je $\mathfrak{m}_P = \langle x, y \rangle$, te je $\mathfrak{m}_P^2 = \langle x^2, xy, y^2 \rangle$. Imamo da je $x = y^2 - x^3$, dakle $x \in \mathfrak{m}_P^2$. Zaključujemo da je $\mathfrak{m}_P/\mathfrak{m}_P^2 = \langle y \rangle$.

Pogledajmo sada C_2. Tu je opet $\mathfrak{m}_P = \langle x, y \rangle$, te je $\mathfrak{m}_P^2 = \langle x^2, xy, y^2 \rangle$,, ali sada se i x i y nalaze u $\mathfrak{m}_P/\mathfrak{m}_P^2$, dakle $\mathfrak{m}_P/\mathfrak{m}_P^2 = \langle x, y \rangle$.

Dakle C_2 je singularna u P, dok je C_1 nesingularna u P.

11.2 Preslikavanja eliptičkih krivulja

Definicija. Neka su C/k i D/k krivulje. **Racionalno preslikavanje** (nad k) $\phi : C \to D$ je preslikavanje definirano s racionalnim funkcijama $\phi = (u, v)$, $u, v \in k(C)$, takvo da u i v nisu oboje 0. Tj, $\phi(P) = (u(P), v(P))$ za $P \in C(k)$.

Primjetimo sljedeće: Neka su $C = C_f$ i $D = D_g$ krivulje, te neka je $\phi : C \to D$ preslikavanje. Ako je a racionalna funkcija $\in k(D)$, tada je $a \circ \phi$ racionalna funkcija $\in k(C)$. Dakle, racionalna funkcija $\phi : C \to D$ inducira injekciju polja

$$\phi^* : k(D) \hookrightarrow k(C),$$

$$a \mapsto a \circ \phi = \phi^* a.$$

Definicija. Stupanj od ϕ je $[k(C) : \phi^* k(D)]$, ako ϕ nekonstantna, a definiramo da je stupanj od ϕ jednak 0 ako je ϕ konstantna.

Primjer 35. Neka su C i D kao u primjerima 32 i 33. Tada je

$$\phi : C \to D, \ \phi(x, y) = (x, 0)$$

racionalno preslikavanje, te vrijedi da ako je $a(x, 0) = x$ racionalna funkcija na $k(D)$, tada je

$$a \circ \phi(x, y) = \phi^* a(x, y) = x$$

Dakle $\phi^* k(D) = k(x)$, te je

$$[k(C) : \phi^* k(D)] = [k(x, \sqrt{x^3 + 1}) : k(x)] = 2,$$

pa slijedi da je ovo preslikavanje stupnja 2.

Činjenica. Neka je k polje algebarskih brojeva, te neka je K konačno proširenje od $k(x)$. Tada postoji krivulja C takva da je $k(C) = K$.

Činjenica. Neka je $i : k(C_2) \hookrightarrow k(C_1)$ ulaganje funkcijskih polja koje fiksira k. Tada postoji jedinstveno ne-konstantno racionalno preslikavanje $\phi : C_1 \to C_2$ takvo da je $\phi^* = i$.

Definicija. Kažemo da je $\phi : C \to D$ **definirano** u točki P ako postoji $g \in k(C)^*$ takav da su ug, vg definirani u P. Ako je ϕ definiran na cijeloj C, tada je ϕ **morfizam**.

Definicija. Ako je $\phi : C \to D$ morfizam takav da postoji morfizam $\psi : D \to C$ takav da su $\psi \circ \phi$ i $\phi \circ \psi$ identiteta na C i D, tada je ϕ **izomorfizam**.

Činjenica. Ako je $\phi : C \to D$ racionalno preslikavanje takvo da je C glatka, tada je ϕ morfizam.

Činjenica. Ako je $\phi : C \to D$ racionalno preslikavanje stupnja 1, te su C i D glatke, tada je ϕ izomorfizam.

Imamo sljedeću ekvivalenciju kategorija:

$$\text{glatke krivulje nad } k \leftrightarrow \text{proširenja polja } K/k(x)$$

$$\text{racionalna preslikavanja (morfizmi)} \leftrightarrow \text{ulaganja polja}$$

$$C \leftrightarrow k(C).$$

Činjenica. Ako su dvije eliptičke krivulje

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$$E' : y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6$$

u Weierstrassovoj formi izomorfne, tada postoji preslikavanje $(x_E, y_E) \mapsto (x_{E'}, y_{E'})$,

$$x_{E'} = u^2x_E + r,$$

$$y_{E'} = u^3y_E + sx_E + t, \text{ gdje } u \in k^*, r, s, t \in k.$$

Također, ako su dvije eliptičke krivulje

$$E : y^2 = x^3 + ax + b, \tag{11.2}$$

$$E' : y^2 = x^3 + a'x + b' \tag{11.3}$$

u kratkoj Weierstrassovoj formi (nad poljem karakteristike $\neq 2, 3$) izomorfne, tada postoji pomjena varijabli

$$x_{E'} = u^2x_E,$$

$$y_{E'} = u^3y_E, \text{ gdje } u \in k^*.$$

Dakle za eliptičke krivulje E i E' u kratkoj Weierstrassovoj formi vrijedi

$$E \simeq E' \Longleftrightarrow (u^3y_E)^2 = (u^2x_E)^3 + a'(u^2x_E) + b',$$

$$\Longleftrightarrow a' = u^4a, \ b' = u^6b$$

$$\Delta(E') = -16(4a'^3 + 27b'^2) = u^{12}\Delta(E)$$

Definicija. j**-invarijanta** eliptičke krivulje $y^2 = x^3 + ax + b$ je

$$j = j(E) = \frac{1728(-4a)^3}{\Delta}.$$

Za eliptičku krivulju u (općoj) Weierstrassovoj formi

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

diskriminanta i j-invarijanta se računaju na sljedeći način:

$$b_2 = a_1^2 + 4a_2,\ b_4 = a_1a_3 + 2a_4,\ b_6 = a_3^2 + 4a_6,\ b_8 = b_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4,\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6,\ \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b^2b^4b^6,\ j = c_4^3/\Delta.$$

Propozicija 70. *Neka je k polje karakteristike $\neq 2, 3$.*

1. *Eliptičke krivulje E i E' su izomorfne nad $\overline{k}$ ako i samo ako je $j(E) = j(E')$.*
2. *Za svaki $j \in k$, postoji eliptička krivulja E/k takva da je $j(E) = j$.*

Dokaz. 1. Pretpostavimo da su E i E' kao u (11.2) i (11.3), to sigurno možemo pošto se svaka eliptička krivulja nad poljem karakteristike $\neq 2, 3$ može zapisati u kratkoj Weierstrassovoj formi.

$$\text{Ako } a, b \neq 0,\ a' = u^4a,\ b' = u^6b, u \in \overline{k}^*, \iff \sqrt[4]{a/a'} = \sqrt[6]{b/b'} \iff$$

$$(a'/a)^3 = (b'/b)^2 \iff \frac{4a^3 + 27b^2}{a^3} = \frac{4a'^3 + 27b'^2}{a'^3} \iff j(E) = j(E').$$

Ako je $a = 0$, tada je $a' = 0$ i $b, b' \neq 0$, pa dobivamo izomorfizam uzimanjem $u = \sqrt[6]{b'/b}$. Ako je $b = 0$, tada je $b' = 0$, te $a, a' \neq 0$. Dobivamo izomorfizam uzimanjem $u = \sqrt[4]{a'/a}$.

2. Za $j \neq 0, 1728$ eliptička krivulja

$$E : y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}$$

ima

$$j(E) = j,\ \Delta(E) = \frac{j^2}{(j - 1728)^3}.$$

Za

$$E_1 : y^2 = x^3 + ax,\ j(E_1) = 1728,$$

$$E_2 : y^2 = x^3 + b,\ j(E_2) = 0.$$

□

Korolar 71. *Postoji bijekcija između {eliptičke krivulje $/k$ do na $\overline{k}$-izomorfizam} i k.*

Korolar 72. *Grupa automorfizama eliptičke krivulje (nad $\overline{k}$)*

$$\operatorname{Aut} E = \{izomorfizmi : E \to E\}$$

je

$$\mathbb{Z}/2\mathbb{Z} \text{ za } y^2 = x^3 + ax + b, a, b \neq 0$$
$$\mathbb{Z}/4\mathbb{Z} \text{ za } y^2 = x^3 + ax,$$
$$\mathbb{Z}/6\mathbb{Z} \text{ za } y^2 = x^3 + b.$$

Dokaz. $\operatorname{Aut} E = \{u \in \overline{k}^\times : u^4 a = a,\ u^6 b = b\}$, pa slijedi da je

$$\operatorname{Aut} E = \langle -1 \rangle, \text{ ako } a, b \neq 0,$$

$$\operatorname{Aut} E = \langle i \rangle, \text{ ako } b = 0,$$

$$\operatorname{Aut} E = \langle \zeta_6 \rangle, \text{ ako } a = 0,$$

gdje je ζ_6 primitivni šesti korijen iz jedinice (npr. $\frac{1-\sqrt{-3}}{2}$). □

Propozicija 73. *Neka je E/K eliptička krivulja nad PAB, s $\operatorname{Aut} E \simeq \mathbb{Z}/2\mathbb{Z}$ zadana kao*

$$E : y^2 = x^3 + ax + b,$$

te neka je E'/K eliptička krivulja s $j(E) = j(E')$ i takva da E i E' nisu izomorfne nad K. Tada su E is E' izomorfne nad kvadratnim proširenjem od K.

Dokaz. Vrijedi $a, b \neq 0$, te

$$E' : y^2 = x^3 + au^4 x + bu^6,$$

gdje su $u^4, u^6 \in K$. Dakle imamo da je $u^2 = t \in K$. Zamjenom varijabli

$$y \mapsto yt^2, \quad x \mapsto xt,$$

te dijelnjenjem s t^3 dobijemo $E' : ty^2 = x^3 + ax + b$. Očito nad kvadratnim poljem $K(\sqrt{t})$ te krivulje postaju izomorfne. □

Poglavlje 12

Izogenije

Pretpostavimo u ovom poglavlju da je $\operatorname{char} k \neq 2, 3$.

Definicija. **Izogenija** između dvije eliptičke krivulje je morfizam $\phi : E \to E'$ koji preslikava $\mathcal{O} \in E$ u $\mathcal{O}' \in E'$.

Činjenica. Svaka izogenija je homomorfizam grupa.

Teorem 74 (Mordell-Weil)**.** *Skup K-racionalnih točaka eliptičke krivulje nad PAB K čini konačno generiranu Abelovu grupu.*

Primjer 36. Množenje s m na eliptičkoj krivulji $[m]$ je za svaki $m \geq 1$ izogenija.

$[0] : E \to E$ je nul-izogenija. Definiraimo $\operatorname{st}[0] = 0$, tako da bi vrijedilo

$$\operatorname{st} \phi \circ \psi = \operatorname{st} \phi \cdot \operatorname{st} \psi$$

za sve izogenije $\phi : E \to E'$, $\psi : E' \to E$.

Primjer 37. Neka je $E : y^2 = x^3 + ax + b$. Promotrimo množenje s 2 na E, $[2] : E \to E$,

$$[2] : (x, y) \to \left(\frac{x^4 - 2ax^2 + a^2 - 8b}{4(x^3 + ax + b)}, \ldots \right).$$

Preslikavanje $[2]$ je definirano racionalnim funkcijama, te je $[2]\mathcal{O} = \mathcal{O}$, tako da je $[2]$ izogenija.

Neka su E_1 i E_2 eliptičke krivulje. Tada je

$$\operatorname{Hom}(E_1, E_2) = \{\text{izogenije} : E_1 \to E_2\}$$

grupa uz operaciju zbrajanja.

Nadalje, $\operatorname{End} E = \operatorname{Hom}(E, E)$ je prsten s jedinicom (s operacijama zbrajanja i kompozicije) koji sadrži $\mathbb{Z}$, pošto je množenje s m izogenija za svaki $m \in \mathbb{Z}$.

Zapravo, za eliptičke krivulje definirane nad poljima algebarskih brojeva, skoro uvijek će vrijediti $\operatorname{End} E = \mathbb{Z}$.

Napomena. Ako u subskriptu imamo polje, npr. $\mathrm{End}_k(E)$ ili $\mathrm{Hom}_k(E_1, E_2)$, tada to označava skup preslikavanja tog tipa nad k. Ako ne piše ništa u subskriptu, onda se uvijek misli na preslikavanja definirana nad $\overline{k}$.

Primjer 38. Neka je $E : y^2 = x^3 - x$, te $[i] \in \mathrm{End}\, E$, $[i] : (x, y) = (-x, iy)$. Primjetimo $[i]([i][-1]) = [1]$, te je $[i]$ automorfizam. Slijedi $\mathrm{End}\, E \supset \mathbb{Z}[i]$. Međutim, $\mathrm{End}_{\mathbb{Q}}\, E = \mathbb{Z}$.

Neka su C i D glatke projektivne krivulje. Sjetimo se da je stupanj nekog nekonstantnog racionalnog preslikavanja krivulja $\phi : C \to D$ jednak maksimalnom broju točaka $\in C$ u praslici od $\phi(P)$ za neki $P \in D$. Ako je preslikavanje stupnja n, tada će $|\phi^{-1}(P)| = n$ za sve osim konačno mnogo P-ova. Ako je $|\phi^{-1}(P)| < n$ tada je ϕ **razgranato** u P, ako je $|\phi^{-1}(P)| = n$ onda je **nerazgranato** u P.

Ako je $\phi : E_1 \to E_2$ ne-nul izogenija, tada je $\mathrm{Ker}\, \phi = \phi^{-1}(\mathcal{O})$ konačna podgrupa (od $E(\overline{k})$).

Primjer 39. Neka je $E : y^2 = (x - a_1)(x - a_2)(x - a_3), a_i \in \mathbb{Q}$, $T_i = (a_i, 0)$. Tada je
$$\mathrm{Ker}[2] = \{\mathcal{O}, T_1, T_2, T_3\} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Neka je E eliptička krivulja, $\mathcal{O} \neq P \in E$. Definiramo
$$\tau_P : E \to E,$$
$$\tau_P(Q) = P + Q$$
tj. τ_p je translacija s P. Preslikavanje τ_p je morfizam (ali nije homomorfizam grupa).

Teorem 75. *Neka su E_1, E_2 eliptičke krivulje nad poljem algebarskih brojeva k, te $\phi : E_1 \to E_2$ izogenija stupnja $n \neq 0$.*

1. *ϕ je nerazgranato preslikavanje, tj. $|\phi^{-1}(P)| = n$ za svaki $P \in D$.*

2. *Neka je $K_1 = \overline{k}(E_1)$, $K_2 = \phi^*(\overline{k}(E_2))$. Tada je K_1 Galoisovo proširenje od K_2, te je $\mathrm{Gal}(K_1/K_2) \simeq \mathrm{Ker}\, \phi$.*

3. *Ako je $\psi : E_1 \to E_3$ izogenija i $\mathrm{Ker}\, \psi \supset \mathrm{Ker}\, \phi$, tada postoji jedinstvena izogenija $\chi : E_2 \to E_3$ takva da je $\psi = \chi \circ \phi$.*

Dokaz. 1. Pošto je ϕ preslikavanje stupnja n, vrijedi da postoji točka $P \in E_2$, t.d. $|\phi^{-1}(P)| = n$. Definirajmo $\phi^{-1}(P) = \{Q_i, i = 1, \dots, n\}$. Neka je sada P' proizvoljna točka $\in E_2$, te neka je $Q' \in \phi^{-1}(P')$. Tada su $Q' + Q_i - Q_1,\ i = 1, \dots n$ različite točke te pošto je ϕ homomorfizam grupa, vrijedi da je $\phi(Q' + Q_i - Q_1) = P',\ i = 1, \dots n$.

2. Neka je $\Phi = \mathrm{Ker}\, \phi = \{T_1, \dots, T_n\}$. Promotrimo $\tau_{T_i} : E_1 \to E_1$. To preslikavanje je izomorfizam krivulja, pa inducira automorfizam $\tau_{T_i}^*$ funkcijskog polja K_1. Neka je $P \in E_1$, te neka je $\phi^* f \in K_2$. Tada je

$$\tau_{T_i}^* \phi^* f(P) = (\phi^* f)\tau_{T_i}(P) = f(\phi(P + T_i)) = f(\phi(P) + \phi(T_i)) = f\phi(P) =$$

$$= \phi^* f(P).$$

Slijedi da je $\tau_{T_i}^*$ automorfizam od K_1 koji fiksira K_2, tj. $|Aut(K_1/K_2)| \geq n$. Pošto je $[K_1 : K_2] = n$ slijedi da je $|Aut(K_1/K_2)| = n$, te K_1/K_2 Galoisovo, te

$$\mathrm{Gal}(K_1/K_2) \simeq \mathrm{Ker}\,\phi.$$

Primjetimo da slijedi i da će $\mathrm{Gal}(K_1/K_2)$ biti Abelova grupa.

3. Neka je $K_3 = \psi^* \overline{k}(E_3)$. Tada je kao i prije K_3 fiksiran sa svim $\mathrm{Gal}(K_1/K_3) = \{\tau_P^* : P \in \mathrm{Ker}\,\psi\} \leq \{\tau_P^* : P \in \mathrm{Ker}\,\phi\} = \mathrm{Gal}(K_1/K_2)$. Po Fundamentalnom teoremu Galoisove teorije

$$K_3 = K_1^{\mathrm{Gal}(K_1/K_3)} \subset K_1^{\mathrm{Gal}(K_1/K_2)} = K_2,$$

tj. K_3 je potpolje od K_2. Dakle, postoji jedinstveni $\chi : E_2 \to E_3$ koji inducira ovu inkluziju funkcijskih polja. Pošto je (po konstrukciji koju smo upravo napravili) $\phi^*(\chi^* K_3) = \psi^* K_3$, vrijedi $\psi = \chi\phi$. Da bi završili dokaz da je ovo izogenija, treba primjetiti

$$\chi(\mathcal{O}) = \chi(\phi(\mathcal{O})) = \psi(\mathcal{O}) = \mathcal{O}.$$

$\square$

Na sličan način uz korištenje Riemann-Hurwitzove formule za genus, dobiva se sljedeća važna činjenica.

Činjenica. Ako je Φ podgrupa od E, tada postoji jedinstvena eliptička krivulja E' i izogenija

$$\phi : E \to E'$$

takva da je $\ker\phi = \Phi$.

Poglavlje 13

Eliptičke krivulje nad $\mathbb{C}$

Sjetimo se da kažemo da je kompleksna funkcija f **meromorfna** ako je holomorfna osim na skupu izoliranih točaka, u kojima ima polove. U ovom poglavlju ćemo također izreći neke tvrdnje bez dokaza (pogledajte [7] za detalje).

Definicija. Rešetka $\Lambda \subset \mathbb{C}$ je diskretna podgrupa ranga 2, tj.

$$\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2,\ w_1, w_2 \in \mathbb{C},$$

takva da su w_1 i w_2 linearno nezavisni nad $\mathbb{R}$.

Baza w_1, w_2 je jedinstvena do na $\mathrm{GL}_2(\mathbb{Z})$.

Definicija. **Eliptička funkcija** (s obzirom na Λ) je meromorfna funkcija f za koju vrijedi

$$f(z+w) = f(z),\ \forall z \in \mathbb{C},\ \forall w \in \Lambda.$$

Definicija. **Fundamentalni paralelogram** za Λ je skup

$$D = \{a + t_1 w_1 + t_2 w_2 : 0 \le t_1, t_2 < 1\},$$

gdje je $a \in \mathbb{C}$, te su w_1, w_2 baza za Λ.

Propozicija 76. *Eliptička funkcija koja nema nultočke ili nema polove je konstanta.*

Dokaz. Pretpostavimo da je f holomorfna. Pošto je f eliptička vrijedi da je

$$\sup_{z \in \mathbb{C}} |f(z)| = \sup_{z \in \overline{D}} |f(z)|,$$

pa pošto je f neprekidna i $\overline{D}$ je kompaktan skup slijedi da je $\sup_{z\in\mathbb{C}} |f(z)|$ omeđen, pa je po Liouvilleovom teoremu f konstanta. Ako f nema nultočaka, isti argument za $1/f$ dokazuje tvrdnju. $\square$

Definicija. **Eisensteinov red** težine $2k$ s obzirom na Λ je

$$G_{2k} = G_{2k}(\Lambda) = \sum_{w \in \Lambda \setminus \{0\}} w^{-2k}, \quad k \geq 2.$$

Teorem 77. *Postoji jedinstvena eliptička funkcija $\wp(z)$ (s obzirom na fixiranu rešetku Λ) takva da je*

$$\wp(z) = \frac{1}{z^2} + O(z) \text{ oko } z = 0.$$

Funkcija $\wp$ je holomorfna na $\mathbb{C} \setminus \Lambda$.

Točnije, vrijedi

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k}.$$

Funkcija $\wp(z)$ se zove "Weierstrasssova p-funkcija".

Teorem 78. *Napišimo $g_2 = g_2(\Lambda) = 60G_4$ i $g_3 = g_3(\Lambda) = 140G_6$. Tada je $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$.*

Dokaz. Vrijedi (oko $z = 0$)

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + \cdots$$

$$\wp(z)^3 = \frac{1}{z^6} + 9G_4 \frac{1}{z^2} + 15G_6 + \cdots$$

$$\wp'(z)^2 = \frac{1}{4z^6} - 14G_4 \frac{1}{z^2} - 80G_6 + \cdots$$

pa je $\wp'(z)^2 - (4\wp(z)^3 - g_2\wp(z) - g_3)$ funkcija koja je holomorfna u 0, pa pošto je eliptička, onda je holomorfna i na Λ. Također iz prošlog teorema znamo da je holorfna na $\mathbb{C} \setminus \Lambda$. Po Liouvilleovom teoremu slijedi da je funkcija 0. $\square$

Definicija. Neka je Λ rešetka. Tada definiramo

$$E_\Lambda : y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda).$$

Teorem 79. *Preslikavanje*

$$\phi : \mathbb{C}/\Lambda \to E_\Lambda, \quad z \to (\wp(z), \wp'(z))$$

je izomorfizam (kompleksnih Liejevih) grupa.

Napomena. Točnije, izomorfizam je $z \to (\wp(z) : \wp'(z) : 1) \in \mathbb{P}^2(\mathbb{C})$ za $z \neq 0 \in \mathbb{C}/\Lambda$, te $\Lambda \to (0 : 1 : 0)$.

Napomena. Vrijedi i obrat teorema 79, tj, svaka eliptička krivulja nad $\mathbb{C}$ je izomorfna $\mathbb{C}/\Lambda$, za neku rešetku Λ.

Definicija. Neka je E/k eliptička krivulja nad poljem algebarskih brojeva k. Tada je

$$E[m] = \mathrm{Ker}[m] = \{P \in E(\overline{k}) : mP = \mathcal{O}\},$$
$$E(k)[m] = \{P \in E(k) : mP = \mathcal{O}\}.$$

Korolar 80. *Vrijedi* $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$.

Dokaz. $E \simeq \mathbb{C}/\Lambda \simeq (\mathbb{R}/\mathbb{Z})^2$, pa vrijedi $E[m] \simeq (\frac{1}{m}\mathbb{Z}/\mathbb{Z})^2 \simeq (\mathbb{Z}/m\mathbb{Z})^2$. □

Sljedeće što nas zanima su izogenije

$$E = \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda' = E'$$

nad $\mathbb{C}$.

Ako je $\alpha \in \mathbb{C}$ takav da $\alpha\Lambda \subset \Lambda'$, tada je

$$\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda', z \to \alpha z$$

dobro definirano, holomorfno preslikavanje $E \to E'$ takvo da je $\mathcal{O} \to \mathcal{O}$, dano sa

$$\phi_\alpha : (\wp_\Lambda(z), \wp'_\Lambda(z)) \to (\wp_{\Lambda'}(\alpha z), \wp'_{\Lambda'}(\alpha z)).$$

Također, preslikavanje $z \to \wp_{\Lambda'}(\alpha z)$ je eliptičko s obzirom na Λ:

$$\wp_{\Lambda'}(\alpha(z+w)) = \wp_{\Lambda'}(\alpha z + \alpha w) = \wp_{\Lambda'}(\alpha z) \text{ za } w \in \Lambda,$$

jer je $\alpha w \in \Lambda$, dakle $z \to \wp_{\Lambda'}(\alpha z)$ je funkcija $\in \mathbb{C}(E)$. Isto se može dokazati i za $\wp'_{\Lambda'}(\alpha z)$.

Obrnuto, ako je $\phi : E \to E'$ holomorfno preslikavanje takvo da je $\phi(\mathcal{O}) = \mathcal{O}$, tada se $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ može "podignuti" ili proširiti do holomorfnog preslikavanja $f : \mathbb{C} \to \mathbb{C}$, takvo da je $f(0) = 0$.

Za svaki

$$w \in \Lambda, f(z+w) \equiv f(z) \pmod{\Lambda'},$$

tj. $f(z+w) - f(z)$ ne ovisi o z, tj. $(f(z+w) - f(z))' = 0$, odnosno

$$f'(z+w) = f'(z), \ \forall z \in \mathbb{C}, \ \forall w \in \Lambda.$$

Dakle f' je holomorfna eliptička funkcija, dakle kostanta je po Propoziciji 76. Slijedi da je $f(z) = \alpha z + \beta$, s tim da je $\beta = 0$ jer $f(0) = 0$.

Imamo i sljedeću lemu

Lema 81. *Neka su E i E' eliptičke krivulje koje odgovaraju rešetkama Λ i Λ'. Tada postoji bijekcija*

$$\{\textit{izogenije } \phi : E \to E'\} \leftrightarrow \{\textit{holomorfna preslikavanja } \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'\}.$$

Teorem 82. *Postoji bijekcija između sljedećih skupova*

$$\{\textit{izogenije } \phi : E \to E'\} \leftrightarrow \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda'\}.$$

Napomena. Ako su elementi iz $\operatorname{Ker}\phi$ $\operatorname{Gal}(\overline{k}/k)$-invarijantni za neko PAB (polje algebarskih brojeva) k, tada ϕ mora biti definirana nad k.

Definicija. Rešetke Λ i Λ' su **homotetične** ako postoji $\alpha \in \mathbb{C}$ takav da $\alpha\Lambda = \Lambda'$.

Korolar 83. *$E \simeq E'$ ako i samo ako $\Lambda = \alpha\Lambda'$ za neki $\alpha \in \mathbb{C}^*$. Dakle, nad $\mathbb{C}$,*

$$\{\textit{eliptičke krivulje}/\simeq\} \leftrightarrow \{\textit{rešetke}/\textit{homotetija}\}.$$

Očito je svaka rešetka homotetična rešetci $\mathbb{Z} + \mathbb{Z}\tau$, za neki τ (npr. $\tau = w_2/w_1$). Izbor elementa τ je jedinstven do na djelovanje $\mathrm{SL}_2(\mathbb{Z})$ na bazu $\{1, \tau\}$. Npr. ako je $\{1, \tau\}$ baza za Λ, tada je i $\{1, 1+\tau\}$ također baza za rešetku Λ.

Poglavlje 14

Kompleksno moženje nad $\mathbb{C}$

U ovom poglavlju ćemo dosta vjerno slijediti [8, Chapter II].

Definicija. Neka je k polje algebarskih brojeva. Tada je **red** O od k potprsten od k koji je konačno generiran kao $\mathbb{Z}$-modul i zadovoljava $O \otimes \mathbb{Q} = k$.

Teorem 84. *Neka je $E/\mathbb{C}$ eliptička krivulja, te neka je $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$ rešetka koja odgovora krivulji E. Tada postoje 2 slučaja:*

1. $\operatorname{End} E = \mathbb{Z}$.

2. *$\mathbb{Q}(\tau)$ je kvadratno imaginarno proširenje od $\mathbb{Q}$, te je $\operatorname{End} E$ izomorfno redu od $\mathbb{Q}(\tau)$.*

Dokaz. Neka je $R = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$. Slijedi $R \simeq \operatorname{End} E$. Tada za svaki $\alpha \in R$, postoje $a, b, c, d \in \mathbb{Z}$ takvi da

$$\alpha 1 = a + b\tau \text{ i } \alpha\tau = c + d\tau. \tag{14.1}$$

Eliminirajući τ dobijemo

$$\alpha^2 - (a + d)\alpha + bc - ad = 0.$$

Dakle, α je element prstena cijelih brojeva kvadratnog polja ili od $\mathbb{Q}$.

Pretpostavimo da je $R \neq \mathbb{Z}$ i neka je $\alpha \in R$, $\alpha \notin \mathbb{Z}$. Eliminirajući α iz (14.1) dobijemo ($b \neq 0$) i

$$b\tau^2 - (a - d)\tau + c = 0.$$

Dakle $\mathbb{Q}(\tau)$ je kvadratno imaginarno polje. To vidimo jer kada bi $\tau \in \mathbb{R}$, tada $\{1, \tau\}$ ne bi bila rešetka. Konačno, pošto je R sadržan u prstenu cijelih brojeva kvadratnog polja, slijedi da je R red u $\mathbb{Q}(\tau)$. $\square$

Definicija. Neka je E/k eliptička krivulja nad poljem algebarskih brojeva k. Ako je $\operatorname{End} E \supsetneq \mathbb{Z}$ tada kažemo da E ima **kompleksno množenje**.

Neka je sada R red u nekom imaginarnom kvadratnom polju K. Tada je

$$\mathcal{ELL}(R) = \{\text{eliptičke krivulje } E/\mathbb{C} \text{ takve da } \operatorname{End} E \simeq R\}/\simeq$$

$$= \{\text{rešetke } \Lambda \text{ takve da } \operatorname{End} E_\Lambda \simeq R\}/\text{homotetija}.$$

Možemo se zapitati sljedeće: počevši sa prstenom cijelih $R := \mathcal{O}_K$ u kvadratnom imaginarnom polju K, kako dobiti eliptičku krivulju s kompleksnim množenjem s R? Uzmimo ideal $\mathfrak{a} \neq 0$ u R, te vidimo da je $\mathfrak{a}$ rešetka u $\mathbb{C}$ (ovo se jasno vidi iz definicije razlomljenih ideala). Pošto je K kvadratno imaginarno polje, $\mathfrak{a}$ nije sadržano u $\mathbb{R}$. Dakle možemo napraviti kirivulju $E_\mathfrak{a}$ takvu da je

$$\operatorname{End} E_\mathfrak{a} \simeq \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subseteq \mathfrak{a}\} = \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathfrak{a}\} = \mathcal{O}_K,$$

pošto je $\mathfrak{a}$ (razlomljeni) ideal u $\mathcal{O}_K$. Dakle, imamo da svaki razlomljeni ideal daje eliptičku krivulju s kompleksnim množenjem s R! Naravno, moramo se pitati koji ideali daju različite krivulje. Znamo da homotetične rešetke daju izomorfne eliptičke krivulje. Dakle $\mathfrak{a}$ i $c\mathfrak{a}$ će dati istu eliptičku krivulju za svaki $c \in K$. Dakle, trebamo promatrati sve razlomljene ideale modulo glavni ideala, što nam daje da postoji bijekcija između eliptičkih krivulja s kompleksnim množenjem s R i s CL_K. Ta bijekcija je zadana na sljedeći način: neka je $\mathfrak{a}$ neki razlomljeni ideal, te označimo s $\overline{\mathfrak{a}}$ njegovu klasu u CL_K. Dakle imamo preslikavanje

$$CL_K \to \mathcal{ELL}(\mathcal{R}), \quad \overline{\mathfrak{a}} \mapsto E_\mathfrak{a}.$$

Definirajmo sada množenje ideala s rešetkama: neka je $\mathfrak{a}$ razlomljeni ideal kao i do sada, te Λ neka rešetka. Definiramo:

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \ldots + \alpha_r\lambda_r, \alpha_i \in \mathfrak{a}, \lambda_i \in \Lambda\}.$$

Sada ćemo dokazati da množenje s elementima iz CL_K na (R) djeluje slobodno (tj bez fiksnih točaka) i tranzitivno na $\mathcal{ELL}(R)$.

Propozicija 85. *a) Neka je Λ rešetka s $E_\Lambda \in \mathcal{ELL}(R)$, i neka su $\mathfrak{a}$ i $\mathfrak{b}$ ne-nul razlomljeni ideali u K. Tada*

(i) $\mathfrak{a}\Lambda$ je rešetka u $\mathbb{C}$.

(ii) $E_{\mathfrak{a}\Lambda} \in \mathcal{ELL}(R)$.

(iii) $E_{\mathfrak{a}\Lambda} \simeq E_{\mathfrak{b}\Lambda}$ ako i samo ako je $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$.

Dakle, postoji dobro definirano djelovanje od CL_K na $\mathcal{ELL}(R)$ definirano s

$$\overline{\mathfrak{a}} \cdot \Lambda = E_{\mathfrak{a}^{-1}\Lambda}.$$

b) Djelovanje od CL_K na $\mathcal{ELL}(R)$ definirano u a) je slobodno i tranzitivno, te je

$$|CL_K| = |\mathcal{ELL}(R)|.$$

Dokaz. a) (i) Pošto je po pretpostavci $\operatorname{End} E_\Lambda = R$, imamo da je $R\Lambda = \Lambda$. Pošto je $\mathfrak{a}$ razlomljeni ideal, možemo uzeti neki $d \in \mathbb{Z}$ takava da je $d\mathfrak{a}$ u R. Tada je $\mathfrak{a}\Lambda \subseteq (1/d)\Lambda$, pa zaključujemo da je $\mathfrak{a}\Lambda$ diskretna podgrupa od $\mathbb{C}$. Isto tako možemo naći $0 \neq d \in \mathbb{Z}$ takav da je $dR \subseteq \mathfrak{a}\Lambda$, pa zaključujemo da $\mathfrak{a}\Lambda$ nije sadržan u $\mathbb{R}$.

(ii) Za svaki $\alpha \in \mathbb{C}$ i svaki razlomljeni ideal $\mathfrak{a} \neq 0$, imamo

$$\alpha\mathfrak{a}\Lambda \subseteq \mathfrak{a}\Lambda \iff \mathfrak{a}^{-1}\alpha\mathfrak{a}\Lambda \subseteq \mathfrak{a}^{-1}\mathfrak{a}\Lambda \iff \alpha\Lambda \subseteq \Lambda.$$

Dakle,

$$E_{\mathfrak{a}\Lambda} = \{\alpha \in \mathbb{C} : \alpha\mathfrak{a}\Lambda \subseteq \mathfrak{a}\Lambda\} = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\} = \operatorname{End} E_\Lambda = R.$$

(iii) Kao što smo dokazali, klasa izomorfizama od $E_{\mathfrak{a}\Lambda}$ je određena klasom homotetije od $\mathfrak{a}\Lambda$. Dakle imamo da je $E_{\mathfrak{a}\Lambda} \simeq E_{\mathfrak{b}\Lambda}$ ako i samo ako postoji $c \in \mathbb{C}^*$ takva da je $\mathfrak{a}\Lambda = c\mathfrak{b}\Lambda$. Množeći s $\mathfrak{a}^{-1}$, te koristeći da je $R\Lambda = \Lambda$, imamo

$$E_{\mathfrak{a}\Lambda} \simeq E_{\mathfrak{b}\Lambda} \iff \Lambda = c\mathfrak{a}^{-1}\mathfrak{b}\Lambda.$$

Također, množeći s $c^{-1}\mathfrak{b}^{-1}$ dobivamo

$$E_{\mathfrak{a}\Lambda} \simeq E_{\mathfrak{b}\Lambda} \iff \Lambda = c^{-1}\mathfrak{a}\mathfrak{b}^{-1}\Lambda.$$

Dakle ako je $E_{\mathfrak{a}\Lambda} \simeq E_{\mathfrak{b}\Lambda}$, imamo da množenje i s $(c\mathfrak{a}^{-1}\mathfrak{b})$ i s $(c\mathfrak{a}^{-1}\mathfrak{b})^{-1}$ šalje Λ u samu sebe, pa su i $(c\mathfrak{a}^{-1}\mathfrak{b})$ i s $(c\mathfrak{a}^{-1}\mathfrak{b})^{-1}$ sadržani u R, pa zaključujemo da su oba jednaka R. Dakle, imamo da je $\mathfrak{a} = c\mathfrak{b}$, tj $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$.

Ostaje dokazati da CL_K djeluje na $\mathcal{ELL}(R)$. To se vidi iz

$$\overline{\mathfrak{a}} \cdot (\overline{\mathfrak{b}} \cdot E_\Lambda) = \mathfrak{a} \cdot E_{\mathfrak{b}^{-1}\Lambda} = E_{\mathfrak{a}^{-1}\mathfrak{b}^{-1}\Lambda} = E_{(\mathfrak{a}\mathfrak{b})^{-1}\Lambda} = (\overline{\mathfrak{a}}\overline{\mathfrak{b}}) \cdot E_\Lambda.$$

b) Neka su E_{Λ_1} i E_{Λ_2} dvije eliptičke krivulje u $\mathcal{ELL}(R)$. Da bi pokazali da CL_K djeluje tranzitivno na $\mathcal{ELL}(R)$, moramo naći $\mathfrak{a}$ takav da je $\mathfrak{a} \cdot E_{\Lambda_1} = E_{\Lambda_2}$.Uzmimo bilo koji $\lambda_1 \in \Lambda_1$, te promotrimo $\mathfrak{a}_1 = \frac{1}{\lambda_1}\Lambda_1$. Kao i prije vidimo da je to razlomljeni ideal. Analogno konstruirajmo razlomljeni ideal $\mathfrak{a}_2 = \frac{1}{\lambda_2}\Lambda_2$. Tada je

$$\frac{\lambda_2}{\lambda_1}\mathfrak{a}_2\mathfrak{a}_1^{-1}\Lambda_1 = \Lambda_2.$$

Neka je sada $\mathfrak{a} = \mathfrak{a}_2^{-1}\mathfrak{a}_1$. Imamo

$$\overline{\mathfrak{a}} \cdot E_{\Lambda_1} = E_{\mathfrak{a}^{-1}\Lambda_1} = E_{\frac{\lambda_1}{\lambda_2}\Lambda_2} \simeq E_{\Lambda_2}.$$

Zadnja jednakost slijedi iz činjenice da homotetične rešetke daju izomorfne eliptičke krivulje. Dakle, dokazali smo tranzitivnost ovog djelovanja. To da je djelovanje slobodno slijedi iz a) (iii).

□

Primjer 40. Neka je $\Lambda = \mathbb{Z}[i]$. Odredimo E_Λ. Vidmo da je $g_3(i\Lambda) = i^6 g_3(\Lambda) = -g_3(\Lambda)$, dakle $g_3(\Lambda) = 0$. Dakle, $E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x$, pa vidimo da je $j(E_\Lambda) = 1728$. Eliptička krivulja E_Λ je izomorfna nad $\mathbb{C}$ s $y^2 = x^3 + x$.

Analogno, pogledajmo $\Lambda = \mathbb{Z}[\zeta_3]$. Imamo da je $\zeta_3\Lambda = \Lambda$, pa je $g_2(\Lambda) = g_2(\zeta_3\Lambda) = \zeta_3^4 g_2(\Lambda) = \zeta^4 g_2(\Lambda)$, pa je $g_2(\Lambda) = 0$. Vidmo da je $j(E_\Lambda) = 0$, te da je E_Λ izomorfan nad $\mathbb{C}$ s $y^2 = x^3 + 1$.

Jedan od glavnih rezultata teorije kompleksnog množenja je da će torzijske točke neke eliptičke krivulje s kompleksnim množenje generirati Abelova proširenja nekih polja algerbarskih brojeva.

Definicija. Neka je $E \in \mathcal{ELL}(R)$, gdje je R red u kvadratnom imaginarnom polju, te neka je $\mathfrak{a}$ neki cijeli ideal od R. Definiramo

$$E[\mathfrak{a}] = \{P \in E : \alpha P = 0 \text{ za svaki } \alpha \in \mathfrak{a}\}.$$

Grupa $E[\mathfrak{a}]$ se naziva grupa $\mathfrak{a}$-torzijskih točaka od E.

Ako je $\mathfrak{a} = mR$, onda je $E[\mathfrak{a}] = E[m]$.

Neka je sada $\mathfrak{a}$ cijeli ideal od R takav da je $\Lambda \subseteq \mathfrak{a}^{-1}\Lambda$. Dakle, postoji kanonski homomorfizam

$$\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda, \quad z \mapsto z,$$

koji inducira kanonsku izogeniju

$$E_\Lambda \to \overline{\mathfrak{a}} \cdot E_\Lambda.$$

Propozicija 86. *Neka je $E \in \mathcal{ELL}(R)$, i neka je $\mathfrak{a}$ cijeli ideal u R. Tada*

(a) Grupa $E[\mathfrak{a}]$ je jezgra od kanonskog preslikavanja $E_\Lambda \to \overline{\mathfrak{a}} \cdot E_\Lambda$.

(b) Grupa $E[\mathfrak{a}]$ je slobodan $R/\mathfrak{a}$-modul ranga 1.

Dokaz. (a) Neka je Λ rešetka koja odgovara E. Fixirajući izomorfizam $\mathbb{C}/\Lambda \simeq E(\mathbb{C})$, imamo

$$E[\mathfrak{a}] \simeq \{z \in \mathbb{C}/\Lambda : \alpha z = 0 \text{ za sve } \alpha \in \mathfrak{a}\} = \{z \in \mathbb{C} : \alpha z \in \Lambda \text{ za sve } \alpha \in \mathfrak{a}\}/\Lambda$$
$$= \{z \in \mathbb{C} : z\mathfrak{a} \subseteq \Lambda\}/\Lambda = \mathfrak{a}^{-1}\Lambda/\Lambda = \ker(\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda) = \ker(E_\Lambda \to \overline{\mathfrak{a}} \cdot E_\Lambda).$$

(b) Vidite [8, Proposition 1.4. p.102]. □

Odmah dobivamo sljedeći korolar.

Korolar 87. *Neka je $E \in \mathcal{ELL}(R)$.*

(a) Za sve cijele ideale $\mathfrak{a}$ od R, preslikavanje $E_\Lambda \to \overline{\mathfrak{a}} \cdot E_\Lambda$ je stupnja $N_{K/\mathbb{Q}}(\mathfrak{a})$.

(b) Za svaki $\alpha \in R$, endomorfizam $[\alpha] : E \to E$ je stupnja $N_{K/\mathbb{Q}}(\alpha)$.

Dokaz. Jasno je da (b) slijedi iz (a) uzimanjem glavnog ideala $\mathfrak{a} = (\alpha)$. Tvrdnju (a) imamo iz

$$\deg(E_\Lambda \to \overline{\mathfrak{a}} \cdot E_\Lambda) = |E[\mathfrak{a}]|, \text{ prema Propoziciji 86 (a)}$$
$$= |R/\mathfrak{a}| = N_{K/\mathbb{Q}}(\mathfrak{a}), \text{ prema Propoziciji 86 (b).}$$

□

Poglavlje 15

Polja definicije

Kako nas zanimaju "aritmetička" pitanja, tj. svojstava PAB i eliptičkih krivulja nad PAB, bit će nam bitno odrediti koje je polje definicije neke eliptičke krivulje s kompleksnim množenjem s R.

Propozicija 88. *(a) Neka je $E/\mathbb{C}$ elitpička krivulja, $\sigma \in \mathrm{Aut}(\mathbb{C})$. Tada je* $\mathrm{End}(E) \simeq \mathrm{End}(E^\sigma)$.

(b) Neka je $E/\mathbb{C}$ elitpička krivulja s kompleksnim množenjem s $R := \mathcal{O}_K$ prsten cijelih nekog imaginarnog kvadratnog polja K. Tada je $j(E) \in \overline{\mathbb{Q}}$.

(c) $\mathcal{ELL}(R) \simeq \{$eliptičke krivulje $E/\overline{\mathbb{Q}}:\ \mathrm{End}\,E \simeq R\}/$izomorfizmi nad $\overline{\mathbb{Q}}$.

Dokaz. (a) Ovo je očito: ako je $\phi : E \to E$ endomorfizam od E, tada je $\phi^\sigma : E^\sigma \to E^\sigma$ endomorfizam od E^σ. Ovdje E^σ označava eliptičku krivulju na čije je koeficijente djelovano s σ.
(b) Neka je $\sigma \in \mathrm{Aut}(\mathbb{C})$. Lako se direktno provjeri da je $j(E)^\sigma = j(E^\sigma)$, pošto je j racionalna funkcija na koeficijentima od E. Međutim, ranije smo dokazali da ima konačno (točnije CL_K) eliptičkih krivulja s $\mathrm{End}\,E_{\mathbb{R}}$, a j-invariajanta određuje klasu izomorfizma (nad $\mathbb{C}$) od E. Dakle skup $\{j(E)^\sigma : \sigma \in \mathrm{Aut}\,\mathbb{C}\}$ je konačan. Slijedi da je $j(E)$ algebarski.
(c) Definirajmo da je

$$\mathcal{ELL}_F(R) \simeq \{\text{eliptičke krivulje } E/\overline{F}:\ \mathrm{End}\,E \simeq R\}/\text{izomorfizmi nad } F.$$

Promotrimo prirodno preslikavanje

$$\epsilon : \mathcal{ELL}_{\overline{\mathbb{Q}}}(R) \to \mathcal{ELL}_{\mathbb{C}}(R).$$

Trebamo dokazati da je ϵ bijekcija. Neka je $E/\mathbb{C}$ reprezent nekog elementa od $\mathcal{ELL}_{\mathbb{C}}(R)$. Tada je po točki (b) $j(E) \in \overline{\mathbb{Q}}$. Znamo da postoji eliptička krivulja $E'/\mathbb{Q}(j(E))$ takva da je $j(E') = j(E)$, te da su E i E' izomorfne nad $\mathbb{C}$. Dakle, $\epsilon(E') = E$, pa je ϵ surjekcija.

Dokažimo sada da je ϵ injekcija. Neka su $E_1/\overline{\mathbb{Q}}$ i $E_2/\overline{\mathbb{Q}}$ reprezenti elemenata od $\mathcal{ELL}_{\overline{\mathbb{Q}}}(R)$, te neka je $\epsilon(E_1) = \epsilon(E_2)$. Tada je $j(E_1) = j(E_2)$, te su E_1 i

E_2 izomorfni nad $\overline{\mathbb{Q}}$ (štoviše, izomorfni su and nekim poljem stupnja ≤ 6 nad $\mathbb{Q}(j(E_1))$. Dakle E_1 i E_2 su u istoj klasi u $\mathcal{ELL}_{\overline{\mathbb{Q}}}(R)$. Dakle, ϵ je injekcija. $\square$

Sada nas zanima polje definicija preslikavanja $[\alpha] : E \to E$, za $\alpha \in R$.

Teorem 89. *(a) Neka je $E/\mathbb{C}$ eliptička krivulja s kompleksnim množenjem s nekim prstenom $R \subseteq \mathbb{C}$. Tada je $([\alpha]_E)^\sigma = [\alpha^\sigma]_{E^\sigma}$ za sve $\alpha \in R$ i $\sigma \in \operatorname{Aut}\mathbb{C}$.*

(b) Neka je E eliptička krivulja definirana nad nekim poljem $L \subseteq \mathbb{C}$ s kompleksnim množenjem s nekim redom $R \subseteq K$, gdje je K imaginarno kvadratno polje. Tada su svi endomorfizmi od E definirani nad LK.

(c) Neka su E_1 i E_2 eliptičke krivulje definriane nad poljem $L \subseteq \mathbb{C}$. Tada postoji konačno proširenje L'/L takvo da su sve izogenije s E_1 u E_2 definirane nad L'.

Dokaz. Tvrdnju (a) nećemo dokazivati, dokaz se može naći na [8, p.106].
(b) Neka je $\sigma \in \operatorname{Aut}\mathbb{C}$ takav da fiksira L. Imamo da je $E = E^\sigma$, pošto je E definirana nad L. Po (a) imamo da je $([\alpha]_E)^\sigma = [\alpha^\sigma]_{E^\sigma} = [\alpha^\sigma]_E$. Ako σ fiksira i K i L, tada je $\alpha^\sigma = \alpha$. Dakle imamo da je $([\alpha]_E)^\sigma = [\alpha]_E$ za sve $\sigma \in \operatorname{Aut}\mathbb{C}$ koji fiksiraju LK, pa je $[\alpha]$ defiiran nad LK.
(c) Neka je $\phi : E_1 \to E_2$ izogenija. Za svaki $\sigma \in \operatorname{Aut}\mathbb{C}$ koji fixira L imamo da je $\phi^\sigma \in Hom(E_1, E_2)$. Dokazali smo da je svaka izogenija jedinstveno određena svojom jezgrom. Pošto svaka eliptička krivulja ima samo konačno mnogo podgrupa nekog fiksnog konačnog reda, te pošto su $\operatorname{Aut} E_1$ i $\operatorname{Aut} E_2$ konačni, zaključujemo da $\operatorname{Hom}(E_1, E_2)$ sadrži samo konačno mnogo izogenija nekog fiksnog stupnja. Dakle skup

$$\{\phi^\sigma : \sigma \in \operatorname{Aut}\mathbb{C}, \sigma \text{ fiksira } L\}$$

je konačan, pa je dakle ϕ definiran nad konačnim proširenjem od L. Sada koristimo činjenicu (vidi [7, Corollary III.7.5., p.91]) da je $\operatorname{Hom}(E_1, E_2)$ slobodan $\mathbb{Z}$-modul ranga najviše 4, te nakon što uzmemo kompozitum polja definicije svih generatora, tada će i svaki element od $\operatorname{Hom}(E_1, E_2)$ biti definiran nad tim poljem.

$\square$

Vidi [8, Remarks 2.2.1-2.2.3., p.107] za neke primjere i komentare.

Teorem 90. *Neka je $E/\mathbb{C}$ eliptička krivulja s kompleksnim množenjem s $\mathcal{O}_K$ imaginarnog kvadratnog polja K, te neka je*

$$L = K(j(E), E_{tors})$$

polje generirano s j-invarijanotom od E i s koordinatama svih torzijskih točaka od E. Tada je L Abelovo proširenje od $K(j(E))$.

Dokaz. Stavimo $H = K(j(E))$, te neka je $L_m = H(E[m])$. Pošto je L kompozitum svih L_m-ova, dosta je dokazati da je L_m Abelovo proširenje od H.

Neka je $\rho : \mathrm{Gal}(\overline{K}/H) \to \mathrm{Aut}(E[m])$ mod m Galoisova reprezentacija pridružena E. Za prouizvoljnu elitpičku krivulju, sve što možemo reći je da je slika od ρ sadržana u $\mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Međutim, u našem slučaju, činjenica da imamo kompleksno množenje će nam dati dodatne informacije. Teorem 89 (b) nam kaže da su svi endomorfizmi od E definirani nad H.

Dakle imamo da elementi od $\mathrm{Gal}(L_m/H)$ komutiraju s elementima od $\mathcal{O}_K$ u djelovanju na $E[m]$, tj. $([\alpha]T)^\sigma = [\alpha]T^\sigma$ za sve $\sigma \in \mathrm{Gal}(L_m/H)$, $T \in E[m]$ i $\alpha \in \mathcal{O}_K$.

Zaključujemo da pošto $E[m]$ nije samo $\mathbb{Z}/m\mathbb{Z}$-modul, nego $\mathcal{O}_K/m\mathcal{O}_K$ modul, da nam je ρ zapravo homomorfizam iz $\mathrm{Gal}(L_m/H)$ u grupu automorfizama od $E[m]$ kao $\mathcal{O}_K/m\mathcal{O}_K$-modula. Dakle, ρ inducira injekciju

$$\phi : \mathrm{Gal}(L_m/H) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_K/m\mathcal{O}_K} E[m].$$

Međutim, pošto je $E[m]$ slobodan $\mathcal{O}_K/m\mathcal{O}_K$-modul ranga 1 po 86 (b), imamo da je

$$\mathrm{Aut}_{\mathcal{O}_K/m\mathcal{O}_K} E[m] \simeq (\mathcal{O}_K/m\mathcal{O}_K)^\times,$$

te je očito $\mathrm{Gal}(L_m/H)$ Abelova. □

Neka je u daljnjoj argumentaciji $R = \mathcal{O}_K$ za neko kvadratno imaginarno polje K. Postoji prirodno djelovanje od $\mathrm{Gal}(\overline{K}/K)$ na $\mathcal{ELL}(R)$, koje šalje klasu od E u klasu od E^σ za svaki $\sigma \in \mathrm{Gal}(\overline{K}/K)$. S druge strane, pokazali smo da CL_K djeluje slobodno i tranzitivno na $\mathcal{ELL}(R)$. Dakle postoji jedinstveni $\overline{\mathfrak{a}} \in CL_K$ takav da je $\overline{\mathfrak{a}} \cdot E = E^\sigma$. Dakle, dobili smo dobro definirnao preslikavanje:

$$F : \mathrm{Gal}(\overline{K}/K) \to CL(R)$$

određeno s

$$E^\sigma = F(\sigma) \cdot E \text{ za sve } \sigma \in \mathrm{Gal}(\overline{K}/K).$$

Proučavanje ovog presalikavanja će nam biti ključno kako bi razumjeli polje $K(j(E))$. Dokazat ćemo da je F homomorfizam, te da F ne ovisi o izboru E (što nije očito iz definicije).

Sljedeću lemu ostavljamo bez dokaza. Dokaz se može naći u [8, p.113–115.]

Lema 91. *Neka je $E/\overline{\mathbb{Q}}$ eliptička krivulja koja je reprezent elementa iz $\mathcal{ELL}(R)$, te neka je $\overline{\mathfrak{a}}$. Tada je*

$$(\mathfrak{a} \cdot E)^\sigma = \overline{\mathfrak{a}}^\sigma \cdot E^\sigma.$$

Propozicija 92. *Neka je $K/\mathbb{Q}$ kvadratno imaginarno polje. Tada postoji homomorfizam*

$$F : \mathrm{Gal}(\overline{K}/K) \to CL(R) \tag{15.1}$$

koji je jedinstveno određen svojstvima

$$E^\sigma = F(\sigma) \cdot E \textit{ za sve } \sigma \in \mathrm{Gal}(\overline{K}/K) \textit{ i sve } E \in \mathcal{ELL}(R).$$

Dokaz. Prema prethodno dokazanom i argumentiranom, za svaki $\sigma \in \mathrm{Gal}(\overline{K}/K)$ postoji jedinstveni $\overline{\mathfrak{a}} \in CL_K$ takav da je $\overline{\mathfrak{a}} \cdot E = E^\sigma$.

Pokažimo da je F homomorfizam. Neka su $\sigma, \tau \in \mathrm{Gal}(\overline{K}/K)$. Tada je

$$F(\sigma\tau) \cdot E = E^{\sigma\tau} = (E^\sigma)^\tau = (F(\sigma) \cdot E)^\tau = F(\tau) \cdot (F(\sigma) \cdot E)) = (F(\sigma)F(\tau)) \cdot E.$$

Posljednja jednakost slijedi iz djelovanja $CL(K)$ na $\mathcal{ELL}(R)$, te iz toga što je $CL(K)$ Abelova grupa.

Ostaje nam dokazati da F ne ovisi o izboru eliptičke krivulje E. Neka su $E_1, E_2 \in \mathcal{ELL}(R)$ i neka je $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Neka su $\mathfrak{a}_1, \mathfrak{a}_2$ takvi da je $E_1^\sigma = \overline{\mathfrak{a}}_1 \cdot E_1$ i $E_2^\sigma = \overline{\mathfrak{a}}_2 \cdot E_2$. Trebamo pokazati da je $\overline{\mathfrak{a}}_1 = \overline{\mathfrak{a}}_2$. Pošto CL_K djeluje tranzitivno na $\mathcal{ELL}(R)$, postoji neki $\mathfrak{b}$ takav da je $E_2 = \overline{\mathfrak{b}} \cdot E_1$. Sada imamo

$$(\overline{\mathfrak{b}} \cdot E_1)^\sigma = E_2^\sigma = \overline{\mathfrak{a}}_2 \cdot E_2 = \overline{\mathfrak{a}}_2 \cdot (\overline{\mathfrak{b}} \cdot E_1) = (\overline{\mathfrak{a}}_2 \overline{\mathfrak{b}} \overline{\mathfrak{a}}_1^{-1}) \cdot E_1^\sigma,$$

pošto je $(\overline{\mathfrak{b}} \cdot E_1)^\sigma = \overline{\mathfrak{b}} \cdot E_1^\sigma$. Pošto je $\overline{\mathfrak{b}} = \overline{\mathfrak{b}}^\sigma$, pošto je $\mathfrak{b}$ ideal u K, tvrdnja slijedi iz Leme 91. □

15.1 Hilbertovo polje klasa

Sada nam je cilj dokazati sljedeći teorem.

Teorem 93. *Neka je $K/\mathbb{Q}$ kvadratno imaginarno polje s prstenom cijelih R i neka je* $\mathrm{End}\, E \simeq R$. *Tada je $K(j(E))$ Hilbertovo polje klasa H od K.*

Napomena. Primjetimo da je nije teško konstruirati eliptičku krivulju E koja zadovoljava $\mathrm{End}\, E \simeq R$. Možemo jednostavno uzeti E_R, gdje R promatramo kao rešetku. Tada imamo da je

$$j(E) = j(R) = 1728 g_2^3(R)/(g_2^3(R) - 27 g_3^2(R)).$$

Dokažimo sljedeću tehničku propoziciju koja će nam trebati.

Propozicija 94. *Neka je L PAB, $\mathfrak{P}$ maksimalni ideal od L, E_1 i E_2 eliptičke krivulje nad L s dobrom redukcijom u $\mathfrak{P}$, te neka su $\tilde{E}_1$ i $\tilde{E}_2$ njihove redukcije modulod $\mathfrak{P}$. Tada je redukcija modulo $\mathfrak{P}$*

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(\tilde{E}_1, \tilde{E}_2), \quad \phi \mapsto \tilde{\phi}$$

injektivno preslikavanje. Također, $\mathrm{st}\, \phi = \mathrm{st}\, \tilde{\phi}$.

Dokaz. Mi ćemo samo dokazati injektivnost, dok se dokaz očuvanja stupnjeva može naći u [8, p.124].

Neka je $\phi : E_1 \to E_2$ izogenija koja zadovoljava $\tilde{\phi} = [0]$. Znamo da je redukcija modulo $\mathfrak{p}$ injektivna na $E_2[m]$ ako $\mathfrak{p}$ ne dijeli m. Ako je $T \in E_1[m]$, tada je po pretpostavci $\widetilde{\Phi}(T) = \tilde{\phi}(\tilde{T}) = \tilde{O}$. Pošto je $T \in E_2[m]$, slijedi da je $\phi(T) = O$. Dakle $E_1[m] \subseteq \ker \phi$. Ovo vrijedi za sve m koje $\mathfrak{p}$ ne dijeli, dakle za proizvoljno velike m. Dakle, $\phi = [0]$. □

Sljedeća će nam propozicija dati dosta informacija o funkciji F iz 15.1. Ostavljamo je bez dokaza.

Propozicija 95. *Neka je K kvadratno imaginarno polje. Postoji konačan skup prostih brojeva ($\in \mathbb{Z}$) takvih da ako $p \notin S$, te ako se p cijepa u K, tj. $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, tada je*

$$F(\sigma_{\mathfrak{p}}) = \overline{\mathfrak{p}} \in CL(K),$$

gdje $\sigma_{\mathfrak{p}}$ Frobenius u $\mathfrak{p}$, a F je funkcija definirana u 15.1.

Dokžimo posljedice Propozicije 95.

Teorem 96. *Neka je E reprezent nekog elementa od $\mathcal{ELL}(R)$, gdje je R prsten glavnih od kvadratnog imaginarnog polja K. Tada*

(a) *$K(j(E))$ je Hilbertovo polje klasa H od K.*

(b) *$[\mathbb{Q}(j(E)) : \mathbb{Q}] = [K(j(E)) : K] = h_K$.*

(c) *Neka su $E_1, \dots E_h$ reprezenti za sve klase iz $\mathcal{ELL}(R)$. Tada su $j(E_1), \dots, j(E_h)$ svi $\mathrm{Gal}(\overline{K}/K)$ konujugati od $j(E)$.*

(d) *Za svaki prosti ideal $\mathfrak{p}$ od K,*

$$j(E)^{\sigma_{\mathfrak{p}}} = j(\overline{\mathfrak{p}} \cdot E).$$

Općenitije, za svaki razlomljeni ideal $0 \neq \mathfrak{a}$ od K, vrijedi

$$j(E)^{(\mathfrak{a}, H/K)} = j(\overline{\mathfrak{a}} \cdot E).$$

Dokaz. Neka je L fiksno polje jezgre od $F : \mathrm{Gal}(\overline{K}/K) \to CL(K)$. Pošto je $\ker F$ konačnog indeksa u $\mathrm{Gal}(\overline{K}/K)$, slijedi da je L končno proširenje od K, te pošto je $\ker F$ normalna, slijedi da je L/K normalno proširenje. Štoviše, pošto je

$$\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\overline{K}/L)/\ker F \simeq CL(K),$$

slijedi da je L/K Abelovo. Imamo

$$\mathrm{Gal}(\overline{K}/L) = \ker F = \{\sigma \in \mathrm{Gal}(\overline{K}/K) : F(\sigma) = 1\}$$
$$= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : F(\sigma) \cdot E = E\}.$$

Zadnja jednakost vrijedi jer $CL(K)$ djeluje slobodno na $\mathcal{ELL}(R)$. Nadalje, imamo

$$\{\sigma \in \mathrm{Gal}(\overline{K}/K) : F(\sigma) \cdot E = E\} = \{\sigma \in \mathrm{Gal}(\overline{K}/K) : E^{\sigma} = E\}$$
$$= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : j(E^{\sigma}) = j(E)\} = \{\sigma \in \mathrm{Gal}(\overline{K}/K) : j(E)^{\sigma} = j(E)\}$$
$$= \mathrm{Gal}(\overline{K}/K(j(E))).$$

Dakle $L = K(j(E))$. Neka je $\mathfrak{f}$ konduktor od L/K. Promotrimo sad kompoziciju Artinovog presliakvanja i F

$$I_{\mathfrak{f}} \xrightarrow{(\cdot,L/K)} \mathrm{Gal}(L/K) \xrightarrow{F} CL(K).$$

Tvrdimo da je ovo preslikavanje prirodna projekcija, tj. da je

$$F((\mathfrak{a}, L/K)) = \overline{\mathfrak{a}} \quad \text{za sve } \mathfrak{a} \in I_f.$$

Dokažimo to. Neka je $\mathfrak{a} \in I_{\mathfrak{f}}$ i neka je S skup (konačan) svih prostih brojeva koji zadovoljavaju neko od sljedećih svojstava:

(i) p se grana u L.

(ii) Neki od E_i-ova ima lošu redukciju u nekom prostom idealu od L koji dijeli p.

(iii) p dijeli ili brojnik ili nazivnik od $N(j(E_i) - j(E_k))$ za neke $i \neq k$.

U dokazu ćemo koristiti nešto jaču verziju generaliziranog Dirichletovog teorema: u svakoj generaliziranoj klasi postoji beskonačno mnogo prostih ideala inercijskog stupnja 1. Sada nam (generalizirani) Dirichletov teorem kaže da postoji prosti prosti ideal $\mathfrak{p}$ u svakoj $P_{\mathfrak{f}}$-klasi inercijskog stupnja 1, (tj. ideal od $\mathbb{Z}$ nad njim se grana) koji nije iz S. Neka je $\mathfrak{p}$ takav koji je u istoj klasi kao i $\mathfrak{a}$. Dakle, postoji $\alpha \in K^*$ takav da je

$$\alpha \equiv 1 \pmod{\mathfrak{f}} \text{ i } \mathfrak{a} = (\alpha)\mathfrak{p}.$$

Imamo da je

$$\begin{aligned}
F((\mathfrak{a}, L/K)) &= F((\alpha)\mathfrak{p}, L/K) && (15.2)\\
&= F((\mathfrak{p}, L/K)) \qquad \text{jer je } (\alpha) \in P_{\mathfrak{f}} && (15.3)\\
&= \overline{\mathfrak{p}} \qquad \text{zbog Propozicije 95} && (15.4)\\
&= \overline{\mathfrak{a}} \qquad \text{jer } \overline{\mathfrak{a}} = \overline{\mathfrak{p}} && (15.5)
\end{aligned}$$

Primjetimo da je direktna posljedica da je

$$F(((\alpha), L/K)) = 1 \text{ za sve glavne ideale } (\alpha) \in I_{\mathfrak{f}}.$$

Također znamo da je $F : \mathrm{Gal}(L/K) \to CL(K)$ injektivno, pa je

$$((\alpha), L/K) = 1$$

za sve $(\alpha) \in I_{\mathfrak{f}}$. Međutim, znamo d aje konduktor $\mathfrak{f}$ najmanji cijeli ideal od K takav da zadovoljava

$$\alpha \equiv 1 \pmod{\mathfrak{f}} \Longrightarrow ((\alpha), L/K) = 1.$$

Dakle $\mathfrak{f} = (1)$, dakle L/K je nerazgranto po svojstvima konduktora. Dakle, L je sadržano u Hilbertovom polju klasa H od K.

Primjetimo sada da je prirodno preslikavanje $I(1) \to CL(K)$ očito surjektivno, pa zaključujemo i da je $F : \mathrm{Gal}(L/K) \to CL(K)$ surjektivno, pa time i izomorfizam. Dakle imamo da je

$$[L : K] = \# \mathrm{Gal}(L/K) = \#CL(K) = \# \mathrm{Gal}(H/K) = [H : K],$$

pa zajedno s $L \subseteq H$, to nam daje $L = H$. Time smo dokazali (a) i drugu jednakost u (b).

Sjetimo se da smo prethodni put dokazali da je $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq \#\mathcal{ELL}(\mathcal{O}_K) = h_K$. Pošto je

$$h_K = [K(j(E)) : K] \leq [\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_k,$$

imamo da su u gornjoj jednadžbi svugdje jednakosti, što dokazuje (b).

Znamo da $CL(K)$ tranzitivno djeluje na skup j-invarijanti

$$J = \{j(E_1), \dots, j(E_h)\}.$$

Preslikavanje $F : \mathrm{Gal}(\overline{K}/K) \to CL(K)$ se definira tako da oba skupa djeluju na isti način na J, dakle zaključujemo da $\mathrm{Gal}(\overline{K}/K)$ tranzitivno djeluje na J. Dakle J je potpuni skup Galoisovih kojugata od $j(E)$, što dokazuje (c).

(d) slijedi iz dokazane tvrdnje za $I_{\mathfrak{f}}$. Pošto je $\mathfrak{f} = (1)$, tvrdnja je dokazana za sve razlomljene ideale. $\square$

Poglavlje 16

Maksimalno Abelovo proširenje

Prije nego što krenemo dalje, iskažimo sljedeću slabu verziju Artinovog reciprociteta (vidi [8, Proposition 3.3.1]) koju smo zapravo koristili i u prethodnom poglavlju.

Propozicija 97 (Artinov reciprocitet)**.** *Neka je L/K konačno Abelovo proširenje. Tada postoji ideal $\mathfrak{f}$ od $\mathcal{O}_K$, koji je djeljiv točno s onim prostim idealima koji se granaju u L/K, takav da*

$$((\alpha), L/K) = 1 \text{ za sve } \alpha \in K^\times \text{ takvi da } \alpha \equiv 1 \pmod{\mathfrak{f}}.$$

Ideal $\mathfrak{f}$ u prethodnoj propoziciji je naravno konduktor. Primjetimo da propozicija kaže da ako je L Hilbertovo polje klasa, tada je $((\alpha), L/K) = 1$ za sve $\alpha \in K^\times$. Također prisjetimo da se idela od K potpuno cijepa u L ako i samo ako je glavni (u K).

Neka je, kao i do sada E eliptička krivulja s kompleksnim množenjem s $R = \mathcal{O}_K$, te neka je $H = K(j(E))$ Hilbertovo polje klasa od K. Pošto je $j(E) \in H$, možemo uzeti da E ima koeficijente iz H. Ako je $\mathfrak{p}$ ideal od H koji dijeli p, primjetimo da $E \pmod{\mathfrak{p}} =: \tilde{E}$ ima izogeniju $E \to E^{(p)}, (x, y) \mapsto (x^p, y^p)$. Taj endomorfizam $\in \operatorname{End} \tilde{E}$ zovemo Frobenius. Sljedeća propozicija nam govori da je Frobenius redukcija neke izogenije nad H.

Propozicija 98. *Neka je K kvadratno imaginarno polje, H Hilbertovo polje klasa od K, E/H eliptička krivulja s kompleksnim množenje s R. Neka je $\sigma_\mathfrak{p} \in \mathrm{Gal}(H/K)$ takav da je $\sigma_\mathfrak{p} = (\mathfrak{p}, H/K)$ za prosti ideal $\mathfrak{p}$ od $\mathcal{O}_K$, te neka je $\mathfrak{P}$ ideal od $\mathcal{O}_H$ nad $\mathfrak{p}$. Ako je $\mathfrak{p}$ stupnja 1 (pod tim mislimo da je $[k(\mathfrak{p}) : \mathbb{F}_p] = 1$) i nije u skupu S definiranom u dokazu Teorema 96, te time E ima dobru redukciju u $\mathfrak{P}$. Tada postoji izogenija*

$$\lambda : E \to E^{\sigma_\mathfrak{p}}$$

čija je redukcija modulo $\mathfrak{P}$

$$\tilde{\lambda} : \tilde{E} \to \tilde{E}^{(p)}$$

Dokaz. Vidi dokaz[8, Proposition III.5.3, p.132] □

Korolar 99. *Neka je K kvadratno imaginarno polje, H Hilbertovo polje klasa od K, E/H eliptička krivulja s kompleksnim množenjem s R. Za skoro sve proste ideale $\mathfrak{p}$ od K, takve da je $(\mathfrak{p}, H/K) = 1$, postoji jedinstveniu $\pi \in R$ takav da je redukcija od $[\pi] : E \to E$ jednaka Frobeniusu $\tilde{E} \to \tilde{E}$.*

Dokaz. Neka je $\mathfrak{P}$ prost ideal koji leži nad $\mathfrak{p}$ (koji sam leži nad p) koji zadovoljava pretpostavke propozicije. Po prethodnoj propoziciji imamo da je redukcija od $\lambda : E \to E^{\sigma_{\mathfrak{p}}}$ jednaka Frobeniusu $\phi : \tilde{E} \to \tilde{E}^{(p)}$.

Po pretpostavci je $(\mathfrak{p}, H/K) = 1$, pa je $\sigma_{\mathfrak{p}} = id$, dakle λ je endomorfizam, pa je on množenje s nekim $\pi \in R$. To implicira da je $\tilde{E} = \tilde{E}^{(p)}$. Sada imamo da je $N(\mathfrak{p}) = p = \operatorname{st}\phi = \operatorname{st}[\pi] = |N(\pi)|$, pa imamo da pošto je $\mathfrak{p}$ prost ideal u kvadratnom polju K, da je $\mathfrak{p} = \pi R$ ili $\mathfrak{p} = \overline{\pi} R$.

Jedinstvenost nećemo dokazivati □

Prisjetimo se da nam Kronecker-Weberov teorem kaže da je maksimalno Abelovo proširenje od $\mathbb{Q}$ genrirano s korijenima od jedinice, ili ekvivalentno s torzijskim točkama grupe $\mathbb{C}^{\times}$.

Naš cilj u ovom poglavlju je naći maksimalno Abelovo proširenje od K. Bilo bi dobro kada bi torzijske točke od E s $\operatorname{End} E = R$ generirale maksimalno Abelovo proširenje od K. Međutim, to nije istina: one će generirati maksimalno abelovo proširenje od $H := K(j(E))$.

Neka je

$$h : E \to E/\operatorname{Aut}(E) \simeq \mathbb{P}^1$$

morfizam definiran nad H; takav morizam se zove *Weberova funkcija* za E/H.

Primjer 41. Neka je

$$E : y^2 = x^3 + ax + b, \quad a, b \in H.$$

Tada imamo sljedeću Weberovu funkciju:

$$h(P) := h(x, y) = \begin{cases} x & ab \neq 0 \\ x^2 & b = 0 \\ x^3 & a = 0. \end{cases}.$$

Da bi generirali Abelova proširenja od K, koristit ćemo Weberovu funkciju od E, dakle u osnovi ćemo dodavati x-koordinate od torzijskih točaka.

Imamo sljedeći teorem:

Teorem 100. *Neka je K kvadratno imaginarno polje, E eliptička krivulja s kompleksnim množenjem s R, i neka je $h : E \to \mathbb{P}^1$ Weberova funkcija iz prethodnog primjera. Neka je $\mathfrak{m}$ (cijeli) ideal od R. Tada je polje*

$$K(j(E), h(E[\mathfrak{m}]))$$

polje klasa od K zrake $\mathfrak{m}$.

Dokaz. Neka je $L = K(j(E), h(E[\mathfrak{m}]))$. Tada je $L \supseteq K(j(E))$, te znamo da je $H := K(j(E))$ Hilbertovo polje klasa od K. Da bi dokazali da je L polje klasa od K zrake $\mathfrak{m}$ trebamo pokazati da je

$$(\mathfrak{p}, L/K) = 1 \Longleftrightarrow \mathfrak{p} \in P_{\mathfrak{m}},$$

za sve osim konačno mnogo prostih idela u K. Ovdje opet možemo iskoristiti činjenicu da u svakoj klasi od $I_{\mathfrak{m}}/P_{\mathfrak{m}}$ ima beskonačno mnogo prostih ideala stupnja 1, pa je dosta tvrdnju dokazati za ideale stupnja 1, pošto Frobenius ovisi samo o klasi u kojoj je $\mathfrak{p}$ (klasa ne mora apriori biti modulo $P_{\mathfrak{m}}$, ali mora biti modulo neka generalizirana klasa ideala H).

Pretpostavimo da je $\mathfrak{p}$ prost ideal od K stupnja 1 takav da je $\mathfrak{p} \in P_{\mathfrak{m}}$. Znači da je

$$\mathfrak{p} = \mu R \text{ za neki } \mu \in R \text{ takav da je } \mu \equiv 1 \pmod{\mathfrak{m}}.$$

Dakle, po definciji, $\mathfrak{p}$ je glavni ideal pa je $(\mathfrak{p}, H/K) = 1$. Dakle, možemo primjeniti prethodnu propoziciju da bismo dobili neki $\pi \in R$ takav da je $\mathfrak{p} = \pi R$ i da je redukcija množenja s $\pi : E \to E$ jednaka Frobeniusu $\tilde{E} \to \tilde{E}$. Zaključujemo da je $\pi R = \mathfrak{p} = \mu R$, pa je $\pi = \xi\mu$ za neki $\xi \in R^{\times}$. Pošto je $[\xi] \in \operatorname{Aut} E$, $[\pi]$ i $[\mu]$ se razlikuju za neki automorfizam od E.

Znamo da $(\mathfrak{p}, L/K)$ fiksira $H = K(j(E))$, pa da bi dokazali da fiksira L, moramo dokazati da fiksira $h(E[\mathfrak{m}])$. Neka je $T \in E[\mathfrak{m}]$ bilo koja $\mathfrak{m}$-torzijska točka. Tada imamo da je

$$\widetilde{T^{(\mathfrak{p}, L/K)}} = \phi(\tilde{T}) = \widetilde{[\pi]T},$$

gdje je ϕ Frobenius. Kao i prije, znamo da je redukcija modulo $\mathfrak{p}$ injektivna na $E[\mathfrak{m}]$ za sve $\mathfrak{p}$ relativno proste s $\mathfrak{m}$. Dakle imamo da je

$$T^{(\mathfrak{p}, L/K)} = [\pi]T.$$

Sada imamo da je

$$\begin{aligned} h(T)^{(\mathfrak{p}, L/K)} &= h(T^{(\mathfrak{p}, L/K)}) \text{ jer je } (\mathfrak{p}, H/K) = 1 \text{ i } h \text{ je definiran nad } H, \\ &= h([\pi]T) = h([\xi] \circ [\mu]T) = h([\mu]T) \text{ pošto je } h \text{ cijepanje s } \operatorname{Aut} E, \\ &= h(T) \text{ pošto je } T \in E[\mathfrak{m}], \text{ te } \mu \equiv 1 \pmod{\mathfrak{m}}. \end{aligned}$$

Dakle dokazali smo $\mathfrak{p} \in P_{\mathfrak{m}} \Longrightarrow (\mathfrak{p}, L/K) = 1$.

Dokažimo sada obrat. Neka je $\mathfrak{p}$ prost ideal stupnja 1 koji zadovoljava $(\mathfrak{p}, L/K) = 1$. Tada je $(\mathfrak{p}, H/K) = (\mathfrak{p}, L/K)|_H = 1$. Kao i prije, postoji $\pi \in R$ takav da je Frobenius ϕ reduckija od $[\pi] : E \to E$.

Izaberimo $\sigma \in \operatorname{Gal}(\overline{K}/K)$ čija je restrikcija na L je $(\mathfrak{p}, L/K) = 1$. Neka je sada $T \in E[\mathfrak{m}]$. Imamo da je

$$\begin{aligned}
\tilde{h}(\tilde{[\pi]}\tilde{T}) &= \tilde{h}(\widetilde{[\pi]T}) = \tilde{h}(\phi(\tilde{T})) \\
&= \tilde{h}(\widetilde{T^\sigma}) && \text{jer se } \sigma \text{ reducira u } \phi \\
&= \widetilde{h(T^\sigma)} = \widetilde{h(T)^\sigma} && \text{jer je } \sigma|_H = 1, \text{ te je } h \text{ definiran nad } H \\
&= \widetilde{h(T)} && \text{jer je } h(T) \in L \text{ in } \sigma|_L = 1. \\
&= \tilde{h}(\tilde{T}).
\end{aligned}$$

Sada primjetimo da je redukcija $\tilde{h}$ modulo $\mathfrak{P}$ od h preslikavanje

$$\tilde{h} : \tilde{E} \to \widetilde{E/\operatorname{Aut} E} \simeq \tilde{E}/\widetilde{\operatorname{Aut} E}.$$

Iz ove činjenice i i pošto je $h(\widetilde{[\pi]}\tilde{T}) = \tilde{h}(\tilde{T})$, slijdi da postoji automorfizam $[\xi] \in \operatorname{Aut} E$ takav da je $\widetilde{[\pi]}\tilde{T} = \widetilde{[\xi]}\tilde{T}$. Pošto je, kao i prije redukcija mod $\mathfrak{P}$ na $E[\mathfrak{m}]$ injektivna, imamo da je $[\pi - \xi]T = O$. Pošto znamo da je $E[\mathfrak{m}]$ slobodan $R/\mathfrak{m}$-modul ranga 1, slijedi da postoji jedinstven $\xi \in R^\times$ takav da $[\pi - \xi]$ poiništava cijeli $E[\mathfrak{m}]$ (izaberemo T takav da je generator of $E[\mathfrak{m}]$ kao $R/\mathfrak{m}$-modula). Dakle imamo da je $\pi \equiv \xi \pmod{\mathfrak{m}}$, pa je $\xi^{-1}\pi \equiv 1 \pmod{\mathfrak{m}}$. Dakle, imamo da je $\mathfrak{p} = \pi R = (\xi^{-1}\pi)R$, pošto je ξ jedinica u R. Dakle $\mathfrak{p} \in P_\mathfrak{m}$, što smo i htjeli dokazati.

□

Korolar 101. *Koristeći notaciju iz prethodnog teorema, imamo da je*

$$K^{ab} = K(j(E), h(E_{tors})).$$

Dokaz. Neka je L/K neko konačno Abelovo proširenje i $\mathfrak{f}$ konduktor od L/K. Po TPK, imamo da je L sadržan u polju klasa od K zrake $\mathfrak{f}$. Po prethodnom teoremu, to znači da je $L \subseteq K(j(E), h(E[\mathfrak{f}]))$. Ako uzmem kompozitum po svim konduktorima dobijemo $L \subseteq K(j(E), h(E_{tors}))$, te ako uzmemo kompozitum po svim Abelovim proširenjima od L imamo da je $K^{ab} \subseteq K(j(E), h(E_{tors}))$. Međutim, prošli teorem nam kaže da je $K(j(E), h(E_{tors}))$ kompozitum Abelovih proširenja, pa je sadržan u K^{ab}, dakle $K(j(E), h(E_{tors})) = K^{ab}$. □

Poglavlje 17

Integralnost j-invarijante

U ovom poglavlju ćemo dokazati (tj. skicirati dokaz) da je j-invarijanta cijeli algebarski broj. Postoje tri dokaza ove činjenice: mi ćemo tvrdnju dokazati "p-adskim" pristupom (to je Serreov dokaz).

Prvo ćemo promotiriti eliptičke krivulje nad p-adskim poljima.

17.1 Tateova krivulja

Kao što smo konstruirali eliptičke krivulje nad $\mathbb{C}$ kao kvocijent od $\mathbb{C}$ s diskretnom podgrupom Λ, slično želimo napraviti i nad $\mathbb{Q}_p$. Međutim, ovaj pristup odmah ne uspijeva: neka je $\Lambda \leq \mathbb{Q}_p$ neka netrivijalna podgrupa, te neka je $0 \neq t \in \Lambda$. Tada imamo da je

$$p^n t \in \Lambda \text{ za sve } n \geq 0 \text{ i } \lim_{n\to\infty} p^n t = 0,$$

pa je 0 gomilište od Λ, dakle ne postoje diskretne podrupe od $\mathbb{Q}_p$.

Međutim promijenimo pristup (koristeći Tateovu ideju): imamo da je $z \mapsto e^{2\pi i z}$ surjektivni homomorfizam grupa iz $\mathbb{C}$ u $\mathbb{C}^\times$ s jezgrom $\mathbb{Z}$, dakle $\mathbb{C}/\mathbb{Z} \simeq \mathbb{C}^*$. Neka je $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, te neka je $q = e^{2\pi i\tau}$, sada vidimo da je

$$\mathbb{C}/\Lambda \simeq \mathbb{C}^*/q^{\mathbb{Z}},$$

te je ovo alternativan način zapisivanja eliptičkih krivulja nad $\mathbb{C}$. Tateova ideja je isto napraviti nad $\mathbb{Q}_p$, pošto $\mathbb{Q}_p^\times$ ima puno diskretenih podgrupa. Na primjer za $|q| < 1$ imamo $q^{\mathbb{Z}} = \{q^n : n \in \mathbb{Z}\}$, te će nam $\mathbb{Q}_p^\times/q^{\mathbb{Z}}$. Od sada nadalje pretpostavljamo da je $|q| < 1$.

Teorem 102 (Tate)**.** *Neka je K p-adsko polje (konačno proširenje od $\mathbb{Q}_p$). Postoje nizovi $a_4(q)$ i $a_6(q)$ koji konvergiraju u K, te **Tateova krivulja***

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

s

$$j(E_q) = \frac{1}{q} + 744 + 196884q + \dots,$$

te surjektivni homomorfizam

$$\phi : \overline{K}^{\times} \to E_q(\overline{K})$$

s jezgrom $q^{\mathbb{Z}}$. *Štoviše, preslikavanje* ϕ *je kompatibilno s djelovanjem grupe* $\mathrm{Gal}(\overline{K}/K)$ *u smislu da je*

$$\phi(u^\sigma) = \phi(u)^\sigma \textit{ za sve } u \in \overline{K}^{\times}, \sigma \in \mathrm{Gal}(\overline{K}/K).$$

Posljedično, za vako algebarsko proširenje L/K, ϕ *inducira izomorfizam*

$$\phi : L^{\times}/q^{\mathbb{Z}} \to E_q(L).$$

Napomena. Precizniji iskaz, s eksplicitno opisanim a_4, a_6, ϕ, te dokaz teorema se može naći u [8, Poglavje V.3]. Primjetimo da izomorfizam $\mathbb{C}^*/q^{\mathbb{Z}} \simeq E(\mathbb{C})$ nije kompatibilan s djelovanjem Galoisove grupe, dakle u p-adskom slučaju se sve posebno lijepo izgleda.

17.2 Eliptičke krivulje nad p-adskim poljima

Tateov teorem nam kaže da je za svaki q, takava da je $|q| < 1$, $K^{\times}/q^{\mathbb{Z}}$ izomorfno s $E_q(K)$. Tako možemo dobiti svaku eliptičku korvilju s valuacijom većom od od 1. To je očito nuža uvjet pošto je

$$|j(E_q)| = \left|\frac{1}{q} + 744 + 196884q + \dots\right| = \left|\frac{1}{q}\right| > 1.$$

Lema 103. *Neka je* $\alpha \in \overline{\mathbb{Q}}_p$ *takav da je* $|\alpha| > 1$. *Tada postoji jedinstveni* $q \in \mathbb{Q}_p(\alpha)^{\times}$, *za koji je* $|q| < 1$ *takav da je* $j(E_q) = \alpha$.

Iskažimo sada Tateov teorem o uniformizaciji.

Teorem 104 (Tateov teorem o uniformizaciji)**.** *Neka je* K *p-adsko polje,* E/K *eliptička krivulja, s* $|j(E)| > 1$. *Tada postoji jedinstveni* $q \in K^*$, $|q| < 1$ *takav da je* E *izomorfan nad* $\overline{K}$ *s Tateov krivuljom* E_q. *Također,* E *je izomorfan nad* E_q *nad* K *ako i samo ako* E *ima rascijepanu multiplikativnu redukciju.*

Napomena. Tateov teorem o uniformizaciji nam kaže da će E biti izomfran s E_q nad kvadratnim proširenjem od K.

17.3 Cjelobrojnost j-invartijante

Propozicija 105. *Neka je* K *p-adsko polje s normaliziranom valuacijom* v, E/K *eliptička krivulja,* $|j(E)| > 1$, *te neka je* $\ell \geq 3$ *prost broj koji ne dijeli*

$v(j(E))$. Tada postoji element σ u inercijskoj podgrupi od $\mathrm{Gal}(\overline{K}/K)$ koji djeluje na ℓ-torzijsku podgrupu $E[\ell]$ od E kao matrica $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, tj. postoji baza $P_1, P_2 \in E[\ell]$ takva da je

$$P_1^\sigma = P_1 \text{ i } P_2^\sigma = P_1 + P_2.$$

Dokaz. Prvo primjetimo da ako je L/K konačno proširenje stupnja relativno prostog s ℓ, tada ako je tvrdnja istinita za L, istinita je i za K. To slijedi jer, ako je w valuacija u L, tj. proširenje od v, tada je $w(j(E)) = e \cdot v(j(E))$. Pošto e dijeli $[L : K]$, imamo da je e relativno prost s ℓ, tada postoji $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, (koji je reda ℓ) u $\mathrm{Gal}(\overline{K}/K)$ ako i samo ako postoji u $\mathrm{Gal}(\overline{K}/L)$.

Po Tateov teoremu o uniformizaciji, E je izomrofna nad kvadratnim poljem nekoj Tateovoj krivulji s E_q. Dakle možemo pretpostaviti da sve radimo nad tim kvadratnim proširenjem, te dokazivati tvrdnju za E_q, gdje je $q \in K^*$. Također možemo dodati u polje $\zeta = \zeta_\ell$, primitivni ℓ-ti korijen iz jedinice, pošto tada dobivamo proširenje stupnja koje dijeli $\ell - 1$, te koje je očito relativno prostog stupnja s ℓ. Nazovimo to novo polje opet K.

Neka je $Q = q^{1/\ell} \in \overline{K}$ fiksan ℓ-ti korijen iz q. Kummerova teorija nam kaže da je $K(Q)/K$ potpuno razgranato proširenje stupnja ℓ, pa postoji σ u inerciiskoj podgrupi od $\mathrm{Gal}(\overline{K}/K)$ takav da je $Q^\sigma = \zeta Q$. Tvrdimo da je to upravo traženi σ nakon dobrog izbora baze za $E_q[\ell]$. Sjetimo se da je

$$E_q(\overline{K}) \simeq \overline{K}^\times / q^{\mathbb{Z}}.$$

Uz ovu identifikaciju imamo da očito Q i ζ generiraju $E_q[\ell]$. Pošto djelovanje od $\mathrm{Gal}(\overline{K}/K)$ komutira s uniformizacijom imamo da je djelovanje od $\mathrm{Gal}(\overline{K}/K)$ na $E_q[\ell]$ određeno djelovanjem na Q i ζ. Neka su $\phi(\zeta)$ i $\phi(Q)$ baza za $E_q[\ell]$, gdje je ϕ izomorizam između $E_q(\overline{K})$ i $\overline{K}^\times / q^{\mathbb{Z}}$.

Sada imamo da je

$$P_1^\sigma = \phi(\zeta)^\sigma = \phi(\zeta^\sigma) = \phi(\zeta) = P_1,$$
$$P_2^\sigma = \phi(Q)^\sigma = \phi(Q^\sigma) = \phi(\zeta Q) = \phi(\zeta) + \phi(Q) = P_1 + P_2.$$

□

Primjetimo da je ova propozicija istinita i nad poljima algebarskih brojeva.

Korolar 106. *Neka je $K/\mathbb{Q}$ polje algebarskih brojeva, E/K eliptička krivulja, i pretpostavimo da j-invarijanta nije iz O_K. Tada za sve ocim konačno mnogo prostih projeva ℓ, mod ℓ repreztnetacija pridružena E $\rho_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[\ell])$ sadrži element*

$$\rho_\ell(\sigma) \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \pmod{\ell}$$

s obzirom na neku bazu od $E[\ell]$.

Dokaz. Neka je v konačno mjesto od K takvo da je $|j(E)|_v > 1$. Neka je $\mathrm{Gal}(\overline{K}_v/K_v) \leq \mathrm{Gal}(\overline{K}/K)$. Po prethodnom rezultatu postoji $\sigma \in \mathrm{Gal}(\overline{K}_v/K_v)$ koji djeluje kao $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ na $E[\ell]$. Pošto imamo da je $E[\ell] \subseteq \overline{K} \subseteq \overline{K}_v$, gotovi smo. □

Teorem 107. *Neka je $K/\mathbb{Q}$ polje algebarskih brojeva, E/K eliptička krivulja takva da je $j(E) \notin \mathcal{O}_K$. Tada je* $\mathrm{End}\, E = \mathbb{Z}$.

Dokaz. Neka je ℓ prost broj. Prvo konstruiramo reprezentaciju nekog endomorfizma

$$\mathrm{End}\, E \to \mathrm{End}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

određenog djelovanjem endomorfizma na $T_\ell E$. Koristimo činjenicu da je

$$\deg \psi \equiv \det \psi \pmod{\ell}$$

kojeg nećemo dokazivati.

Neka je $\psi \in \mathrm{End}\, E$ izogenija. Readeći, ako je potrebno nad konačnim proširenjem od K, možemo pretpostaviti da je E definirana nad K. Dakle

$$\psi(P^\sigma) = \psi(P)^\sigma \text{ za sve } \psi \in \mathrm{Gal}(\overline{K}/K) \text{ i sve } P \in \mathrm{Gal}(\overline{K}/K),$$

dakle djelovanje od ψ i σ na $E[\ell]$ komutira. Tvrdimo da je $\psi \in \mathbb{Z}$. Neka je $m = \deg(1+\psi) - \deg(\psi) - 1$. Kad bi ψ bio u $\mathbb{Z}$, tada bi bilo $m = 2\psi$. Upravo ćemo to htjeti dokazati. Neka je $\sigma \in \mathrm{Gal}(\overline{K}/K)$ takav da je

$$\rho_l(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

u nekoj bazi $\{P_1, P_2\}$; ovo je po prethodnom korolaru istina za sve osim konačno mnogo prostih ℓ-ova. Analogno, imamo da je

$$\psi = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

za neke $a, b, c, d \in \mathbb{Z}/\ell\mathbb{Z}$. Pošto djelovanje od ψ i σ na $E[\ell]$ komutira, imamo da je

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

dobijemo da je $a = d$ i $c = 0$, dakle

$$\psi_\ell = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}.$$

Sada imamo da je

$$\begin{aligned}
m &= \deg(1+\psi) - \deg(\psi) - 1 \\
&\equiv \det(1+\psi) - \det(\psi) - 1 \equiv \det \begin{pmatrix} 1+a & b \\ 0 & 1+a \end{pmatrix} - \det \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} - 1 \pmod{\ell} \\
&\equiv 2a \pmod{\ell}
\end{aligned}$$

□

Sada imamo da je

$$\deg(m-2\psi) \equiv \det(m-2\psi) \equiv \det \left[\begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix} - 2 \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \right] \equiv m^2 - 4a^2 \equiv 0 \pmod{\ell},$$

pošto je $m - 2a \equiv 0 \pmod{\ell}$. Dakle imamo da je $\deg(m - 2\psi) \equiv 0 \pmod{\ell}$ za sve osim konačno mnogo ℓ-ova, pa možemo zaključiti da je $\deg(m - 2\psi) = 0$, dakle $m = 2\psi$. Znamo da je ψ cijeli algebarski broj, pa poošto je $m \in \mathbb{Z}$, zaključujemo da je i $\psi \in \mathbb{Z}$. Dakle $\operatorname{End} E = \mathbb{Z}$.

Bibliografija

[1] N. Childress, Class Field Theory, Springer, 2009.

[2] K. Conrad, History of Class Field Theory, `www.math.uconn.edu/~kconrad/blurbs/gradnumthy/cfthistory.pdf`

[3] D. A. Cox, Primes of the form $x^2 + ny^2$, : Fermat, Class Field Theory, and Complex Multiplication, 2nd Edition, Wiley, 2013.

[4] G. Janusz, Algebraic Number Fields, Academic Press, New York, 1973.

[5] H. Lenstra and P. Stevenhagen, *Chebotarev and his density theorem*, The Mathematical Inteligencer, **18** (1996), 26–37. `http://www.math.leidenuniv.nl/~hwl/papers/cheb.pdf`

[6] J. S. Milne, Class Field Theory, `www.jmilne.org/math/CourseNotes/CFT310.pdf`

[7] J. Silverman, Arithmetic of Elliptic Curves, 2nd edition, Springer, 2009.

[8] J. Silverman, Anvanced Topics in the Arithmetic of Elliptic Curves, Springer, 1994.

[9] P. Stevenhagen, Class Field Theory, `websites.math.leidenuniv.nl/algebra/Stevenhagen-CFT.pdf`