ПОЛИНОМИ И АЛГЕБАРСКЕ ЈЕДНАЧИНЕ

ПРЕДАВАЊА

ЗОРАН ПЕТРОВИЋ

ШКОЛСКА 2024/25 ГОДИНА

1 Конструкције лењиром и шестаром

1.1 Формулација проблема и класична питања

У школи смо имали прилике да изучавамо конструкције које се могу извршити лењиром и шестаром. Наравно, ту се подразумева да лењир није 'баждарен', тј. да не можемо одмеравати дужине помоћу лењира (без обзира на чињеницу да лењири који се продају као школски прибор јесу баждарени). Лењири само служе за повлачење правих кроз две дате тачке. У вези са тим су добро позната три конструктивна проблема Антике (за који су вероватно неки од читалаца и чули).

1. Удвостручавање коцке. За дату коцку, наћи коцку двоструко веће запремине. С обзиром да је запремина коцке странице a једнака a^3 за налажење странице b за коју је $b^3 = 2a^3$ потребно је и довољно конструисати број $\sqrt[3]{2}$.

2. Трисекција угла. Дати угао поделити на три једнака дела. Добро нам је познато како да преполовимо угао, а и како да дату дуж поделимо на три једнака дела, али како поделити угао на три једнака дела? Показаћемо да се и то своди на питање конструкције броја који је решење неке једначине трећег степена (као што је и $\sqrt[3]{2}$ решење једначине $x^3 = 2$).

3. Квадратура круга. За дати круг наћи квадрат чија је површина једнака површини датог круга. С обзиром да је површина круга полупречника r дата формулом πr^2, а да је површина квадрата странице a једнака a^2 решавање проблема се своди на конструкцију броја $\sqrt{\pi}$.

У овом одељку, укратко ћемо описати главне алгебарске идеје које се налазе у оквиру проблема конструкције лењиром и шестаром и

показати да се прва два наведена проблема не могу решити на тај начин.

Све конструкције наравно вршимо у равни. У њој ћемо изабрати једну тачку O и две нормалне праве које кроз њу пролазе. Замислићемо, ради лакшег описа да је једна 'хоризонтална', а друга 'вертикална' (оне представљају координатне осе). На хоризонталној оси, изабраћемо 'са десне стране' од тачке O једну тачку P и сматраћемо да дуж OP представља јединичну дуж. Дакле, тачка P ће имати координате $(1, 0)$.

Основна конструкција лењиром је повлачење праве кроз две већ конструисане тачке, док је основна конструкција шестаром цртање круга са центром у једној конструисаној тачки која пролази кроз другу конструисану тачку. У пресеку тако конструисаних правих и кругова, добијамо нове тачке. Тачка у равни је конструктибилна уколико се може добити понављањем основних конструкција коначно много пута.

Приметимо да можемо посебно разматрати и конструкције тачака на координатним осама. Тако добијамо и појам конструктибилних реалних бројева. Није тешко уверити се да важи следећи став.

Став 1 Тачка у равни са координатама (a, b) је конструктибилна ако и само ако су a и b конструктибилни реални бројеви.

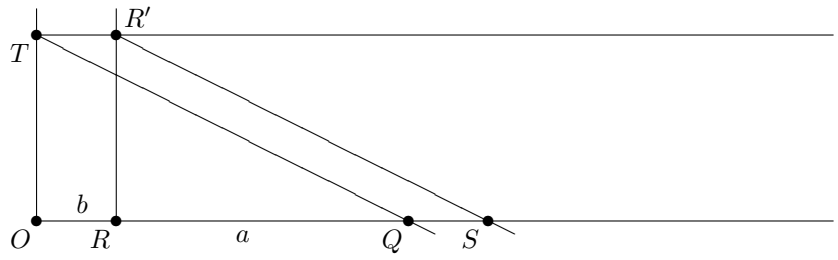
Тачке у равни можемо да видимо и као комплексне бројеве на стандардан начин.

Следећи став је занимљив.

Став 2 Конструктибилни бројеви чине поље.

Доказ. Дајемо доказ за реалне бројеве. С обзиром на то како се изводе операције са комплексним бројевима, лако се потом добија резултат и за комплексне бројеве. Ми ћемо доказати да реални конструктибилни бројеви чине потпоље од $\mathbb{R}$. У ту сврху треба показати да, ако су a и b конструктибилни реални бројеви, онда су то и бројеви $a \pm b$, $a \cdot b$, као и да је $\frac{1}{a}$ конструктибилан број за сваки конструктибилан број $a \neq 0$.

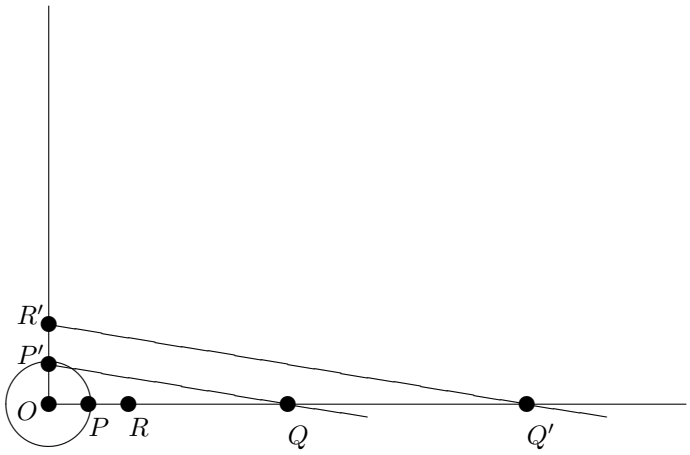
Није тешко уверити се да је довољно ово показати када имамо позитивне реалне бројеве (негативни бројеви само уводе више случајева). Конструкција броја $a + b$ дата је следећим цртежом.



Наиме, ако је број a одређен тачком Q, а број b тачком R, онда најпре кроз неку тачку T (такву да је дужина дужи OT неки конструктибилан број) на вертикалној оси конструишемо праву паралелну хоризонталној оси (то знамо да конструишемо помоћу лењира и шестара). Потом кроз тачку R конструишемо праву паралелну вертикалној оси и у пресеку добијамо тачку R'. Повлачимо и праву кроз тачке T и Q. На крају повлачимо праву кроз R' паралелну правој кроз тачке T и Q. У пресеку са хоризонталном осом добијамо тачку S која и одговара броју $a + b$.

Читаоцима остављамо да провере како се може конструисати број $a - b$.

За конструкцију броја $a \cdot b$ користимо следећу пропорцију: $ab : b = a : 1$. Ево цртежа (тачка P означава позицију броја 1).



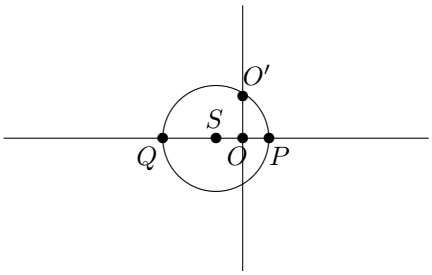
Постављамо кругове са центром у O који пролазе кроз тачке P (која одговара броју 1) и тачку R (која одговара броју b). У пресеку добијамо тачке P' и R' на вертикалној оси. Права кроз R' паралелна правој кроз тачке P' и Q сече хоризонталну осу у тачки Q' и та тачка одговара тачки $a \cdot b$. Наиме, правоугли троуглови $\triangle QOP'$ и $\triangle Q'OR'$ су слични, па је $OQ : OP' = OQ' : OR'$, односно $a : 1 = OQ' : b$. Стога тачка Q' заиста одговара тачки $a \cdot b$.

Остављамо читаоцима за вежбу да покажу како се може конструисати $\frac{1}{a}$ ако је a већ конструисан. □

Није тачно само то да конструктибилни бројеви чине потпоље од $\mathbb{R}$.

Став 3 Ако је позитиван реалан број a конструктибилан, конструктибилан је и $\sqrt{a}$.

Доказ. Препоручујемо читаоцима да се увере да цртеж



даје решење. Овде тачка P одговара, као и раније броју 1, тачка Q броју $-a$, а S је центар конструисаног круга. Дужина OO' одговара броју $\sqrt{a}$. □

Став 4 Нека су дате тачке A, B, C, D чије су координате у неком потпољу F поља $\mathbb{R}$. Тада су координате тачака које се добијају у пресеку две праве, два круга, или праве и круга, који пролазе кроз две од ових тачака или у поље F или у пољу $F(\sqrt{r})$, где је $r \in F$.

Доказ. Дакле, дате су тачке $A(x_1, y_1)$, $B(x_2, y_2)$, $C(x_3, y_3)$ и $D(x_4, y_4)$. Једначина праве кроз тачке A и B дата је са:

$$\frac{x - x_1}{y - y_1} = \frac{x_2 - x_1}{y_2 - y_1},$$

док је једначина круга који има центар у C и пролази кроз D дата са:

$$(x - x_3)^2 + (y - y_3)^3 = (x_4 - x_3)^2 + (y_4 - y_3)^2.$$

Стога се налажење пресека те праве и тог круга своди на решавање система од једне линеарне и једне квадратне једначине. Посматрањем прво линеарне једначине, можемо једну координату изразити преко друге (или се чак добија да је једна координата фиксирана, што опет значи да је изражена преко друге, само преко константне функције) и тако заменом у једначину круга добијамо квадратну једначину, а знамо да њено решавање укључује налажење квадратног корена из неког елемента који је изражен у облику количника полинома по коефицијентима, па стога припада пољу F. Дакле, нове координате су или из F или су у пољу $F(\sqrt{r})$, где је r тај број чији се корен тражи у поступку решавања једначине, а сигурно припада пољу F.

У случају да посматрамо пресек две праве, ситуација је још једноставнија, јер решења морају припадати пољу F, док се случај пресека два круга своди, одузимањем, на случај тражења решења система једне линеарне и једне квадратне једначине (квадратни чланови ће се одузимањем скратити). □

Подсетимо се неких резултата о проширењима поља. Најпре, ако су E и F поља, при чему је $F \subseteq E$, онда кажемо да је поље E једно ПРОШИРЕЊЕ поља F и означавамо са: проширење E/F. Елементе поља E наравно да можемо да сабирамо, али можемо и да их множимо елементима поља F и резултат је у пољу E. Узимајући у обзир сва својства особина сабирања и множења у пољима можемо да закључимо да је поље E један векторски простор над поље F. Уколико је то простор коначне димензије, кажемо да је проширење E/F коначно и димензију поља E над пољем F, тј. $\dim_F E$ означавамо са $[E : F]$ и називамо СТЕПЕН ПРОШИРЕЊА поља E над F.

Уколико је E_1 коначно проширење поља F, а E_2 коначно проширење поља E_1, онда је наравно E_2 и једно проширење поља F.

Став 5 Ако су F, E_1 и E_2 поља као у претходној реченици, онда је E_2 коначно проширење поља F и важи

$$[E_2 : F] = [E_2 : E_1][E_1 : F].$$

Доказ. Нека је $[E_1 : F] = n$ и $[E_2 : E_1] = m$. Како је димензија E_1 као векторског простора над пољем F једнака n, то постоји нека база $[\alpha_1, \ldots, \alpha_n]$. Слично, нека је $[\beta_1, \ldots, \beta_m]$ база векторског простора E_2 над пољем E_1. Докажимо да производи $\alpha_i\beta_j$, $i = \overline{1,n}$, $j = \overline{1,m}$ чине базу простора E_2 над пољем F.
Линеарна независност. Претпоставимо да је

$$\sum_{j=1}^{m}\sum_{i=1}^{n} c_{ij}\alpha_i\beta_j = 0,$$

за неке $c_{ij} \in F$. Нека је $d_j = \sum_{i=1}^{n} c_{ij}\alpha_i$, $j = \overline{1,m}$. Елементи d_j су из поља E_1 и за њих важи:

$$\sum_{j=1}^{m} d_j\beta_j = 0.$$

Како је $[\beta_1, \ldots, \beta_m]$ база за E_2 над E_1, то мора бити $d_j = 0$ за све $j \in \{1, \ldots, m\}$. Но, како је $[\alpha_1, \ldots, \alpha_n]$ база за E_1 над пољем F, то из $\sum_{i=1}^{n} c_{ij}\alpha_i = 0$, за $j = \overline{1,m}$ следи да је $c_{ij} = 0$ за $i = \overline{1,n}$, $j = \overline{1,m}$.

Генератриса. Нека је $\gamma \in E_2$. Како је $[\beta_1, \ldots, \beta_m]$ база за E_2 над E_1, то постоје $r_j \in E_1$ такви да је

$$\gamma = \sum_{j=1}^{m} r_j\beta_j.$$

Но, како је $[\alpha_1, \ldots, \alpha_n]$ база за E_1 над F то за свако $j \in \{1, \ldots, m\}$ постоје s_{ij} за које је

$$r_j = \sum_{i=1}^{n} s_{ij}\alpha_i.$$

Коначно добијамо да је

$$\gamma = \sum_{j=1}^{m} \sum_{i=1}^{n} s_{ij} \alpha_i \beta_j.$$

□

Наведимо сада најважнију теорему у овом одељку.

Теорема 6 Нека је α конструктибилан реалан број, који није из $\mathbb{Q}$. Тада постоји низ потпоља од $\mathbb{R}$

$$\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n = F,$$

тако да $\alpha \in F$, $F_i = F_{i-1}(\sqrt{r_i})$, где је $r_i > 0$, $r_i \in F_{i-1}$, $\sqrt{r_i} \neq F_{i-1}$. Дакле,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^s$$

за неко $s \geq 1$.

Доказ. Као што знамо, нека тачка је конструктибилна ако се може добити од конструктибилних тачака у коначно много корака од којих се сваки састоји од налажења пресека две праве, или праве и круга. А реалан број је конструктибилан уколико је координата неке конструктибилне тачке. Дакле, α је координата неке тачке A, која је добијена као последња тачка у низу. Као што знамо, сви рационални бројеви се могу конструисати почев од 0 и 1. Затим, евентуално, додајемо корен неког позитивног рационалног броја r_1 и добијамо поље $\mathbb{Q}(\sqrt{r_1})$, при чему $\sqrt{r_1} \notin \mathbb{Q}$ На основу става, у следећем кораку, највише што је потребно додати је опет корен неког броја из $Q(\sqrt{r_1})$, који се ту не налази. Дакле, заиста добијамо низ поља као што је наведено и $\alpha \in F$, где је F то последње поље. Но, с обзиром да је $F_i = F_{i-1}(\sqrt{r_i})$, при чему је $r_i \in F_{i-1}$ и $\sqrt{r_i} \neq F_{i-1}$, јасно је да је

$$[F_i : F_{i-1}] = 2,$$

јер је полином $X^2 - r_i$ минималан полином елемента $\sqrt{r_i}$ над пољем F_{i-1}. Стога је

$$[F : \mathbb{Q}] = [F_n : F_{n-1}] \cdot [F_{n-1} : F_{n-2}] \cdots [F_1 : F_0] = 2^n.$$

Но, како $\alpha \in F$, добијамо да је

$$2^n = [F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}],$$

те је заиста $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^s$ за неко $s \geq 1$. □

Напомена 7 Одговарајући резултат важи и за конструктибилне комплексне бројеве: ако је $\alpha \in \mathbb{C} \setminus \mathbb{Q}$ конструктибилан, онда је $[\mathbb{Q}(\alpha) : Q] = 2^s$ за неко $s \geqslant 1$. ♠

Сада можемо да решимо она два проблема. Позабавимо се најпре удвостручавањем коцке.

Став 8 Удвостручавање коцке није могуће извршити коришћењем искључиво лењира и шестара.

Доказ. Видели смо да се то своди на конструктибилност броја $\sqrt[3]{2}$. Но, полином $X^3 - 2$ је нерастављив над $\mathbb{Q}$. То нам је лако показати коришћењем знања из претходних курсева. На пример, можемо користити Ајзенштајнов критеријум, или констатовати да полином нема рационалну нулу. Уверите се у ово.

Дакле, полином $a(X) = X^3 - 2$ је нерастављив над $\mathbb{Q}$ и како је $a(\sqrt[3]{2}) = 0$, то је $a(X)$ минимални полином елемента $\sqrt[3]{2}$, те је $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg a(X) = 3$, што противречи претходној теореми, јер 3 није степен двојке. □

Да бисмо доказали да није могуће извршити трисекцију произвољног угла коришћењем лењира и шестара, довољно је показати да се не може конструисати угао од $20°$. Наиме, добро нам је познато да се угао од $60°$ може конструисати лењиром и шестаром, а ако је доказано да се угао од $20°$ не може конструисати лењиром ни шестаром, то се ни угао од $60°$ не може поделити на три једнака дела.

Разматрањем јединичног круга, видимо да се немогућност конструкције угла од $20°$ своди на немогућност конструкције броја $\cos 20°$. Докажимо то.

Став 9 Број $\cos 20°$ није конструктибилан.

Доказ. Користићемо следећи идентитет

$$\cos 3\varphi = 4\cos^3 \varphi - 3\cos \varphi.$$

Читаоци би требало да провере како се добија овај идентитет. У сваком случају, ако узмемо да је $\varphi = 20°$ добијамо

$$4\cos^3 20° - 3\cos 20° = \cos 60° = \frac{1}{2}.$$

Дакле,

$$\cos^3 20° - \frac{3}{4}\cos 20° - \frac{1}{8} = 0.$$

Посматрајмо полином $a(X) = X^3 - \frac{3}{4}X - \frac{1}{8} \in \mathbb{Q}[X]$. Докажимо да је он нерастављив над $\mathbb{Q}$. С обзиром да је у питању полином трећег степена, доказ се своди на проверу да ли полином има нулу у $\mathbb{Q}$. То би била и нула полинома $8a(X) = 8X^3 - 6X - 1$. Но, ако је $\frac{p}{q} \in \mathbb{Q}$ једна нула тог полинома, при чему је $q > 0$ и овај разломак нескратив, онда $p \mid -1$, а

$q \mid 8$ по добро нам познатом критеријуму од раније. Лако је проверити да такви p и q не постоје.

Добили смо да полином $a(X)$ није растављив над $\mathbb{Q}$, Како је испуњено: $a(\cos 20^\circ) = 0$, закључујемо да је $a(X)$ минимални полином за $\cos 20^\circ$ над $\mathbb{Q}$, те је $[Q(\cos 20^\circ) : \mathbb{Q}] = 3$, што показује да број $\cos 20^\circ$ није конструктибилан. □

Овај резултат нам показује да лењиром и шестаром није могуће конструисати правилни 18-оугао. Наиме, јасно је да се конструкција правилног n-тоугла може свести на конструкцију централног угла над његовом страницом, а то је угао од $\frac{360^\circ}{n}$, односно у нашем случају, то је угао од 20°.

1.2 Напреднија питања

Следећи резултат је нешто тежи за доказ.

Став 10 Помоћу лењира и шестара није могуће конструисати правилни седмоугао.

Доказ. Као што је већ речено, доказ се своди на немогућност конструкције броја $\cos \frac{2\pi}{7}$ (сада ћемо, због краћег записа, користити радијане). Нека је $\zeta = \cos \frac{2\pi}{7} + i \sin \frac{2\pi}{7}$. Приметимо да је ζ заправо седми корен из јединице: $\zeta^7 = 1$. Како је $\zeta \neq 1$, добијамо да је

$$\zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0.$$

Поделимо ову једнакост са ζ^3. Добијамо

$$\zeta^3 + \zeta^2 + \zeta + 1 + \frac{1}{\zeta} + \frac{1}{\zeta^2} + \frac{1}{\zeta^3} = 0. \tag{1}$$

Приметимо да је

$$z = \zeta + \frac{1}{\zeta} \left(= 2 \cos \frac{2\pi}{7} \right).$$

Довољно је, дакле, да докажемо да z није конструктибилан. Но,

$$z^3 = \zeta^3 + \frac{1}{\zeta^3} + 3 \left(\zeta + \frac{1}{\zeta} \right),$$

те је

$$\zeta^3 + \frac{1}{\zeta^3} = z^3 - 3z.$$

На сличан начин

$$z^2 = \zeta^2 + 2 + \frac{1}{\zeta^2},$$

те је

$$\zeta^2 + \frac{1}{\zeta^2} = z^2 - 2.$$

Стога из једначине (**1**) добијамо

$$z^3 - 3z + z^2 - 2 + z + 1 = 0,$$

тј.

$$z^3 + z^2 - 2z - 1 = 0.$$

Покажимо да је полином $a(X) = X^3+X^2-2X-1 \in \mathbb{Q}[X]$ нерастављив над $\mathbb{Q}$. Као и пре, довољно је показати да он нема нула у $\mathbb{Q}$. Уколико је $\frac{p}{q} \in \mathbb{Q}$ нека нула овог полинома, при чему је $q > 0$ и ово нескратив разломак, онда она мора бити испуњено: $p \mid -1$, $q \mid 1$, тј. $\frac{p}{q} \in \{-1, 1\}$. Но, лако се провери да ово нису нуле полинома $a(X)$, па он није растављив над $\mathbb{Q}$. Стога је он минимални полином за елемент z. Како је тај полином степена 3, тај елемент није конструктибилан, што је требало и доказати. □

Докажимо сада јачи резултат од овог.

Став 11 Ако је p непаран прост број и ако је могуће конструисати правилан p-угао, онда је p Фермаов прост број, тј. прост број облика $p = 2^{2^n} + 1$ за неко $n \geq 0$.

Доказ. Посматрамо полином

$$a(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

По претпоставци је број $\zeta = e^{\frac{2\pi i}{p}}$ конструктибилан ($1, \zeta, \ldots, \zeta^{p-1}$ чине темена правилног p-тоугла). Важи да је $\zeta^p = 1$ и, како је $\zeta \neq 1$, то је $a(\zeta) = 0$. Полином $a(X) \in \mathbb{Q}[X]$ је нерастављив **акко** је нерастављив полином $a(X + 1)$. Како је

$$(X - 1)a(X) = X^p - 1,$$

то је

$$Xa(X + 1) = (X + 1)^p - 1 = \sum_{k=0}^{p} \binom{p}{p-k} X^{p-k} - 1 = \sum_{k=0}^{p-1} \binom{p}{p-k} X^{p-k}.$$

Стога је

$$a(X + 1) = X^{p-1} + pX^{p-2} + \binom{p}{2} X^{p-3} + \cdots + p.$$

Како за све $1 \leq k \leq p - 1$ важи да $p \mid \binom{p}{k}$, $p^2 \nmid p$ и $p \nmid 1$, то је полином $a(X + 1)$ нерастављив по Ајзенштајновом критеријуму. Стога је $a(X)$ минимални полином елемента ζ и $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg a(X) = p - 1$. Како је ζ конструктибилан број, добијамо да је $p - 1 = 2^m$ за неки природан број m. Нека је $m = 2^n(2l + 1)$ за неке $n \geq 0$ и $l \geq 0$. Ако $l \neq 0$, онда је

$$p = 2^m + 1 = 2^{2^n(2l+1)} + 1 = (2^{2^n} + 1)(2^{2^n 2l} - 2^{2^n(2l-1)} + \cdots + 1),$$

те p не би био прост број. Стога мора бити $p = 2^{2^n} + 1$ за неко $n \geq 0$, тј. p је Фермаов прост број. □

Напомена 12 Ако је $F_n := 2^{2^n}+1$, онда знамо да су ово прости бројеви за $n = \overline{0,4}$. Нису познати други Фермаови прости бројеви. Посебно, за $n = 2$ имамо да је $F_2 = 17$. Гаус је доказао, када је имао 19 година, да је могуће конструисати правилни 17-оугао (још је од Еуклида познато да је могуће конструисати правилни троугао и правилни петоугао) и то му је, по његовим речима, указало на то да је математика обећавајућа професија за њега... ♠

Дакле, знамо да, ако је број α конструктибилан мора бити $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^s$ за неко $s \geq 0$. Покажимо примером да обрат не важи.

Пример 13 Не могу сви корени полинома $X^4 + 4X + 2 \in \mathbb{Q}[X]$ да буду конструктибилни.

Приметимо најпре да је дати полином нерастављив по Ајзенштајну $(2 \mid 2,\ 2 \mid 4,\ 2 \nmid 1,\ 2^2 \nmid 2)$ те је степен сваког корена над $\mathbb{Q}$ једнак 4 што је степен двојке.

Решимо једначину $x^4+4x+2 = 0$. Ако је $p(x) = x^4+4x+2$, можемо да приметимо да, пошто је $p(x) > 0$ за $x \geq 0$, $p'(x) < 0$ за $x < -1$, $p'(x) > 0$ за $x > -1$, $p(-1) = -1 < 0$ и $p(x) > 0$ за $x << 0$, овај полином има тачно две реалне нуле и то су негативни бројеви.

Користићемо Ојлеров метод, где решење тражимо у облику $x = u + v + w$. Тада је

$$x^2 = u^2 + v^2 + w^2 + 2(uv + uw + vw),$$

те је

$$(x^2 - (u^2 + v^2 + w^2))^2 = 4(uv + uw + vw)^2.$$

Дакле

$$x^4-2(u^2+v^2+w^2)x^2+(u^2+v^2+w^2)^2 = 4(u^2v^2+u^2w^2+v^2w^2+2(u^2vw+uv^2+uvw^2)).$$

Приметимо да је

$$u^2vw + uv^2 + uvw^2 = uvw(u + v + w) = uvwx.$$

Ако ово искористимо и средимо претходну једнакост, добијамо:

$$x^4 - 2(u^2 + v^2 + w^2)x^2 - 8uvwx + (u^2 + v^2 + w^2)^2 - 4(u^2v^2 + u^2w^2 + v^2w^2) = 0.$$

Како је $x^4 + 4x + 2 = 0$, добијамо да је

$$\begin{aligned} u^2 + v^2 + w^2 &= 0 && (2)\\ -8uvw &= 4 && (3)\\ (u^2 + v^2 + w^2)^2 - 4(u^2v^2 + u^2w^2 + v^2w^2) &= 2. && (4) \end{aligned}$$

Из прве и треће једначине добијамо да је

$$u^2v^2 + u^2w^2 + v^2w^2 = -\frac{1}{2},$$

а из друге да је

$$uvw = -\frac{1}{2},$$

те је

$$u^2v^2w^2 = \frac{1}{4}.$$

Добили смо нови систем једначина:

$$u^2 + v^2 + w^2 = 0 \tag{5}$$

$$u^2v^2 + u^2w^2 + v^2w^2 = -\frac{1}{2} \tag{6}$$

$$u^2v^2w^2 = \frac{1}{4}. \tag{7}$$

Видимо да су u^2, v^2, w^2 нуле полинома

$$q(X) = (X - u^2)(X - v^2)(X - w^2) = X^3 - \frac{1}{2}X - \frac{1}{4} \in \mathbb{Q}[X].$$

Приметимо да је

$$8q(X) = 8X^3 - 4X - 2 = (2X)^3 - 2 \cdot (2X) = 2.$$

Заменом $Y = 2X$ добијамо полином $r(Y) = Y^3 - 2Y - 2 \in \mathbb{Q}[Y]$ и он је нерастављив по Ајзенштајну (за прост $p = 2$ наравно). Стога је и $q(X)$ нерастављив над $\mathbb{Q}$ те његове нуле u^2, v^2, w^2 нису конструктибилни бројеви. Но, та се једначина може решити и тако добити бројеви u^2, v^2, w^2. Ми можемо да изаберемо неке корене из ових бројева и прогласимо их за u, v, w. Но, ако је $x_1 = u + v + w$ једно од решења почетне једначине, онда су остала решења:

$$x_2 = u - v - w \tag{8}$$

$$x_3 = -u + v - w \tag{9}$$

$$x_4 = -u - v + w. \tag{10}$$

Важно је приметити да је $uvw = -\frac{1}{2}$ за сваки избор u, v, w, те немамо 16 могућности како се, можда, на први поглед чини. Кад изаберемо неке u, v, w, остају само још три могућности које су наведене. Но, ако би сви x_1, x_2, x_3, x_4 били конструктибилни, онда би био конструктибилан и број $2u = x_1 + x_2$, па онда и u, те нужно и u^2, а знамо да он није конструктибилан. Дакле, не могу сви корени бити конструктибилни и то показује да обрат у наведеном ставу не важи. ♣

2 Нормална раширења поља

2.1 Неки основни појмови и резултати

Подсетимо се најпре следеће чињенице.

Став 14 Ако је $\varphi\colon K \to L$ хомоморфизам поља, онда је φ нужно мономорфизам.

Доказ. Знамо да је $\operatorname{Ker}\varphi$ идеал у K. Такође знамо да је $\varphi(1_K) = 1_L$, те $1_K \notin \operatorname{Ker}\varphi$. Како су у пољу K једини идеали $\{0\}$ и K, то је $\operatorname{Ker}\varphi = \{0\}$, те је φ мономорфизам. □

На пример, не постоји никакав хомоморфизам $\varphi\colon \mathbb{C} \to \mathbb{R}$, јер би то значило да $\mathbb{R}$ садржи у себи потпоље изоморфно са $\mathbb{C}$.

Дефиниција 15 Просто поље је поље које нема правих потпоља.

Став 16 1. Поље је карактеристике нула ако и само ако садржи као своје потпоље поље изоморфно са $\mathbb{Q}$.
2. Поље је карактеристике p ако и само ако садржи као своје потпоље поље изоморфно са $\mathbb{Z}_p$.

Доказ. Приметимо најпре да је карактеристика поља K једнака карактеристици ма ког његовог потпоља, пошто сва потпоља имају заједничку јединицу 1_K и садрже све елементе облика $n1_K$ за $n \geq 1$. Тако да је потребно доказати само један смер у доказу еквиваленције.

1. Нека је K поље карактеристике 0. Тада је $n1_K \neq 0_K$ за све $n \in \mathbb{Z} \setminus \{0\}$. Дефинишимо $\varphi\colon \mathbb{Q} \to K$ са:

$$\varphi\left(\frac{m}{n}\right) := (m1_K)(n1_K)^{-1}.$$

Покажимо да је φ добро дефинисано:

$$\begin{aligned}
\frac{m}{n} = \frac{r}{s} &\implies sm = nr \\
&\implies (sm)1_K = (nr)1_K \\
&\implies (s1_K)(m1_K) = (n1_K)(r1_K) \\
&\implies (m1_k)(n1_K)^{-1} = (r1_K)(s1_K)^{-1}.
\end{aligned}$$

Наравно, φ је хомоморфизам:

$$\begin{aligned}
\varphi\left(\frac{m}{n} + \frac{r}{s}\right) &= \varphi\left(\frac{sm+nr}{ns}\right) \\
&= (sm+nr)1_K((ns)1_K)^{-1} \\
&= ((s1_K)(m1_K) + (n1_K)(r1_K))(n1_K)^{-1}(s1_K)^{-1} \\
&= (s1_K)(m1_K)(n1_K)^{-1}(s1_K)^{-1} + (n1_K)(r1_K)(n1_K)^{-1}(s1_K)^{-1} \\
&= (m1_K)(n1_K)^{-1} + (s1_K)^{-1} \\
&= \varphi\left(\frac{m}{n}\right) + \varphi\left(\frac{r}{s}\right).
\end{aligned}$$

Провера за производ је још једноставнија. Наравно, $\varphi(1) = 1_K$. Како је φ нужно мономорфизам по претходном ставу, то је $\operatorname{Im}\varphi$ потпоље од K изоморфно са $\mathbb{Q}$.

2. Нека је K поље карактеристике p. Тада је $p1_K = 0_K$. Дефинишемо $\varphi\colon \mathbb{Z}_p \to K$ са: $\varphi(r) := r1_K$, за $r \in Z_p(= \{0, 1, \ldots, p-1\})$. Овде наравно не морамо да проверавамо добру дефинисаност. Проверимо само да је φ хомоморфизам. Нека су $r, s \in Z_p$. Подсетимо се да су операције у $\mathbb{Z}_p$ сабирање и множење по модулу p: $r \cdot_p s = \rho(r \cdot s, p)$, где је са $\rho(m, p)$ означен остатак при дељењу m са p. Дакле, $rs = qp + r \cdot_p s$, за неки $q \in \mathbb{N}$. Стога је

$$\varphi(r)\cdot\varphi(s) = (r1_K)\cdot(s1_K) = (rs)1_K = q(\underbrace{p1_K}_{=0_K}) + (r\cdot_p s)1_K = (r\cdot_p s)1_K = \varphi(r\cdot_p s).$$

Слагање у односу на сабирање се још лакше проверава. Дакле, како је φ хомоморфизам поља, φ је нужно мономорфизам, па K садржи потпоље изоморфно са $\mathbb{Z}_p$. □

Напомена 17 У даљем ћемо поље $\mathbb{Z}_p$ означавати најчешће са $\mathbb{F}_p$. Због претходног резултата, поља $\mathbb{Q}$ и $\mathbb{F}_p$ називају се и ОСНОВНИМ ПОЉИМА и често ћемо сматрати да је баш $\mathbb{Q} \subseteq K$ уколико је K карактеристике 0, односно да је $\mathbb{F}_p \subseteq K$ ако је K карактеристике p. То користимо већ у следећем ставу. ♠

Став 18 Нека је K поље карактеристике 0 и $\varphi \in \operatorname{Aut}(K)$. Тада је $\varphi(q) = q$ за све $q \in \mathbb{Q}$.

Доказ. Како је $\mathbb{Q} \subseteq K$, то је $1_K = 1(= 1_{\mathbb{Q}})$. С обзиром на то да је $\varphi(1) = 1$, индукцијом се лако покаже да је $\varphi(n) = n$ за све $n \in \mathbb{N}$, а из чињенице да је $\varphi(-\alpha) = -\varphi(\alpha)$ за све α, добијамо да је и $\varphi(m) = m$ за све $m \in \mathbb{Z}$. Стога је $\varphi(m/n) = \varphi(m)/\varphi(n) = m/n$ за све $m \in \mathbb{Z}$, $n \in \mathbb{N}\setminus\{0\}$, те је заиста $\varphi(q) = q$ за све $q \in \mathbb{Q}$. □

2.2 Појам нормалног раширења

Започнимо једним примером.

Пример 19 Нека је $K = \mathbb{Q}(\sqrt[3]{2})$. Одредити групу $\operatorname{Aut}(K)$.

Нека је $\varphi \in \operatorname{Aut}(K)$. Знамо да по ставу **18** важи: $\varphi(q) = q$ за све $q \in \mathbb{Q}$. Сваки елемент из $\alpha \in K$ је облика $\alpha = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$ за неке $a, b, c \in \mathbb{Q}$. Дакле,

$$\begin{aligned}\varphi(\alpha) &= \varphi\left(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2\right)\\ &= \varphi(a) + \varphi(b)\varphi(\sqrt[3]{2}) + \varphi(c)\varphi(\sqrt[3]{2})^2\\ &= a + b\varphi(\sqrt[3]{2}) + c\varphi(\sqrt[3]{2})^2.\end{aligned}$$

Према томе, вредност $\varphi(\alpha)$ је потпуно одређена вредношћу $\varphi(\sqrt[3]{2})$. Но, $(\sqrt[3]{2})^3 = 2$, па је $\varphi(\sqrt[3]{2})^3 = 2$. С обзиром на то да $\varphi(\sqrt[3]{2}) \in \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ и да из средње школе знамо да је једино решење у $\mathbb{R}$ једначине $x^3 = 2$ баш $\sqrt[3]{2}$ то је $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$ и $\varphi = \mathrm{id}_K$. Стога је група $\mathrm{Aut}(K)$ тривијална: $\mathrm{Aut}(K) = \{id_K\}$. ♣

Стога, да бисмо добили занимљивију групу, морамо у K додати још трећих корена из 2. Знамо да су сви трећи корени из 2: $\sqrt[3]{2}, \varepsilon\sqrt[3]{2}, \varepsilon^2\sqrt[3]{2}$, где је $\varepsilon = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$ нетривијални трећи корен из јединице. Одређивање групе $\mathrm{Aut}(L)$ за $L = \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ је свакако занимљивије од претходног примера.

Мотивисани овим примером, дајемо следећу дефиницију.

Дефиниција 20 Алгебарско раширење F поља K је НОРМАЛНО уколико важи следеће. Ако је полином $p \in K[X]$ нерастављив у $K[X]$ и ако F садржи неку нулу тог полинома, онда су у F све нуле тог полинома.

На пример, раширење K поља $\mathbb{Q}$ из претходног примера није нормално, јер полином $X^3 - 2 \in \mathbb{Q}[X]$ јесте нерастављив у $\mathbb{Q}[X]$, а K не садржи све нуле овог полинома. Док раширење L садржи све његове нуле. Наравно, ми не знамо баш само на основу тога да је то раширење нормално, јер можда постоји неки други полином који нам то „поквари". Но, следећи став нам у томе помаже.

Пре формулације тог става, подсетимо се неких чињеница. Ако је $p \in K[X]$ онда је коренско поље овог полинома минимално раширење поља K у коме се полином p растављa („цепа") на линеарне факторе, дакле минимално раширење које садржи све корене овог полинома. Важи следеће. Ако је поље K изоморфно пољу $\overline{K}$, $\varphi\colon K \to \overline{K}$ изоморфизам, $p = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ и полином $\overline{p} \in \overline{K}[X]$ дефинисан са: $\overline{p} = \varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n$, онда ако је F коренско поље полинома p, а $\overline{F}$ коренско поље полинома $\overline{p}$, важи: $F \cong \overline{F}$. Посебно, свака два коренска поља једног полинома су изоморфна.

Став 21 Коначно раширење F поља K је нормално ако и само ако је оно коренско поље неког полинома p из $K[X]$.

Доказ става 21. $\Longleftarrow$. Нека је F коренско поље полинома $p \in K[X]$, $q \in K[X]$ нерастављив полином и $\alpha \in F$ такво да је $q(\alpha) = 0$. Треба доказати да све нуле полинома q леже у F. Нека је E коренско поље полинома $p \cdot q \in K[X]$ и $\beta \in E$ такво да је $q(\beta) = 0$. Треба показати да $\beta \in F$. Из курса Алгебре 2 знамо да је

$$K(\alpha) \cong K[X]/_{\langle q \rangle} \cong K(\beta),$$

пошто је q нерастављив. Поље F је коренско поље за полином p, било да га гледамо као полином из $K[X]$, било као полином из $K(\alpha)[X]$

(свакако $\alpha \in F$). Осим тога је $F(\beta)$ коренско поље за полином $p \in K(\beta)[X]$. Но, како је $K(\beta) \cong K(\alpha)$, према претходном следи да су и та коренска поља $F(\beta)$ и F полинома p изоморфна. То посебно значи да су она изоморфна и као векторски простори над пољем K. Стога су $F(\beta)$ и F коначно димензионални векторски простори над K исте димензије, при чему је $F \subseteq F(\beta)$. Закључујемо да се они морају поклапати, из чега следи да $\beta \in F$.

$\Longrightarrow$. Нека је F коначно и нормално раширење над K. Дакле, $F = K(\alpha_1, \ldots, \alpha_n)$ за неке $\alpha_i \in F$, који су наравно алгебарски над K јер је F коначно раширење. Нека су $\mu_{\alpha_1}, \ldots, \mu_{\alpha_n} \in K[X]$ минимални полиноми ових елемената. Пошто је F нормално раширење поља K, μ_{α_i}, нерастављив полином из $K[X]$ за који је $\mu_{\alpha_i}(\alpha_i) = 0$, у F се налазе и све остале нуле полинома μ_{α_i}. Ово је наравно тачно за све i, те је F заправо коренско поље полинома $p = \mu_{\alpha_1} \cdots \mu_{\alpha_n}$. □

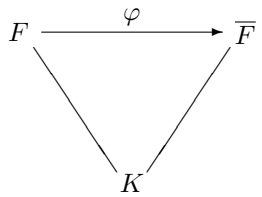
Дефиниција 22 Ако је L раширење поља K, онда је НОРМАЛНО ЗАТВОРЕЊЕ поља L најмање раширење $\overline{L}$ поља L тако да је раширење $\overline{L}/K$ нормално.

На пример, ако је $L = K(\alpha_1, \ldots, \alpha_n)$, где су α_i алгебарски над K, онда је $\overline{L}$ заправо коренско поље полинома $\mu_{\alpha_1} \cdots \mu_{\alpha_n}$, где је $\mu_{\alpha_i} \in K[X]$ минимални полином елемента α_i. Уколико је $L = K(\sqrt[3]{2})$, $\overline{L} = K(\sqrt[3]{2}, \varepsilon)$.

3 Сепарабилна раширења поља

Видели смо да су нормална раширења неког поља она раширења у којима се налазе све нуле нерастављивих полинома са коефицијентима у почетном пољу, чим је ту једна нула. Сада ће нас занимати да ли су те нуле „раздвојене" („сепариране").

Нека су F и $\overline{F}$ коренска поља полинома $p \in K[X]$ и $\varphi\colon F \to \overline{F}$ изоморфизам „над" K, тј. такав изоморфизам да је $\varphi(c) = c$ за све $c \in K$. Како су F и $\overline{F}$ не само векторски простори над K, него и алгебре над K, овде имамо заправо изоморфизам алгебри над K (K-алгебри).



Изоморфизам $\varphi\colon F \to \overline{F}$ можемо продужити до изоморфизма $\widetilde{\varphi}\colon F[X] \to \overline{F}[X]$ тако што ћемо „додефинисати" да је $\widetilde{\varphi}(X) = X$. Ако је $\overline{\alpha} = \varphi(\alpha)$,

за $\alpha \in F$, онда је

$$p(\alpha) = 0 \text{ акко је } \varphi(p(\alpha)) = 0 \text{ акко је } p(\overline{\alpha}) = 0.$$

Не само то, него за све $k \geq 1$ важи:

$$(X - \alpha)^k \mid p \text{ у } F[X] \text{ акко } (X - \overline{\alpha})^k \mid p \text{ у } \overline{F}[X].$$

Наиме:

$$\begin{aligned}
(X-\alpha)^k \mid p \quad & \text{акко} \quad p = (X-\alpha)^k q, \text{ за неки } q \in F[X] \\
& \text{акко} \quad \widetilde{\varphi}(p) = \widetilde{\varphi}\left((X-\alpha)^k q\right) (\widetilde{\varphi} \text{ је „1–1”}) \\
& \text{акко} \quad \widetilde{\varphi}(p) = (X-\overline{\alpha})^k \widetilde{\varphi}(q) \\
& \text{акко} \quad p = (X-\overline{\alpha})^k \widetilde{\varphi}(q) \\
& \text{акко} \quad p = (X-\overline{\alpha})^k \overline{q}, \text{ за неки } \overline{q} \in \overline{F}[X] \\
& \text{акко} \quad (X-\overline{\alpha})^k \mid p.
\end{aligned}$$

Претпоследња еквиваленција наравно важи због тога што је $\widetilde{\varphi}$ „на”.

Дакле, свака нула полинома p у неком коренском пољу тог полинома одговара некој нули у другом коренском пољу и то са истим мултиплицитетом. Следећи став нам даје потребан и довољан услов да су све нуле датог полинома просте у неком коренском пољу тог полинома. Према претходном је онда то тачно и за свако коренско поље тог полинома.

Став 23 Ако је $f \in K[X] \setminus K$, онда су све његове нуле у неком његовом коренском пољу просте **акко** је $\mathrm{NZD}(f, f') = 1$. Посебно, ако је f нерастављив полином, све његове нуле су просте **акко** је $f' \neq 0$.

Доказ. Нека је $d = \mathrm{NZD}(f, f')$. Тада постоје полиноми $a, b \in K[X]$ такви да је

$$af + bf' = d. \tag{11}$$

$\Longleftarrow$. Ако је F коренско поље полинома f и $\alpha \in F$ вишеструка нула полинома f онда је она, као што добро знамо, и нула његовог извода f', па је на основу **(11)** она и нула полинома d, те је $d \neq 1$.

$\Longrightarrow$. Нека је $d \neq 1$. Како $d \mid f$, то постоји $q \in K[X]$, тако да је $f = dq$. Ако је E коренско поље полинома d и $\alpha \in E$ нека нула полинома d, онда је $f(\alpha) = d(\alpha)q(\alpha) = 0$, па α припада неком коренском пољу F полинома f, које је раширење поља E. Но, како $d \mid f'$ то је α и нула полинома f', па f има вишеструку нулу у том коренском пољу.

Претпоставимо сада да је f нерастављив. Како $d \mid f$, то мора бити или $d = 1$ или $d = f$. Дакле,

$$d \neq 1 \text{ акко } d = f \text{ акко } f \mid f' \text{ акко } f' = 0$$

Последња еквиваленција следи из чињенице да је степен полинома f' мањи од степена полинома f. Будући да смо установили да су све нуле полинома f просте **акко** је $d = 1$, закључујемо да су све нуле НЕРАСТАВЉИВОГ полинома f просте **акко** $f' \neq 0$. □

Дефиниција 24 Полином је СЕПАРАБИЛАН ако су све његове нуле у неком његовом коренском пољу просте.

Наравно, онда су оне просте и у сваком другом коренском пољу овог полинома.

Последица 25 Нека је $f \in K[X] \setminus K$ нерастављив полином и поље K карактеристике 0. Тада је f сепарабилан.

Доказ. На основу става 23 полином f је сепарабилан акко је $f' \neq 0$. Нека је $f = a_n X^n + \cdots + a_1 X + a_0$, где је $n \geqslant 1$ и $a_n \neq 0$. Тада је $f' = n a_n X^{n-1} + \cdots + a_1$. Како је K карактеристике нула, то је $n1_K \neq 0$, те је и $na_n = (n1_K) \cdot a_n \neq 0$, па је $f' \neq 0$. Тиме је доказ завршен. □

Дефиниција 26 Нека је L алгебарско раширење поља K. Елемент $\alpha \in L$ је СЕПАРАБИЛАН (над K) уколико је његов минимални полином $\mu_\alpha \in K[X]$ сепарабилан. Раширење L је сепарабилно раширење поља K, ако је сваки елемент из L сепарабилан над K.

Последица 27 Нека је K поље карактеристике 0 и L алгебарско раширење поља K. Тада је L/K сепарабилно раширење.

Доказ. У претходној последици смо видели да је сваки нерастављив полином сепарабилан. Стога је минимални полином сваког елемента из L сепарабилан, па је и раширење L/K сепарабилно. □

Напомена 28 Наравно, и само поље L је карактеристике 0, јер је $1_L = 1_K$, па је за свако $n \geqslant 1$: $n1_L = n1_K \neq 0$. ♠

Подсетимо се да за раширење E/F кажемо да је ПРОСТО уколико постоји елемент α такав да је $E = F(\alpha)$. За тај елемент кажемо да је ПРИМИТИВАН елемент тог раширења. Следећа теорема нам говори о егзистенцији примитивног елемента.

Теорема 29 Нека је K поље карактеристике 0 и $L = K(\alpha_1, \ldots, \alpha_n)$ коначно раширење поља K. Тада постоји $\lambda \in L$ такав да је $L = K(\lambda)$.

Доказ. Знамо да је K бесконачно поље. Доказ изводимо индукцијом по n и јасно је да је довољно показати тврђење за $n = 2$. Дакле, нека је $L = K(\alpha, \beta)$ и $\alpha \neq \beta$.

Знамо да су α и β сепарабилни над K и нека су μ_α и μ_β њихови минимални полиноми. Означимо са F коренско поље полинома $\mu_\alpha \cdot \mu_\beta$.

Како су елементи α и β сепарабилни, све нуле њихових минималних полинома су различите. Нека су

$$\alpha = \alpha_1, \alpha_2, \ldots, \alpha_k$$

нуле полинома μ_α, а

$$\beta = \beta_1, \beta_2, \ldots, \beta_l$$

нуле полинома μ_β. Наравно све се оне налазе у F. Нека је $c \in K \setminus \{0\}$. Посматрајмо потпоља E_c поља L задата са: $E_c = K(\alpha + c\beta)$. Желимо да докажемо да је $E_c = L$ за неко c. Посматрамо полином

$$f_c(X) = \mu_\alpha(\alpha + c(\beta - X)) = \mu_\alpha(\alpha + c\beta - cX) \in E_c[X].$$

Приметимо да је f_c формиран тако да је $f_c(\beta) = 0$:

$$f_c(\beta) = \mu_\alpha(\alpha + c(\beta - \beta)) = \mu_\alpha(\alpha) = 0.$$

Да ли је $f_c(\beta_r) = 0$ за неко $r \geq 2$? Видимо да је

$$f_c(\beta_r) = 0 \text{ акко } \mu_\alpha(\alpha + c(\beta - \beta_r)) = 0 \tag{12}$$

$$\text{акко } \alpha + c(\beta - \beta_r) = \alpha_s \text{ за неко } s \geq 2 \tag{13}$$

$$\text{акко } c = \frac{\alpha_s - \alpha}{\beta - \beta_r} \text{за неко } s \geq 2. \tag{14}$$

Посматрајмо скуп

$$R = \left\{ \frac{\alpha_s - \alpha}{\beta - \beta_r} : r \geqslant 2, s \geqslant 2 \right\}.$$

Скуп R је коначан, а поље K бесконачно. Стога сигурно постоји елемент $c_0 \in K \setminus (R \cup \{0\})$. На основу избора елемента c_0 имамо да је $f_{c_0}(\beta) = 0$ и $f_{c_0}(\beta_r) \neq 0$ за све $r \geq 2$. Како је β нула и полинома μ_β погодно је размотрити $\mathrm{NZD}(f_{c_0}, \mu_\beta)$. Полином f_{c_0} припада $E_{c_0}[X]$, док је $\mu_\beta \in K[X]$ и можемо га посматрати и као полином из $E_{c_0}[X]$. Свакако тада и

$$\mathrm{NZD}(f_{c_0}, \mu_\beta) \in E_{c_0}[X]. \tag{15}$$

Но, како је $\mu_\beta(X) = (X-\beta)(X-\beta_2)\cdots(X-\beta_l)$ у $K[X]$, а $f_{c_0}(\beta_r) \neq 0$ за $r \geq 2$, то је $\mathrm{NZD}(f_{c_0}, \mu_\beta) = X - \beta$. На основу **(15)** добијамо да $X - \beta \in E_{c_0}[X]$, те $\beta \in E_{c_0} = K(\alpha + c_0\beta)$. Но, тада имамо и $\alpha = (\alpha + c_0\beta) - c_0\beta \in K(\alpha + c_0\beta)$, те је $K(\alpha, \beta) \subseteq K(\alpha + c_0\beta)$. Обратна инклузија је очигледна и добили смо да је $K(\alpha, \beta) = K(\alpha + c_0\beta)$, те се за тражени примитиван елемент може узети елемент $\lambda = \alpha + c_0\beta$. □

Ако се погледа шта нам даје доказ који бисмо извели индукцијом, видимо да заправо постоје $c_2, \ldots, c_n \in K$ такви да је $K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n)$.

4 Аутоморфизми и конјугације

Посматрајмо два раширења поља L/K и F/K. Може постојати хомоморфизам $\pi\colon L \to F$ за који не важи да је $\pi(c) = c$ за све $c \in K$. Но, уколико је једнакост $\pi(c) = c$ испуњена за све $c \in K$, онда π није само хомоморфизам поља него и K-алгебри. Кажемо и да је π један K-хомоморфизам.

Дефиниција 30 Раширења L и F поља K су КОНЈУГОВАНА уколико постоји бар један K-изоморфизам $\pi\colon L \to F$. Елементи $\alpha \in L$ и $\overline{\alpha} \in F$ су КОНЈУГОВАНИ ако постоји K-изоморфизам π поља $K(\alpha)$ и $K(\overline{\alpha})$ такав да је $\pi(\alpha) = \overline{\alpha}$.

Став 31 Нека су L и F раширења поља K и $\alpha \in L$, $\overline{\alpha} \in F$. Ови елементи су конјуговани **акко** су или оба трансцендентни над K или имају исти минимални полином у $K[X]$.

Доказ. $\Longleftarrow$. Ако су и α и $\overline{\alpha}$ трансцендентни над K, онда је

$$K(\alpha) \cong K(X) \cong K(\overline{\alpha}).$$

Уколико је $\mu_\alpha = \mu_{\overline{\alpha}}$, онда имамо:

$$K(\alpha) \cong K[X]/\langle \mu_\alpha \rangle = K[X]/\langle \mu_{\overline{\alpha}} \rangle \cong K(\overline{\alpha}).$$

Наравно, у оба случаја је у питању K-изоморфизам у коме се α слика у $\overline{\alpha}$.

$\Longrightarrow$. Ако је $\pi\colon K(\alpha) \to K(\overline{\alpha})$ један K-изоморфизам, такав да је $\pi(\alpha) = \overline{\alpha}$, онда за сваки полином $p(X) = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ важи:

$$\pi(p(\alpha)) = \pi(a_0) + \pi(a_1)\pi(\alpha) + \cdots + \pi(a_n)\pi(\alpha)^n = a_0 + a_1\overline{\alpha} + \cdots + a_n\overline{\alpha}^n = p(\overline{\alpha}).$$

Како је π „1–1", то је $p(\alpha) = 0$ **акко** $p(\overline{\alpha}) = 0$. Пошто ово важи за сваки полином, онда су или оба елемента трансцендентна над K (дакле не анулирају ниједан полином над K) или је скуп полинома који анулирају непразан и исти за оба елемента, па тада имају и заједнички минимални полином. □

Сваки K-хоморфизам $\sigma\colon K(\alpha) \to L$, где је L раширење поља K потпуно је одређен вредношћу у α. Стога, ако је α алгебарски над K и ако је $\mu_\alpha \in K[X]$ његов минимални полином, онда различитих K-хомоморфизама из $K(\alpha)$ у L има онолико колико има различитих нула полинома μ_α у L. На пример, не постоји ниједан $\mathbb{Q}$-хомоморфизам из $\mathbb{Q}(i)$ у $\mathbb{R}$.

Наравно, са $\operatorname{Aut} L$ означавамо скуп свих аутоморфизама поља L, док са $G(L/K)$, где је L раширење поља K, означавамо скуп свих K-аутоморфизама поља L. Јасно је да је $G(L/K) \leqslant \operatorname{Aut} L$. Ако је пак $\Pi \leqslant \operatorname{Aut} L$, онда је

$$L^\Pi := \{a \in L : (\forall \pi \in \Pi)(\pi(a) = a)\}$$

потпоље од L. Наиме, ако $a, b \in L^\Pi$ и $\pi \in \Pi$, онда је $\pi(a \pm b) = \pi(a) \pm \pi(b) = a \pm b$, те $a \pm b \in L^\Pi$. Такође је $\pi(a \cdot b) = \pi(a) \cdot \pi(b) = a \cdot b$, те $a \cdot b \in L^\Pi$. Уколико је и $b \neq 0$, онда је $\pi(a/b) = \pi(a)/\pi(b) = a/b$, те и $a/b \in L^\Pi$.

Теорема 32 За свако коначно раширење L поља K следећи услови су еквивалентни.

(1) $K = L^{G(L/K)}$.

(2) $K = L^\Pi$ за неку коначну подгрупу $\Pi \leqslant \operatorname{Aut} L$.

(3) L је нормално и сепарабилно раширење поља K.

У том случају је $|G(L/K)| = [L : K]$.

Доказ. (1) $\Longrightarrow$ (2). Показаћемо да је $G(L/K)$ коначна група. Знамо да је L је векторски простор над K коначне димензије и нека је $n = \dim_K L$. Нека је $[e_1, \ldots, e_n]$ база тог простора. Према ранијој дискусији, ако је $\pi \in G(L/K)$, онда је за све i: $\pi(e_i)$ нула полинома μ_{e_i}. Како је π потпуно одређено вредностима на овој бази и за сваки елемент базе постоји само коначно много могућности, то је група $G(L/K)$ коначна и (2) је испуњено – за Π можемо узети баш $G(L/K)$.

(2) $\Longrightarrow$ (3). Дакле, $K = L^\Pi$ при чему је $\Pi = \{\pi_1, \ldots, \pi_k\}$ ($\pi_1 = \mathrm{id}_L$). Треба показати да се за свако $\alpha \in L$ његов минимални полином μ_α факторише на линеарне факторе у $L[X]$. Нека су $\alpha = \alpha_1, \ldots, \alpha_m$ све различите нуле полинома μ_α које се налазе у L. Тада за свако i, j: $\pi_i(\alpha_j) \in \{\alpha_1, \ldots, \alpha_m\}$. Како је π_i бијекција, то π_i пермутује елементе скупа $\{\alpha_1, \ldots, \alpha_m\}$.

Посматрамо полином

$$p = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_m) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in L[X].$$

Покажимо да је $p = \mu_\alpha$. Нека је $\pi \in \Pi$ и $\widetilde{\pi}\colon L[X] \to L[X]$ продужење дефинисано са $\widetilde{\pi}(X) = X$. Тада имамо

$$\begin{aligned} X^n + \pi(a_{n-1})X^{n-1} + \cdots + \pi(a_1)X + \pi(a_0) &= \widetilde{\pi}(X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0) \\ &= \widetilde{\pi}(p) = \widetilde{\pi}((X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_m)) \\ &= (\widetilde{\pi}(X) - \widetilde{\pi}(\alpha_1))(\widetilde{\pi}(X) - \widetilde{\pi}(\alpha_2)) \cdots (\widetilde{\pi}(X) - \widetilde{\pi}(\alpha_m)) \\ = (X - \pi(\alpha_1))(X - \pi(\alpha_2)) \cdots (X - \pi(\alpha_m)) &= X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0, \end{aligned}$$

пошто је $\{\pi(\alpha_1), \pi(\alpha_2), \ldots, \pi(\alpha_m)\} = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$. Дакле, за све $\pi \in \Pi$ и све $i = \overline{0, n-1}$ је $\pi(a_i) = a_i$, што значи да сви коефицијенти полинома p припадају $L^\Pi = K$. Према томе, $p \in K[X]$. Но, како су једине нуле полинома μ_α у L баш $\alpha_1, \ldots, \alpha_m$, то $p \mid \mu_\alpha$. Из чињенице да је μ_α нерастављив у $K[X]$, закључујемо да је $p = \mu_\alpha$ и видимо да је α сепарабилан над K. Како је α био произвољан елемент из L, то је раширење L/K заиста сепарабилно. Но, овај доказ нам уједно показује да је то раширење и нормално. Наиме, ако је $q \in K[X]$ нерастављив полином и

$\beta \in L$ нека нула тог полинома, онда је q заправо минималан полином тог елемента, а минималан полином сваког елемента се раставља на линеарне факторе у $L[X]$, те су му све нуле у L.

(3) $\Longrightarrow$ (1). Нека је L нормално и сепарабилно раширење поља K. Знамо да је тада $L = K(\alpha)$ за неко α. Посматрајмо минимални полином μ_α тог елемента. Он има тачно $n = [L : K]$ нула у L (раширење је нормално, па су му све нуле у L): $\alpha = \alpha_1, \ldots, \alpha_n$. Ако је $\pi \in G(L/K)$, онда $\pi(\alpha) \in \{\alpha_1, \ldots, \alpha_n\}$ и како је π потпуно одређено са $\pi(\alpha)$, то у $G(L/K)$ има тачно n аутоморфизама. Са π_r ћемо означавати онај аутоморфизам из $G(L/K)$ за који је $\pi_r(\alpha) = \alpha_r$.

Имамо да је $\boxed{|G(L/K)| = n = [L : K]}$. Треба показати да је $K = L^{G(L/K)}$. Јасно је да је $K \subseteq L^{G(L/K)}$.

Нека $a \in L^{G(L/K)}$. То значи да је за свако $r \in \{1, \ldots, n\}$: $\pi_r(a) = a$. Но, како $a \in L = K(\alpha)$, то је $a = p(\alpha)$, за неки полином $p = c_0 + c_1X + \cdots + c_{n-1}X^{n-1} \in K[X]$: $a = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$. Стога је

$$\begin{aligned}\pi_r(a) &= \pi_r(c_0) + \pi_r(c_1)\pi_r(\alpha) + \cdots + \pi_r(c_{n-1})\pi_r(\alpha)^{n-1} \\ &= c_0 + c_1\alpha_r + \cdots + c_{n-1}\alpha_r^{n-1} \\ &= p(\alpha_r).\end{aligned}$$

Дакле, $p(\alpha_r) = \pi_r(a) = a$. Посматрајмо сада полином $q(X) = p(X) - a \in L[X]$. То је полином степена $n-1$, а $q(\alpha_r) = 0$ за све $r \in \{1, \ldots, n\}$. Како ненула полином степена $n-1$ има највише $n-1$ нула у ма ком пољу, закључујемо да је $q(X)$ нула полином. То значи да је $c_1 = c_2 = \cdots = c_{n-1} = 0$ и $c_0 - a = 0$, те је $a = c_0 \in K$. □

5 Галоаова раширења поља

Дефиниција 33 За коначно раширење L поља K кажемо да је Галоаово уколико је $K = L^{G(L/K)}$.

Дакле, доказали смо следећу теорему.

Теорема 34 Коначно раширење L поља K је Галоаово ако и само ако је оно нормално и сепарабилно и тада је $[L : K] = |G(L/K)|$.

Група $G(L/K)$ зове се Галоаова група раширења L над K. Користи се и ознака $\mathrm{Gal}(L/K)$.

5.1 Галоаова кореспонденција

Нека је L/K Галоаово раширење и $G = G(L/K)$. Посматрамо два посета (у оба случаја парцијално уређење је задато инклузијом).

- $\mathcal{F}$ = скуп свих потпоља од L која садрже K.
- $\mathcal{P}$ = скуп свих подгрупа од G.

Постоји природна веза између ова два посета. Наиме, ако је $F \in \mathcal{F}$, онда је $F^\sharp \in \mathcal{P}$, где је $F^\sharp$ дефинисано са:

$$F^\sharp := \{\pi \in G : (\forall a \in F)\pi(a) = a\} = G(L/F).$$

Дакле, $F^\sharp$ чине аутоморфизми који фиксирају све елементе потпоља F. Такође, ако је $\Pi \leq G$, онда је $\Pi^\flat \in \mathcal{F}$, где је $\Pi^\flat$ дефинисано са:

$$\Pi^\flat = \{a \in L : (\forall \pi \in \Pi)\pi(a) = a\} (= L^\Pi).$$

Ово није тешко проверити. Осим тога

$$F_1 \subseteq F_2 \Longrightarrow F_1^\sharp \supseteq F_2^\sharp \qquad \text{и} \qquad \Pi_1 \subseteq \Pi_2 \Longrightarrow \Pi_1^\flat \supseteq \Pi_2^\flat.$$

Ово су таутолошке чињенице, као и следеће две:

$$\Pi \subseteq \Pi^{\flat\sharp}, \qquad F \subseteq F^{\sharp\flat}.$$

Наравно, $\Pi^{\flat\sharp} = \left(\Pi^\flat\right)^\sharp$ и $F^{\sharp\flat} = \left(F^\sharp\right)^\flat$. Уверимо се да ове инклузије важе. Нека $\pi \in \Pi$. Да бисмо се уверили да $\pi \in \Pi^{\flat\sharp}$, треба проверити да ли је $\pi(a) = a$ за све $a \in \Pi^\flat$. Но, $a \in \Pi^\flat$ акко $\sigma(a) = a$ за све $\sigma \in \Pi$. Наравно да је онда и $\pi(a) = a$, јер $\pi \in \Pi$! На сличан начин се доказује и друга инклузија.

Теорема 35 (Основна теорема коначне Галоаове теорије) Нека су ознаке као у претходном, при чему је L Галоаово раширење поља K. Тада важи.

(1) L је Галоаово раширење сваког поља $F \in \mathcal{F}$.

(2) Пресликавања $\Pi \mapsto \Pi^\flat$ и $F \mapsto F^\sharp$ су инверзна једно другом.

(3) $F \in \mathcal{F}$ је Галоаово раширење поља K **акко** је $F^\sharp \lhd G$ и тада је

$$G(F/K) \cong G/F^\sharp.$$

Доказ. (1) Нека је $\alpha \in L$ и $\mu_\alpha \in K[X]$ његов минимални полином. Пошто је раширење L/K нормално и сепарабилно, то се μ_α у L „цепа" на производ различитих линеарних фактора. Нека је сада $M_\alpha \in F[X]$ минимални полином за α над F. Наравно да и $\mu_\alpha \in F[X]$. Из чињенице да је $\mu_\alpha(\alpha) = 0$ и да је M_α минимални полином за α над F, добија се да $M_\alpha \mid \mu_\alpha$ у $F[X]$. Но, како се μ_α „цепа" на различите линеарне факторе у L, то се и његов фактор M_α такође „цепа" на различите линеарне факторе у L, те можемо закључити да је L нормално и сепарабилно раширење поља F.

(2) Треба показати да је $\Pi = \Pi^{\flat\sharp}$ за све $\Pi \in \mathcal{P}$ и да је $F = F^{\sharp\flat}$ за све $F \in \mathcal{F}$. Докажимо најпре

$$\big[L : F\big] = \big|F^{\sharp}\big| \tag{16}$$
$$\big[L : \Pi^{\flat}\big] = \big|\Pi\big|. \tag{17}$$

Приметимо да је $F^{\sharp} = G(L/F)$. Но, како на основу (1) знамо да је L/F Галоаово раширење, то је $[L : F] = |G(L/F)|$ и тиме је **(16)** доказано.

Нека $L = K(\alpha)$ и $M_\alpha \in \Pi^{\flat}[X]$ минимални полином за овај елемент, али над пољем $\Pi^{\flat}(= L^{\Pi})$. Наравно да је $L = \Pi^{\flat}(\alpha)$ и $\deg M_\alpha = [L : \Pi^{\flat}]$. Докажимо да је $\deg M_\alpha = |\Pi|$.

Ако $\pi \in \Pi$, онда је $M_\alpha(\pi(\alpha)) = 0$. Наиме, ако је

$$M_\alpha = d_0 + d_1 X + \cdots + d_{k-1}X^{k-1} + X^k,$$

где $d_i \in \Pi^{\flat}$, онда је $\pi(d_i) = d_i$ и стога из $M_\alpha(\alpha) = 0$, следи

$$\begin{aligned} 0 = \pi(M_\alpha(\alpha)) &= \pi(d_0 + d_1\alpha + \cdots + d_{k-1}\alpha^{k-1} + \alpha^k) \\ &= \pi(d_0) + \pi(d_1)\pi(\alpha) + \cdots + \pi(d_{k-1})\pi(\alpha)^{k-1} + \pi(\alpha)^k \\ &= d_0 + d_1\pi(\alpha) + \cdots + d_{k-1}\pi(\alpha)^{k-1} + \pi(\alpha)^k \\ &= M_\alpha(\pi(\alpha)). \end{aligned}$$

Дакле, $\pi(\alpha)$ је нула полинома M_α, а њих нема више од $\deg M_\alpha$. Осим тога, јасно је да за $\pi_1 \neq \pi_2$ мора бити $\pi_1(\alpha) \neq \pi_2(\alpha)$ (аутоморфизам од L је потпуно одређен вредношћу у α), па добијамо да број аутоморфизама у Π не може бити већи од степена полинома M_α:

$$|\Pi| \leq \deg M_\alpha. \tag{18}$$

Посматрајмо сад полином

$$q(X) = \prod_{\pi\in\Pi}(X - \pi(\alpha)). \tag{19}$$

Ако $\sigma \in \Pi$, ми га, као и пре, можемо продужити до изоморфизма $\widetilde{\sigma}\colon L[X] \to L[X]$. Тада је

$$\begin{aligned} \widetilde{\sigma}(q(X)) = \widetilde{\sigma}\left(\prod_{\pi\in\Pi}(X - \pi(\alpha))\right) &= \prod_{\pi\in\Pi}(\widetilde{\sigma}(X) - \widetilde{\sigma}(\pi(\alpha))) = \prod_{\pi\in\Pi}(X - \underbrace{(\sigma\circ\pi)}_{\pi'}(\alpha)) \\ = \prod_{\sigma^{-1}\circ\pi'\in\Pi}(X - \pi'(\alpha)) &= \prod_{\pi'\in\sigma\circ\Pi}(X - \pi'(\alpha)) = \prod_{\pi'\in\Pi}(X - \pi'(\alpha)) = q(X). \end{aligned}$$

Стога су сви коефицијенти полинома $q(X)$ фиксирани при сваком $\sigma \in \Pi$ и добијамо да је $q(X) \in \Pi^{\flat}[X]$. Но, јасно је да је $q(\alpha) = 0$. Стога је

он дељив минималним полиномом тог елемента, тј. $M_\alpha \mid q(X)$. Тако да добијамо да је

$$\deg M_\alpha \leq \deg q(X) = |\Pi|. \tag{20}$$

Из **(18)** и **(20)** добијамо да је $\deg M_\alpha = |\Pi|$, а како је $\deg M_\alpha = [L : \Pi^\flat]$ доказали смо **(17)**.

Коришћењем **(16)** и **(17)** није тешко доказати да је $\Pi = \Pi^{\flat\sharp}$ и $F = F^{\sharp\flat}$. Наиме:

$$\big|\Pi\big| \overset{\textbf{(17)}}{=\!=} \big[L : \Pi^\flat\big] \overset{\textbf{(16)}}{=\!=} \big|\Pi^{\flat\sharp}\big|.$$

Како су ово коначне групе и $\Pi \subseteq \Pi^{\flat\sharp}$ закључујемо да важи једнакост: $\Pi = \Pi^{\flat\sharp}$. Слично:

$$\big[L : F\big] \overset{\textbf{(16)}}{=\!=} \big|F^\sharp\big| \overset{\textbf{(17)}}{=\!=} \big[L : F^{\sharp\flat}\big].$$

Но, $F \subseteq F^{\sharp\flat}$ и како су све ово коначна раширења, мора бити $F = F^{\sharp\flat}$.

(3) Нека су $F_1, F_2 \in \mathcal{F}$. Докажимо да су ова поља конјугована акко су подгрупе $F_1^\sharp$ и $F_2^\sharp$ конјуговане као подгрупе од $G(L/K)$.

$\Longrightarrow$. Претпоставимо да су поља F_1 и F_2 конјугована, тј. да постоји K-изоморфизам $\sigma\colon F_1 \to F_2$. Како је, на основу ранијих резултата, $L = F_1(\alpha)$ и $L = F_2(\beta)$ за неке $\alpha, \beta \in L$ то можемо σ продужити до аутоморфизма $\widetilde{\sigma}$ поља L тако што додефинишемо $\widetilde{\sigma}(\alpha) = \beta$ (наравно да је $[L : F_1] = [L : F_2]$ пошто су F_1 и F_2 K-изоморфна и сва раширења су коначна). Ради једноставности, уместо $\widetilde{\sigma}$ писаћемо само σ. Тада за сваки $\tau \in G(L/K)$ имамо:

$$\begin{aligned}
\tau \in F_2^\sharp &\iff (\forall b \in F_2)\tau(b) = b \\
&\iff (\forall a \in F_1)\tau(\sigma(a)) = \sigma(a) \\
&\iff (\forall a \in F_1)\sigma^{-1}(\tau(\sigma(a)) = a \\
&\iff (\forall a \in F_1)(\sigma^{-1} \circ \tau \circ \sigma)(a) = a \\
&\iff \sigma^{-1} \circ \tau \circ \sigma \in F_1^\sharp \\
&\iff \tau \in \sigma F_1^\sharp \sigma^{-1}.
\end{aligned}$$

Дакле, $F_2^\sharp = \sigma F_1^\sharp \sigma^{-1}$, те су ове подгрупе конјуговане.

$\Longleftarrow$. Претпоставимо да су подгрупе $F_1^\sharp$ и $F_2^\sharp$ конјуговане, тј. да постоји $\sigma \in G(L/K)$ тако да је $F_2^\sharp = \sigma F_1^\sharp \sigma^{-1}$. Како знамо да је $F_2 = F_2^{\sharp\flat}$, то је $F_2 = (\sigma F_1^\sharp \sigma^{-1})^\flat$. Показаћемо да је $(\sigma F_1^\sharp \sigma^{-1})^\flat = \sigma[F_1]$ што ће нам дати доказ да су F_1 и F_2 конјугована поља (аутоморфизам σ индукује помоћу

сужења домена и кодомена K-изоморфизам ових поља).

$$\begin{aligned} a \in (\sigma F_1^\sharp \sigma^{-1})^\flat &\iff (\forall \tau \in F_1^\sharp)(\sigma \circ \tau \circ \sigma^{-1})(a) = a \\ &\iff (\forall \tau \in F_1^\sharp)(\tau \circ \sigma^{-1})(a) = \sigma^{-1}(a) \\ &\iff (\forall \tau \in F_1^\sharp)\tau(\sigma^{-1}(a)) = \sigma^{-1}(a) \\ &\iff \sigma^{-1}(a) \in F_1^{\sharp\flat} \\ &\iff \sigma^{-1}(a) \in F_1 \\ &\iff a \in \sigma[F_1]. \end{aligned}$$

Дакле, заиста је $(\sigma F_1^\sharp \sigma^{-1})^\flat = \sigma[F_1]$. [1] Посебно:

$$\begin{aligned} F^\sharp \lhd G(L/K) &\iff (\forall \sigma \in G(L/K))\sigma F^\sharp \sigma^{-1} = F^\sharp \\ &\iff (\forall \sigma \in G(L/K))(\sigma F^\sharp \sigma^{-1})^\flat = (F^\sharp)^\flat \\ &\iff (\forall \sigma \in G(L/K))\sigma[F] = F. \end{aligned}$$

Ми треба да докажемо да је у том случају F/K Галоаово, тј. да је $K = F^{G(F/K)}$. Довољно је доказати да је $F^{G(F/K)} \subseteq K$ пошто обратна инклузија тривијално важи. Претпоставимо да $a \in F^{G(F/K)}$. То значи да је $\pi(a) = a$ за све $\pi \in G(F/K)$. Докажимо да $a \in L^{G(L/K)}$. Знамо да L/K јесте Галоаово, па је $K = L^{G(L/K)}$ и то ће нам завршити доказ. Нека је $\sigma \in G(L/K)$. Из горње анализе знамо да σ сваки елемент из F слика у F, па стога индукује аутоморфизам $\underline{\sigma} \in G(F/K)$. Но, $a \in F^{G(F/K)}$, па је $\underline{\sigma}(a) = a$. Но, то заправо показује да је $\sigma(a) = a$. Како је ово тачно за свако $\sigma \in G(L/K)$, то $a \in L^{G(L/K)} = K$ и показали смо да је раширење F/K Галоаово.

Докажимо да важи и обратна импликација, тј. да из чињенице да је раширење F/K Галоаово следи да је подгрупа $F^\sharp$ нормална. Видели смо да се то своди на доказ чињенице да је за свако $\sigma \in G$ испуњено $\sigma[F] = F$. Заправо је довољно доказати да је за свако $\sigma \in G$: $\sigma[F] \subseteq F$. Наиме, онда важи и $\sigma^{-1}[F] \subseteq F$, па применом σ на ову инклузију добијамо да је $F \subseteq \sigma[F]$. Нека је $\alpha \in F$ произвољно и $\mu_\alpha \in K[X]$ минимални полином овог елемента. Тада је $\mu_\alpha(\sigma(\alpha)) = \sigma(\mu_\alpha(\alpha)) = \sigma(0) = 0$. Но, како је раширење F/K нормално, $\mu_\alpha \in K[X]$ нерастављив полином, а F садржи његов корен α, онда F садржи и све остале његове корене, те $\sigma(\alpha) \in F$.

Одредимо сада групу $G(F/K)$. Посматрајмо хомоморфизам

$$\phi\colon G(L/K) \to G(F/K)$$

задат са $\phi(\sigma) = \underline{\sigma}$ (користимо горњу ознаку). Имамо да је

$$\operatorname{Ker}\phi = \{\sigma \in G(L/K) : \underline{\sigma} = \mathrm{id}_F\} = \{\sigma \in G(L/K) : (\forall a \in F)\sigma(a) = a\} = F^\sharp.$$

[1] Корисно је овде приметити да за сваку подгрупу Π важи следећа једнакост: $\left(\sigma \Pi \sigma^{-1}\right)^\flat = \sigma\left[\Pi^\flat\right]$. Наиме, $\Pi = F_1^\sharp$ акко $\Pi^\flat = F_1$.

На основу прве теореме о изоморфизму за групе добијамо да је

$$G(L/K)/F^\sharp \cong \operatorname{Im}\phi \leq G(F/K).$$

Но,

$$|G(L/K)/F^\sharp| = \frac{|G(L/K|)}{|F^\sharp|} = \frac{[L:K]}{[L:F]} = \frac{[L:F]\cdot[F:K]}{[L:F]} = [F:K] = G(F/K),$$

па је ϕ заправо „на" и добијамо тражени изоморфизам. □

Приказаћемо сада нешто другачије доказе делова (2) и (посебно) (3) претходне теореме, који могу користити читаоцима да боље сагледају ове важне резултате.

Доказ за (2). Пре свега, $F^{\sharp\flat} = L^{F^\sharp} = L^{G(L/F)} = F$, јер је раширење L/F Галоаово као што смо показали у (1).

Имамо да је $\Pi^{\flat\sharp} = G(L/\Pi^\flat) = G(L/L^\Pi) \supseteq \Pi$, те је $|G(L/L^\Pi)| \geq |\Pi|$. Знамо да је $L = K(\alpha)$ за неко $\alpha \in L$ и нека је $M_\alpha \in L^\Pi[X]$ минимални полином за тај елемент, али над L^Π (наравно да је и $L^\Pi(\alpha) = L$). Посматрајмо као и у претходном доказу полином q задат за **(19)**. Као и пре, покаже се да је $q \in L^\Pi[X]$ и да $M_\alpha \mid q$ те имамо да је

$$|G(L/L^\Pi)| \overset{L/L^\Pi \text{ је Галоаово}}{=\!=\!=} [L:L^\Pi] = [L^\Pi(\alpha):L^\Pi] = \deg M_\alpha \leq \deg q = |\Pi|.$$

Дакле, добили смо да је $|\Pi^{\flat\sharp}| = |G(L/L^\Pi)| = |\Pi|$, те је и $\Pi^{\flat\sharp} = \Pi$. □

Видимо да се овај доказ незнатно разликује од претходног.

Доказ за (3). Приметимо да група G дејствује на $\mathcal{F}$: $\sigma \cdot F := \sigma[F]$. При овом дејству скуп $\mathcal{F}$ се 'распада' на дисјунктну унију орбита. Подсетимо се да су стабилизатори елемената из исте орбите конјуговане подгрупе. Заправо, важи једнакост: $\Sigma_{\sigma[F]} = \sigma\Sigma_F\sigma^{-1}$, где је са Σ_F означен стабилизатор елемента (у нашем случају поља) F. Приметимо да је $\Sigma_F = \{\sigma \in G : \sigma[F] = F\}$, док је $G(L/F) = \{\sigma \in G : (\forall x \in F)\sigma(x) = x\}$. Дакле, јасно је да ово нису исте подгрупе, али важи да је $G(L/F) \subseteq \Sigma_F$, те је, за свако $\sigma \in G$: $\sigma G(L/F)\sigma^{-1} \subseteq \sigma\Sigma_F\sigma^{-1} = \Sigma_{\sigma[F]}$. Покажимо да је заправо за свако $\sigma \in G$:

$$\sigma G(L/F)\sigma^{-1} = G(L/\sigma[F]).$$

Довољно је показати да је $\sigma G(L/F)\sigma^{-1} \subseteq G(L/\sigma[F])$ пошто онда друга инклузија следи из одговарајуће инклузије за σ^{-1}.

Нека је $\tau \in G(L/F)$ и $\alpha \in F$, а $\sigma \in G$ произвољно. Тада је

$$(\sigma\tau\sigma^{-1})(\sigma(\alpha)) = \sigma(\tau(\sigma^{-1}(\sigma(\alpha)))) = \sigma(\tau(\alpha)) \overset{\tau\in G(L/F),\alpha\in F}{=\!=\!=} \sigma(\alpha).$$

Дакле, $\sigma\tau\sigma^{-1} \in G(L/\sigma[F])$.

Посматрајмо сада поља чије су орбите једночлане. То су $F \in \mathcal{F}$ за које важи да је за свако $\sigma \in G$: $\sigma[F] = F$. Но, на основу доказаног тада за свако $\sigma \in G$ имамо да је $\sigma G(L/F)\sigma^{-1} = G(L/\sigma[F]) = G(L/F)$, дакле за свако такво поље F подгрупа $G(L/F)$ јесте нормална. Заправо, лако је видети да из чињенице да је $G(L/F)$ нормална следи да је и $\sigma[F] = F$ за свако $\sigma \in G$. Наиме, како је $G(L/F)$ нормална, према претходном је $G(L/F) = G(L/\sigma[F])$ за свако $\sigma \in G$. Но, тада је и

$$F \overset{L/F \text{ је нормално}}{=\!=\!=} F^{G(L/F)} = F^{G(L/\sigma[F])} \overset{L/\sigma[F] \text{ је нормално}}{=\!=\!=} \sigma[F].$$

Но, покажимо да услов да је $\sigma[F] = F$ за свако $\sigma \in G$ заправо значи да је раширење F/K Галоаово. Наиме, ако $\alpha \in F^{G(F/K)}$, посматрајмо $\sigma \in G$. Како је $\sigma[F] = F$, то σ индукује аутоморфизам $\underline{\sigma} \in G(F/K)$, редуковањем и домена и кодомена од σ на F. Како је тада $\sigma(\alpha) = \underline{\sigma}(\alpha) = \alpha$, закључујемо да $\alpha \in L^{G(L/K)} = K$. Такође, ако је F/K Галоаово, посматрајмо $\sigma \in G(L/K)$. Ако је $\alpha \in F$ и $\mu_\alpha \in K[X]$ његов минималан полином, онда је $\sigma(\alpha)$ нека нула тог полинома, али, пошто је раширење F/K нормално, знамо да су све нуле нерастављивог μ_α такође у F, па и $\sigma(\alpha) \in F$, те је $\sigma[F] \subseteq F$.

Дакле, показали смо да важи: $G(L/F)$ је нормална акко за све $\sigma \in G$ је $\sigma[F] = F$ акко је F/K Галоаово раширење. Одређивање групе $G(F/K)$ је урађено у претходном доказу за (3). □

Придруживање међупоља и подгрупа о којој говори претходна теорема зове се Галоаово придруживање (кореспонденција).

5.2 Једна примена

Тврђење које каже да је поље $\mathbb{C}$ алгебарски затворено, тј. да сваки полином из $\mathbb{C}[X]$ има нулу у $\mathbb{C}$ познато је као Основна теорема алгебре. Но, оно није у потпуности алгебарска теорема пошто конструкција поља $\mathbb{R}$ није алгебарска. Стога и било који доказ ове теореме мора укључити неку непрекидност. Требало би да нам је добро позната чињеница, која се свакако може доказати у оквиру курса Анализе 1, да сваки полином из $\mathbb{R}[X]$ непарног степена има реалну нулу. Осим ове чињенице, знање из средње школе нам показује да сваки полином другог степена из $\mathbb{C}[X]$ има нулу у $\mathbb{C}$.[2]

Теорема 36 (Основна теорема алгебре) Поље $\mathbb{C}$ је алгебарски затворено.

Доказ. Нека је $f \in \mathbb{C}[X]$ и K_f његово коренско поље. Нека је L нормално затворење раширења $K_f/\mathbb{R}$. Тада је раширење $L/\mathbb{R}$ Галоаово раширење као нормално раширење над пољем карактеристике 0. Наравно, знамо да је и раширење $L/\mathbb{C}$ Галоаово.

[2]Ово посебно значи да $\mathbb{C}$ нема раширење степена 2 — не постоји нерастављив полином над $\mathbb{C}$ степена 2.

Желимо да докажемо да је $K_f = \mathbb{C}$, а доказаћемо да је заправо $L = \mathbb{C}$. Претпоставимо да је $[L : \mathbb{C}] = 2^r(2m+1)$, где је $r \geq 0$ и $m \geq 0$. Како је $[\mathbb{C} : \mathbb{R}] = 2$, то је $[L : \mathbb{R}] = 2^{r+1}(2m+1)$ и $|G(L/\mathbb{R})| = 2^{r+1}(2m+1)$.

Претпоставимо да је $m > 0$. Нека је Π Силовљева 2-подгрупа ове групе. На основу **(17)**, имамо да је $[L : \Pi^\flat] = |\Pi| = 2^{r+1}$, те је $[\Pi^\flat : \mathbb{R}] = 2m+1$. Како је раширење $\Pi^\flat/\mathbb{R}$ сепарабилно као коначно раширење поља карактеристике 0, то је $\Pi^\flat = \mathbb{R}(\alpha)$. Ако је $\mu_\alpha \in \mathbb{R}[X]$ минимални полином овог елемента, онда је то нерастављив полином из $\mathbb{R}[X]$ степена $2m+1$, што није могуће, јер знамо да сваки полином из $\mathbb{R}[X]$ непарног степена има нулу у $\mathbb{R}$. Стога закључујемо да је $m = 0$ и $[L : \mathbb{R}] = 2^{r+1}$, тј. $[L : \mathbb{C}] = 2^r$.

Докажимо сада да мора бити $r = 0$. Уколико је $r = 1$, раширење $[L : \mathbb{C}]$ би било степена 2, а закључили смо да $\mathbb{C}$ нема раширење степена 2. Уколико је, пак, $r > 1$, онда $G(L/\mathbb{C})$ садржи подгрупу Π_1 реда 2^{r-1} и, као и горе, добијамо да је $[\Pi_1^\flat : \mathbb{C}] = 2$ и опет добијамо контрадикцију. Закључујемо да мора бити $r = 0$, те је заиста $L = \mathbb{C}$. □

6 Неки примери

Пример 37 Нека је $f = X^4 - 2 \in \mathbb{Q}[X]$ и K_f његово коренско поље. Одредити Галоаову кореспонденцију за раширење $K_f/\mathbb{Q}$.

Пре свега, јасно је да је раширење $K_f/\mathbb{Q}$ Галоаово пошто је K_f коренско поље полинома над пољем карактеристике 0. С обзиром да су сви четврти корени из 2:

$$x_1 = \sqrt[4]{2}, x_2 = i\sqrt[4]{2}(= ix_1), x_3 = -\sqrt[4]{2}(= -x_1), x_4 = -i\sqrt[4]{2}(= -x_2),$$

то је $K_f = \mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(\sqrt[4]{2}, i)$. Пошто $i \notin \mathbb{Q}(\sqrt[4]{2})$ и пошто је полином $X^4 - 2$ нерастављив над $\mathbb{Q}$ по Ајзенштајновом критеријуму, то је

$$[K_f : \mathbb{Q}] = [K_f : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

Потребно је да одредимо групу $G = G(K_f/\mathbb{Q})$ реда 8. Знамо да је она изоморфна некој од следећих група:

$$\mathbb{Z}_8, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{D}_4, \quad \mathbb{Q}_8.$$

Природно је посматрати аутоморфизме $\sigma, \pi \in G(K_f/\mathbb{Q})$ задате са:

$$\sigma(i) = -i, \sigma(\sqrt[4]{2}) = \sqrt[4]{2} \quad \text{и} \quad \pi(i) = i, \pi(\sqrt[4]{2}) = i\sqrt[4]{2}.$$

Јасно је да је $\sigma^2 = \mathrm{id}_{K_f}$. С друге стране,

$$\pi^2(\sqrt[4]{2}) = \pi(i\sqrt[4]{2}) = \pi(i)\pi(\sqrt[4]{2}) = i \cdot i\sqrt[4]{2} = -\sqrt[4]{2},$$

$$\pi^3(\sqrt[4]{2}) = \pi(-\sqrt[4]{2}) = -\pi\sqrt[4]{2} = -i\sqrt[4]{2},$$

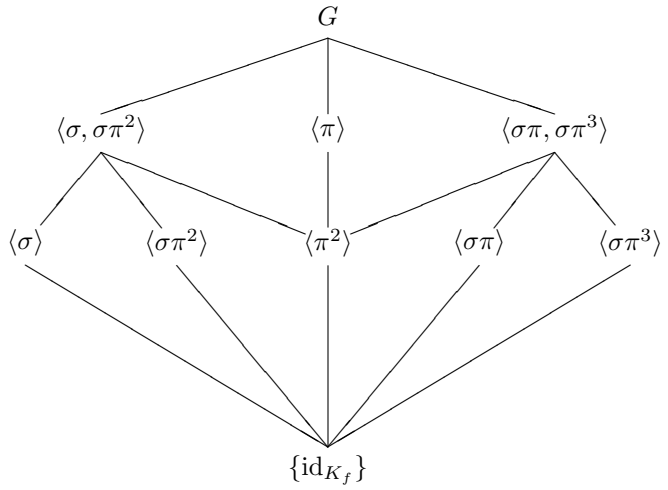
$$\pi^4(\sqrt[4]{2}) = \pi(-i\sqrt[4]{2}) = -\pi(i)\pi(\sqrt[4]{2}) = -i \cdot i\sqrt[4]{2} = \sqrt[4]{2}.$$

Дакле, π је реда 4. Упоредимо $\sigma\pi$ и $\pi^3\sigma$:

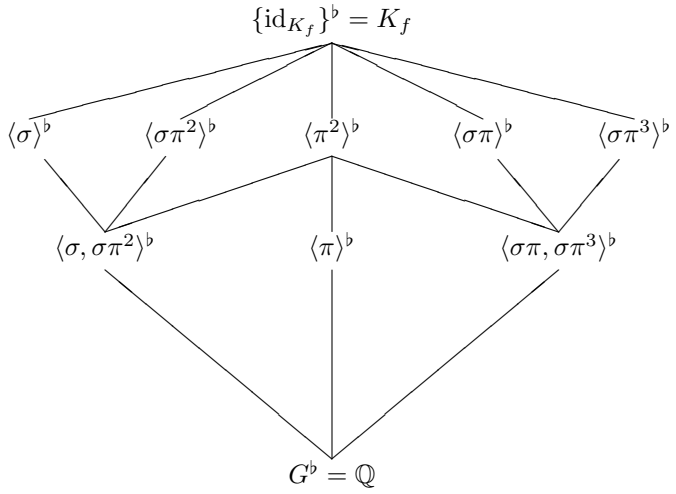
$$i \overset{\pi}{\longmapsto} i \overset{\sigma}{\longmapsto} -i, \quad \sqrt[4]{2} \overset{\pi}{\longmapsto} i\sqrt[4]{2} \overset{\sigma}{\longmapsto} -i\sqrt[4]{2},$$

$$i \overset{\sigma}{\longmapsto} -i \overset{\pi^3}{\longmapsto} -i, \quad \sqrt[4]{2} \overset{\sigma}{\longmapsto} \sqrt[4]{2} \overset{\pi^3}{\longmapsto} -i\sqrt[4]{2}.$$

Дакле, $\sigma\pi = \pi^3\sigma$ и можемо да закључимо да је у питању диједарска група са генераторима σ и π. Мрежа подгрупа групе G:



Одговарајућа мрежа потпоља је дата са:



Потребно је само још идентификовати ова потпоља. На основу **(17)** имамо да је $[\Pi^\flat : \mathbb{Q}] = [G : \Pi]$. Дакле, имамо три раширења од $\mathbb{Q}$ степена 2. На пример,

$$a \in \langle \pi \rangle^\flat \iff \pi(a) = a.$$

Но, фиксан елемент за π је i, а како је ово раширење степена 2, добијамо да је

$$\langle \pi \rangle^\flat = \mathbb{Q}(i).$$

Јасно је и да $\sqrt{2} = \left(\sqrt[4]{2}\right)^2 \in K_f$. Како је $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$, то је и $\sigma(\sqrt{2}) = \sqrt{2}$. Како је $\pi^2(\sqrt[4]{2}) = -\sqrt[4]{2}$, то је $\pi^2(\sqrt{2}) = \sqrt{2}$, те $\sqrt{2} \in \langle \sigma, \sigma\pi^2 \rangle^\flat$, а како је ово раширење степена 2 над $\mathbb{Q}$ имамо да је

$$\langle \sigma, \sigma\pi^2 \rangle^\flat = \mathbb{Q}(\sqrt{2}).$$

Није тешко наћи ни $\langle \sigma \rangle^\flat$. То је раширење од $\mathbb{Q}$ степена 4, а знамо да је $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$. Стога је

$$\langle \sigma \rangle^\flat = \mathbb{Q}(\sqrt[4]{2}).$$

Сложенији је проблем наћи фиксне тачке за, на пример, $\sigma\pi$. Проверимо где се сликају корени нашег полинома f.

	σ	π	$\sigma\pi$	π^2	$\sigma\pi^2$	π^3	$\sigma\pi^3$
x_1	x_1	x_2	x_4	x_3	x_3	x_4	x_2
x_2	x_4	x_3	x_3	x_4	x_2	x_1	x_1
x_3	x_3	x_4	x_2	x_1	x_1	x_2	x_4
x_4	x_2	x_1	x_1	x_2	x_4	x_3	x_3

Видимо да $\sigma\pi$ пермутује x_1 и x_4, те је $(\sigma\pi)(x_1 + x_4) = x_1 + x_4$. Но $x_1 + x_4 = (1 - i)\sqrt[4]{2} \in \langle \sigma\pi \rangle^\flat$, те је $\mathbb{Q}((1 - i)\sqrt[4]{2}) \subseteq \langle \sigma\pi \rangle^\flat$. Јасно је да овај елемент не задовољава ниједну квадратну једначину над $\mathbb{Q}$ (уверите се у то), те је $[\mathbb{Q}((1 - i)\sqrt[4]{2})) : \mathbb{Q}] = 4$, те је

$$\langle \sigma\pi \rangle^\flat = \mathbb{Q}((1 - i)\sqrt[4]{2})).$$

Из таблице се види да $\sigma\pi^3$ пермутује x_1 и x_2 те је $x_1 + x_2 \in \langle \sigma\pi^3 \rangle^\flat$. Како је $x_1 + x_2 = (1 + i)(\sqrt[4]{2})$, то као у претходном добијамо да је

$$\langle \sigma\pi^3 \rangle^\flat = \mathbb{Q}((1 + i)\sqrt[4]{2}).$$

Други начин да дођемо до овог резултата је да приметимо да је

$$\pi\langle \sigma\pi \rangle\pi^{-1} = \langle \pi\sigma \rangle = \langle \sigma\pi^3 \rangle,$$

па је на основу [1] $\langle \sigma\pi^3 \rangle^\flat = \pi\left[\mathbb{Q}((1 - i)\sqrt[4]{2})\right] = \mathbb{Q}((1-i)i\sqrt[4]{2}) = \mathbb{Q}((1+i)\sqrt[4]{2})$.

Како је $\pi^2(\sqrt[4]{2}) = -\sqrt[4]{2}$, то је $\pi^2(\sqrt{2}) = \sqrt{2}$. Узимајући у обзир да је $\pi(i) = i$, добијамо да је $i, \sqrt{2} \in \langle \pi^2 \rangle^\flat$. Као и раније, узимајући у обзир степен раширења, добијамо да је

$$\langle \pi^2 \rangle^\flat = \mathbb{Q}(i, \sqrt{2}) (= \mathbb{Q}(i + \sqrt{2})).$$

Из горње таблице видимо да $x_2 \in \langle \sigma\pi^2 \rangle^\flat$, те је $\mathbb{Q}(x_2) \subseteq \langle \sigma\pi^2 \rangle^\flat$, а како је $[\mathbb{Q}(x_2) : \mathbb{Q}] = 4$, видимо да овде важи једнакост:

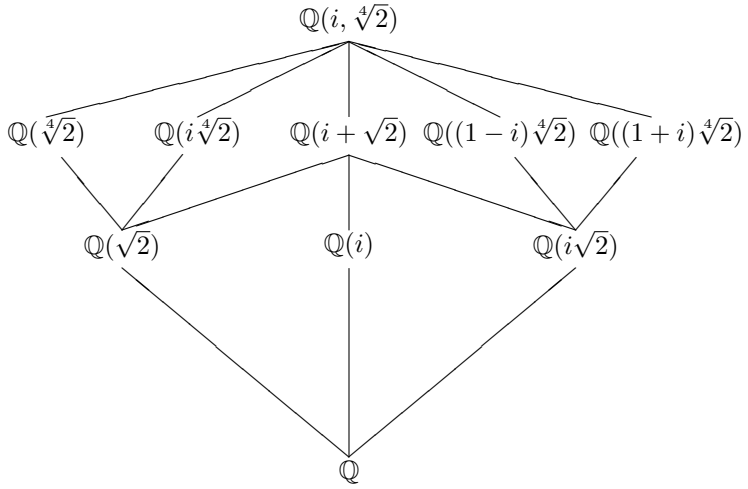
$$\langle \sigma\pi^2 \rangle^\flat = \mathbb{Q}(x_2) = \mathbb{Q}(i\sqrt[4]{2}).$$

И овде се резултат могао добити применом чињенице да је $\pi\langle\sigma\rangle\pi^{-1} = \langle\sigma\pi^2\rangle$ из које следи да је $\langle \sigma\pi^2 \rangle^\flat = \pi\left[\mathbb{Q}(\sqrt[4]{2})\right] = \mathbb{Q}(i\sqrt[4]{2})$.

Остало је још да одредимо $\langle \sigma\pi, \sigma\pi^3 \rangle^\flat$. Но, то је поље раширење степена 2 поља $\mathbb{Q}$ и садржано је у пољу $\mathbb{Q}\left((1+i)\sqrt[4]{2}\right)$. У том пољу се налази и елемент $((1+i)\sqrt[4]{2})^2 = 2i\sqrt{2}$. Но, није тешко проверити да је $i\sqrt{2} \in \langle \sigma\pi, \sigma\pi^3 \rangle^\flat$ те добијамо да је

$$\langle \sigma\pi, \sigma\pi^3 \rangle^\flat = \mathbb{Q}(i\sqrt{2}).$$

Приметимо да овај елемент припада и раширењу $\mathbb{Q}\left((1-i)\sqrt[4]{2}\right)$. Коначно имамо мрежу потпоља.



♣

Пример 38 Нека је $f = X^7 - 1 \in \mathbb{Q}[X]$ и K_f његово коренско поље. Одредити Галоаову кореспонденцију за раширење $K_f/\mathbb{Q}$.

Јасно је да су корени овог полинома сви седми корени из јединице и да су сви генерисани кореном $\zeta = \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$. Дакле, $K_f = \mathbb{Q}(\zeta)$.

Као што знамо од пре, минимални полином за ζ над $\mathbb{Q}$ је полином $\mu_\zeta = X^6 + \cdots + X + 1$, те је $[K_f : \mathbb{Q}] = 6$. За одређивање групе $G = G(K_f/\mathbb{Q})$, реда 6, приметимо да је сваки елемент из G потпуно одређен вредношћу у ζ. Нека је $\sigma_s \in G$ задато са $\sigma_s(\zeta) = \zeta^s$, за $1 \leq s \leq 6$. Проверимо композицију ова два аутоморфизма:

$$(\sigma_r \circ \sigma_s)(\zeta) = \sigma_r(\sigma_s(\zeta)) = \sigma_r(\zeta^s) = (\sigma_r(\zeta))^s = (\zeta^r)^s = \zeta^{rs} = \zeta^{r\cdot_7 s} = \sigma_{r\cdot_7 s}(\zeta).$$

Претпоследња једнакост важи зато што је $\zeta^7 = 1$. Дакле, можемо да констатујемо да је са $\phi(r) = \sigma_r$ задат један изоморфизам $\phi\colon U(\mathbb{Z}_7) \to G$. Стога је група G циклична. Како је $U(\mathbb{Z}_7) = \langle 3 \rangle$, то је $G = \langle \sigma_3 \rangle$. Њене једине праве подгрупе су $\langle \sigma_3^3 \rangle$, која је реда 2 и $\langle \sigma_3^2 \rangle$, која је реда 3. Имамо да је $\sigma_3^3 = \sigma_{3\cdot_7 3\cdot_7 3} = \sigma_6$ и $\sigma_3^2 = \sigma_{3\cdot_7 3} = \sigma_2$.

Одредимо најпре $\langle \sigma_2 \rangle^\flat$. Како је ова група реда 3, знамо да је раширење $\langle \sigma_2 \rangle^\flat / \mathbb{Q}$ степена 2. Елемент $\alpha = a + b\zeta + c\zeta^2 + d\zeta^3 + e\zeta^4 + f\zeta^5$ припада овом потпољу акко је $\sigma_2(\alpha) = \alpha$. Но,

$$\begin{aligned}\sigma_2(\alpha) &= a + b\zeta^2 + c\zeta^4 + d\zeta^8 + e\zeta + f\zeta^{10} \\ &= a + b\zeta^2 + c\zeta^4 + d(-1 - \zeta - \zeta^2 - \zeta^3 - \zeta^4 - \zeta^5) + e\zeta + f\zeta^3 \\ &= a - d + (e - d)\zeta + (b - d)\zeta^2 + (f - d)\zeta^3 + (c - d)\zeta^4 - d\zeta^5.\end{aligned}$$

Стога нам једнакост $\sigma_2(\alpha) = \alpha$ даје:

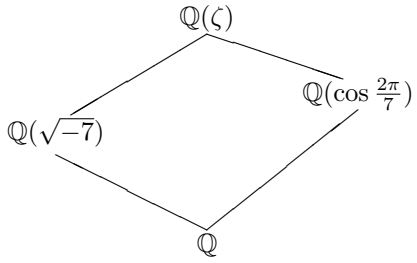
$$a = a - d, \quad b = e - d, \quad c = b - d, \quad d = f - d, \quad e = c - d, \quad f = -d.$$

Дакле, $d = f = 0$, $b = c = e$, па произвољни елемент из $\langle \sigma_2 \rangle^\flat$ облика $a + b(\zeta + \zeta^2 + \zeta^4)$, тј. $\langle \sigma_2 \rangle^\flat = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$. Елемент $\gamma = \zeta + \zeta^2 + \zeta^4$ задовољава неку једначину степена 2. Одредимо која је то једначина.

$$\begin{aligned}&\gamma^2 = (\zeta + \zeta^2 + \zeta^4)^2 = \zeta^2 + \zeta^4 + \zeta^8 + 2\zeta^3 + 2\zeta^5 + 2\zeta^6 \\ &= \zeta^2 + \zeta^4 + \zeta + 2\zeta^3 + 2\zeta^5 + 2(-1 - \zeta - \zeta^2 - \zeta^3 - \zeta^4 - \zeta^5) = -2 - \zeta - \zeta^2 - \zeta^4 = -2 - \gamma.\end{aligned}$$

Дакле, $\gamma^2 + \gamma + 2 = 0$. Стога је $\gamma \in \left\{\frac{-1 \pm \sqrt{-7}}{2}\right\}$. У сваком случају добијамо да је $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{-7})$.

Што се тиче поља $\langle \sigma_6 \rangle^\flat$, то можемо лакше одредити. Наиме, $\sigma_6(\zeta) = \zeta^6 = \zeta^{-1} = \bar{\zeta}$. Стога је $\sigma_6(\zeta + \bar{\zeta} = \zeta + \bar{\zeta}$, те $\mathbb{Q}(\zeta + \bar{\zeta}) \subseteq \langle \sigma_6 \rangle^\flat$. Но, при разматрању проблема конструктибилности правилног седмоугла, видели смо да је овај елемент корен једног нерастављивог полинома степена 3, те је заправо $\langle \sigma_6 \rangle^\flat = \mathbb{Q}(\zeta + \bar{\zeta})$. Приметимо да је $\zeta + \bar{\zeta} = 2\cos\frac{2\pi}{7}$, те је $\langle \sigma_6 \rangle^\flat = \mathbb{Q}(\cos\frac{2\pi}{7})$. Мрежа потпоља је представљена следећом сликом.



♣

Пример 39 Нека је $f = X^5 - 2 \in \mathbb{Q}[X]$ и K_f његово коренско поље. Одредити Галоаову кореспонденцију за раширење $K_f/\mathbb{Q}$.

Јасно је да је овај пример сложенији од претходна два. Заправо је нека врста комбинације претходна два примера. Полином f је нерастављив над $\mathbb{Q}$ и његови корени су сви пети корени из 2, а они су облика $\zeta^k \sqrt[5]{2}$, за $0 \leq k \leq 4$, где је $\zeta = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$. Стога је $K_f = \mathbb{Q}(\zeta, \sqrt[5]{2})$. Но, како је $X^5 - 2$ нерастављив полином, то је $[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$, а такође је и $\mu_\zeta = X^4 + X^3 + X^2 + X + 1$ нерастављив над $\mathbb{Q}$, те је $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$. Дакле, $5 \mid [K_f : \mathbb{Q}]$, као и $4 \mid [K_f : \mathbb{Q}$, а $[K_f : \mathbb{Q}] \leq 5 \cdot 4 = 20$. Стога је $[K_f : \mathbb{Q}] = 20$ и $G = G(K_f/\mathbb{Q})$ је група реда 20. Ако са s_5, односно s_2 означимо број Силовљевих 5-подгрупа, односно Силовљевих 2-подгрупа, онда имамо да $s_5 \mid 4$ и $s_5 \equiv 1 (\mathrm{mod}\, 5)$, те мора бити $s_5 = 1$, те је подгрупа реда 5 нормална. У групи G природно се истичу елементи σ и τ чије је дејство на генераторима задато кратком таблицом:

	σ	τ
ζ	ζ	ζ^2
$\sqrt[5]{2}$	$\zeta\sqrt[5]{2}$	$\sqrt[5]{2}$

Лако је проверити да је $\sigma^k(\sqrt[5]{2}) = \zeta^k \sqrt[5]{2}$ те закључујемо да је $N = \langle\sigma\rangle$ та нормална подгрупа реда 5. С друге стране је $\tau^k(\zeta) = \zeta^{2^k}$ и добијамо да је τ елемент реда 4 у групи G, те је и Силовљева 2-подгрупа циклична. Нека је $H = \langle\tau\rangle$ ту цикличну подгрупу. Како је $N \cap H$ тривијална подгрупа, то је $G = NH$.

Знамо да је N нормална. Да бисмо комплетирали разумевање групе G одредимо колико је $\tau\sigma\tau^{-1}$. Приметимо да је $\tau^{-1} = \tau^3$.

$$\zeta \overset{\tau^{-1}}{\longmapsto} \zeta^{2^3} = \zeta^3 \overset{\sigma}{\longmapsto} \zeta^3 \overset{\tau}{\longmapsto} (\zeta^2)^3 = \zeta,$$

$$\sqrt[5]{2} \overset{\tau^{-1}}{\longmapsto} \sqrt[5]{2} \overset{\sigma}{\longmapsto} \zeta\sqrt[5]{2} \overset{\tau}{\longmapsto} \zeta^2\sqrt[5]{2}.$$

Но, како је $\sigma^2(\zeta) = \zeta$ и $\sigma^2(\sqrt[5]{2}) = \zeta^2\sqrt[5]{2}$ закључујемо да је $\tau\sigma\tau^{-1} = \sigma^2$. Дакле, група G свакако није комутативна, а одатле одмах закључујемо да подгрупа H није нормална. Но, све Силовљеве 2-подгрупе су међусобно коњуговане, те закључујемо да су све подгрупе реда 4 облика $\sigma^k H\sigma^{-k}$ за $0 \leq k \leq 4$. Наиме, све су ове подгрупе различите – у супротном би неки нетривијалан степен од σ био у нормализатору подгрупе H, а како је ред од σ прост број, добили бисмо да је H нормална, што није. Одредимо заправо ове групе тако што ћемо наћи $\sigma^k\tau\sigma^{-k}$.

Приметимо да је $\sigma^{-1} = \sigma^4$. Из $\tau\sigma\tau^{-1} = \sigma^2$, добијамо да је

$$\tau\sigma = \sigma^2\tau. \tag{21}$$

Из **(21)** индукцијом се лако показује да је

$$\tau\sigma^k = \sigma^{2k}\tau. \tag{22}$$

Стога је $\sigma\tau\sigma^{-1} = \sigma\tau\sigma^4 = \sigma\sigma^8\tau = \sigma^4\tau$. Тада је

$$\sigma^2\tau\sigma^{-2} = \sigma(\sigma\tau\sigma^{-1})\sigma^{-1} = \sigma(\sigma^4\tau)\sigma^{-1} = \sigma^5\tau\sigma^4 = \sigma^5\sigma^8\tau = \sigma^3\tau;$$

$$\sigma^3\tau\sigma^{-3} = \sigma(\sigma^2\tau\sigma^{-2})\sigma^{-1} = \sigma(\sigma^3\tau)\sigma^4 = \sigma^4\sigma^8\tau = \sigma^2\tau;$$

$$\sigma^4\tau\sigma^{-4} = \sigma(\sigma^3\tau\sigma^{-3})\sigma^{-1} = \sigma(\sigma^2\tau)\sigma^4 = \sigma^3\sigma^8\tau = \sigma\tau.$$

Дакле, подгрупе реда 5 су: $\langle\sigma^k\tau\rangle$ за $0 \leq k \leq 4$.

Знамо да је свака група реда 2 садржана у некој Силовљевој 2-подгрупи. Но, како су оне све цикличне, и имају тачно по једну подгрупу реда 2, то имамо највише 5 подгрупа реда 2. Питање је да ли се подгрупе реда 4 нетривијално секу. У групи H подгрупа реда 2 генерисана је елементом τ^2. Одредимо колико је $\sigma^k\tau^2\sigma^{-k}$.

$$\sigma\tau^2\sigma^{-1} = (\sigma\tau\sigma^{-1})^2 = (\sigma^4\tau)^2 = \sigma^4\tau\sigma^4\tau = \sigma^4\sigma^8\tau\tau = \sigma^2\tau^2;$$

$$\sigma^2\tau^2\sigma^{-2} = (\sigma^2\tau\sigma^{-2})^2 = (\sigma^3\tau)^2 = \sigma^3\tau\sigma^3\tau = \sigma^3\sigma^6\tau\tau = \sigma^4\tau^2;$$

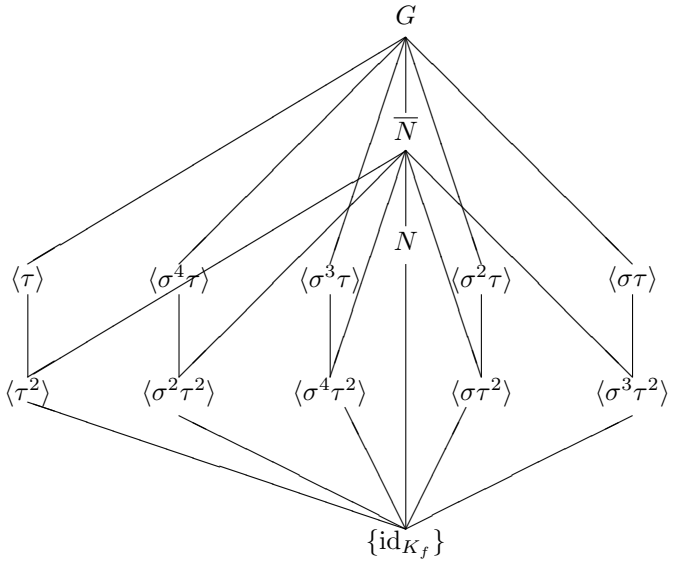
$$\sigma^3\tau^2\sigma^{-3} = (\sigma^3\tau\sigma^{-3})^2 = (\sigma^2\tau)^2 = \sigma^2\tau\sigma^2\tau = \sigma^2\sigma^4\tau\tau = \sigma\tau^2;$$

$$\sigma^4\tau^2\sigma^{-4} = (\sigma^4\tau\sigma^{-4})^2 = (\sigma\tau)^2 = \sigma\tau\sigma\tau = \sigma\sigma^2\tau\tau = \sigma^3\tau^2;$$

Дакле, елементи $\sigma^k\tau^2$, за $0 \leq k \leq 4$ су генератори група реда 2.

Остаје да проверимо има ли група реда 10. С обзиром да је N нормална подгрупа, онда је $\overline{N} = N\cdot\langle\tau^2\rangle \leq G$ реда 10 и она је нормална, јер је индекса 2. Но, то је уједно и једина подгрупа реда 10. Наиме, ова подгрупа садрже све елементе реда 2: сви елементи реда 2 су облика $\sigma^k\tau^2\sigma^{-k}$ и како је та подгрупа нормална и садржи τ^2, она садржи и све ове елементе.

Дакле, имамо једну подгрупу реда 5 која је нормална, 5 подгрупа реда 4 које су све међусобно конјуговане, 5 подгрупа реда 2, које су такође све међусобно конјуговане и једну подгрупу реда 10.



Одредимо сада одговарајућа поља. Пре свега, јасно је да је $N^\flat = \langle\sigma\rangle^\flat = \mathbb{Q}(\zeta)$, пошто је $[\langle\sigma\rangle^\flat : \mathbb{Q}] = [G : N] = 4$, а $\sigma(\zeta) = \zeta$. Како је $\left[\overline{N}^\flat : \mathbb{Q}\right] = \left[G : \overline{N}\right] = 2$, потребно нам је квадратно раширење од $\mathbb{Q}$. Но, $\overline{N} = \langle\sigma, \tau^2\rangle$, па је ово раширење садржано у $\langle\sigma\rangle^\flat = \mathbb{Q}(\zeta)$. Сада можемо да се присетимо шта смо радили раније у случају седмог корена из јединице. Ово ζ задовољава једначину

$$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0,$$

што после дељења са ζ^2 даје:

$$\zeta^2 + \zeta + 1 + \frac{1}{\zeta} + \frac{1}{\zeta^2} = 0. \tag{23}$$

Нека је $\xi = \zeta + \frac{1}{\zeta} = \zeta + \zeta^4$. Приметимо да је

$$\tau^2(\xi) = \tau^2(\zeta + \zeta^4) = \tau(\tau(\zeta)) + (\tau(\tau(\zeta)))^4 = \tau(\zeta^2) + (\tau(\zeta^2))^4 = \zeta^4 + \zeta^{16} = \xi.$$

Дакле, $\xi \in \overline{N}^\flat$. Но, из **(23)** добијамо да је

$$\xi^2 + \xi - 1 = 0.$$

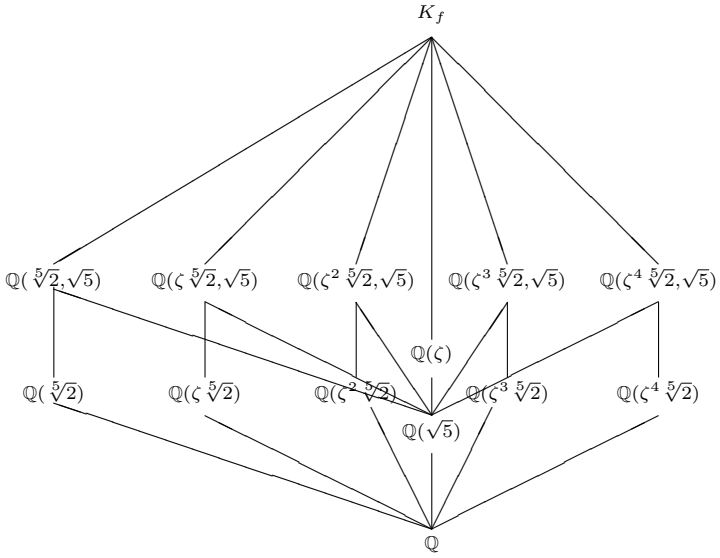
Одавде је $\xi \in \{\frac{-1\pm\sqrt{5}}{2}\}$. Дакле, $\overline{N}^\flat = \mathbb{Q}(\xi) = \mathbb{Q}(\sqrt{5})$.

Како је $\tau(\sqrt[5]{2}) = \sqrt[5]{2}$ и $[\langle\tau\rangle^\flat : \mathbb{Q}] = [G : \langle\tau\rangle] = 5$, то је $\langle\tau\rangle^\flat = \mathbb{Q}(\sqrt[5]{2})$. Сада можемо да одредимо и остала поља облика $\langle\sigma^k\tau\rangle^\flat$, користећи [1]:

$$\begin{aligned}
\langle\sigma\tau\rangle^\flat &= (\sigma^4\langle\tau\rangle\sigma^{-4})^\flat = \sigma^4[\mathbb{Q}(\sqrt[5]{2})] = \mathbb{Q}(\zeta^4\sqrt[5]{2});\\
\langle\sigma^2\tau\rangle^\flat &= (\sigma^3\langle\tau\rangle\sigma^{-3})^\flat = \sigma^3[\mathbb{Q}(\sqrt[5]{2})] = \mathbb{Q}(\zeta^3\sqrt[5]{2});\\
\langle\sigma^3\tau\rangle^\flat &= (\sigma^2\langle\tau\rangle\sigma^{-1})^\flat = \sigma^2[\mathbb{Q}(\sqrt[5]{2})] = \mathbb{Q}(\zeta^2\sqrt[5]{2});\\
\langle\sigma^4\tau\rangle^\flat &= (\sigma\langle\tau\rangle\sigma^{-1})^\flat = \sigma[\mathbb{Q}(\sqrt[5]{2})] = \mathbb{Q}(\zeta\sqrt[5]{2}).
\end{aligned}$$

Већ смо видели да $\sqrt{5} \in \langle\tau^2\rangle^\flat$. Како је и $\tau(\sqrt[5]{2}) = \sqrt[5]{2}$, узимајући у обзир и степен раширења, добијамо да је $\langle\tau^2\rangle^\flat = \mathbb{Q}(\sqrt[5]{2}, \sqrt{5})$. Тада је

$$\begin{aligned}
\langle\sigma^2\tau^2\rangle^\flat &= \sigma[\mathbb{Q}(\sqrt[5]{2}, \sqrt{5})] = \mathbb{Q}(\zeta\sqrt[5]{2}, \sqrt{5});\\
\langle\sigma^4\tau^2\rangle^\flat &= \sigma^2[\mathbb{Q}(\sqrt[5]{2}, \sqrt{5})] = \mathbb{Q}(\zeta^2\sqrt[5]{2}, \sqrt{5});\\
\langle\sigma\tau^2\rangle^\flat &= \sigma^3[\mathbb{Q}(\sqrt[5]{2}, \sqrt{5})] = \mathbb{Q}(\zeta^3\sqrt[5]{2}, \sqrt{5});\\
\langle\sigma^3\tau^2\rangle^\flat &= \sigma^4[\mathbb{Q}(\sqrt[5]{2}, \sqrt{5})] = \mathbb{Q}(\zeta^4\sqrt[5]{2}, \sqrt{5}).
\end{aligned}$$



♣

Читаоци би за вежбу могли да провере која су од ових раширења нормална.

7 Коренско поље сепарабилног полинома

Следећу лему наводимо без доказа.

Лема 40 (Артинова лема) Нека је G коначна група аутоморфизама поља L. Тада је $[L : L^G] \leq |G|$.

Став 41 Нека је K поље, $f \in K[X]$ сепарабилан полином и L његово коренско поље. Тада је раширење L/K Галоаово.

Доказ. Наравно, раширење L/K је коначно. Нека је $G = G(L/K)$. Треба доказати да је $L^G = K$. Нека је $K' = L^G$. Поље L је коренско поље за f и када се f посматра као полином из $K'[X]$. Како је f сепарабилан полином, све његове нуле у L су различите и он ту има $n = \deg f$ нула: $L = K(\alpha_1, \ldots, \alpha_n)$. Покажимо најпре да је $[L : K] = |G(L/K)|$. На потпуно аналоган начин се доказује да је $[L : K'] = |G(L/K')|$.

Нека је $\mu_{\alpha_1} \in K[X]$ минимални полином елемента α_1. Како је $f(\alpha_1) = 0$, то $\mu_{\alpha_1} \mid f$, те је и полином μ_{α_1} сепарабилан. K-хомоморфизама из $K(\alpha_1)$ у L има колико и нула његовог минималног полинома μ_{α_1} у L. Но, с обзиром да се и μ_{α_1} цепа на линеарне факторе у $L[X]$, тих хоморфизама има $\deg \mu_{\alpha_1} = [K(\alpha_1) : K]$. Посматрајмо сада елемент α_2 и његов минималан полином $\mu_{\alpha_2} \in K(\alpha_1)[X]$. И $\mu_{\alpha_2} \mid f$. Стога добијамо да је број проширења K-хомоморфизма из $K(\alpha_1)$ у L до K-хомоморфизама из $K(\alpha_1, \alpha_2)$ у L једнак $\deg \mu_{\alpha_2} = [K(\alpha_1, \alpha_2) : K(\alpha_1)]$. Као последицу добијамо да је број K-хомоморфизама из $K(\alpha_1, \alpha_2)$ у L једнак $[K(\alpha_1) : K] \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)] = [K(\alpha_1, \alpha_2) : K]$. Понављањем поступка коначно добијамо да је број K-хомоморфизама $L = K(\alpha_1, \ldots, \alpha_n)$ у L једнак $[L : K]$. Но, како је раширење L/K коначно, ови K-хомоморфизми нису само „1–1", него су и „на", те је $|G(L/K)| = [L : K]$.

Приметимо да је $G \leq G(L/K')$. Ово је таутолошка чињеница: K' заправо чине они елементи у L који су фиксирани елементима из G, те је свакако сваки K-аутоморфизам од L (дакле, елемент из G) такође и K'-аутоморфизам од L.

Имамо следећи низ неједнакости:

$$[L : K'] = [L : L^G] \leq |G| \leq |G(L/K')| = [L : K'].$$

Прва неједнакост следи из Артинове леме. Дакле, $[L : K'] = |G| = [L : K]$, а како је $K \subseteq K' \subseteq L$ и све су ово коначна раширења, добијамо да је $K' = K$, што је и тражено. □

7.1 Дискриминанта

Нека је $f \in K[X]$ моничан сепарабилан полином и K_f његово коренско поље. Сада знамо да је K_f/K Галоаово раширење. Ако је $\deg f = n$, пошто је то сепарабилан полином, он има n различитих нула (корена) у K_f. Нека су то $\alpha_1, \ldots, \alpha_n$. Ако је $G = G(K_f/K)$ одговарајућа Галоава група, зваћемо је и Галоаовом групом тог полинома. Као и раније,

можемо да констатујемо да за све $\sigma \in G$ и све α_i: $\sigma(\alpha_i) \in \{\alpha_1, \ldots, \alpha_n\}$. Заправо σ пермутује ове корене и имамо дефинисан природан мономорфизам из $\Phi\colon G \to \mathbb{S}_n$ (сваки σ је потпуно одређен вредностима које узима у тим коренима). Нека је $\widetilde{\sigma} = \Phi(\sigma)$, а $\operatorname{Im}\Phi = G_f \leq \mathbb{S}_n$. Природно је запитати се када је, на пример, $G_f \subseteq \mathbb{A}_n$. У ту сврху, дефинишимо два елемента из K_f:

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

$D(f)$ је ДИСКРИМИНАНТА полинома f и може се дефинисати и када нису сви корени различити. У сваком случају је $D(f) \neq 0$ **акко** је полином f сепарабилан.

Став 42 Нека је $f \in K[X]$ сепарабилан полином. Користимо уведене ознаке. Тада је

а) $\sigma(\Delta(f)) = \operatorname{sgn}(\widetilde{\sigma})\Delta(f)$;

б) $\sigma(D(f)) = D(f)$. Посебно, $D(f) \in K$.

Доказ. Заправо, доказ за а) је извођен при дефинисању детерминанте, или при извођењу првих последица. А доказ за б) је једноставна последица резултата под а). □

Последица 43 Ако је $\operatorname{char} K \neq 2$, онда је

$$\{\sigma \in G(K_f/K) : \widetilde{\sigma} \in \mathbb{A}_n\}^\flat = K(\Delta(f)).$$

Посебно: $G_f \subseteq \mathbb{A}_n$ **акко** $\Delta(f) \in K$ **акко** $D(f)$ је квадрат у K.

Доказ. Приметимо да је $\{\sigma \in G(K_f/K) : \widetilde{\sigma} \in \mathbb{A}_n\} = \Phi^{-1}[\mathbb{A}_n]$. Како је $[\mathbb{S}_n : \mathbb{A}_n] = 2$, то је $[G : \Phi^{-1}[\mathbb{A}_n]] \leq 2$. На основу претходног става $\sigma(\Delta(f)) = \Delta(f)$ **акко** $\widetilde{\sigma} \in \mathbb{A}_n$. Дакле,

$$\Delta(f) \in \{\sigma \in G(K_f/K) : \widetilde{\sigma} \in \mathbb{A}_n\}^\flat = \left(\Phi^{-1}[\mathbb{A}_n]\right)^\flat,$$

те је $K(\Delta(f)) \subseteq \{\sigma \in G(K_f/K) : \widetilde{\sigma} \in \mathbb{A}_n\}^\flat$. Но,

$$[\{\sigma \in G(K_f/K) : \widetilde{\sigma} \in \mathbb{A}_n\}^\flat : K] = [G : \Phi^{-1}[\mathbb{A}_n]] \leq 2.$$

Но, како је $[K(\Delta(f)) : K] \leq 2$, можемо да закључимо да је $\{\sigma \in G(K_f/K) : \widetilde{\sigma} \in \mathbb{A}_n\}^\flat = K[\Delta(f)]$. Наиме, $\Delta(f) \in K$ **акко** $G_f \subseteq \mathbb{A}_n$ **акко** $\Phi^{-1}[\mathbb{A}_n] = G$. Остало је да се подсетимо да је $D(f) = \Delta(f)^2$. □

Пример 44 Ако је $f = X^2 + bX + c$ одредити $D(f)$.

Ако је $f = (X - \alpha_1)(X - \alpha_2)$, онда је $c = \alpha_1\alpha_2$, а $b = -(\alpha_1 + \alpha_2)$. Тада $D(f) = (\alpha_1 - \alpha_2)^2 = \alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = b^2 - 4ac$. ♣

Пример 45 Ако је $f = X^3 + bX + c$, одредити $D(f)$.

Ако је $f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$, онда је

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \quad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = b, \quad \alpha_1\alpha_2\alpha_3 = -c.$$

Дакле, $\alpha_3 = -\alpha_1 - \alpha_2$. Стога је

$$b = \alpha_1\alpha_2 - \alpha_1(\alpha_1 + \alpha_2) - \alpha_2(\alpha_1 + \alpha_2) = -(\alpha_1^2 + \alpha_1\alpha_2 + \alpha_2^2).$$

Аналогно добијамо да је и

$$\alpha_1^2 + \alpha_1\alpha_3 + \alpha_3^2 = -b, \quad \alpha_2^2 + \alpha_2\alpha_3 + \alpha_3^2 = -b.$$

Сада рачунамо:

$$\begin{aligned} D(f) &= (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 \\ &= (\alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2)(\alpha_1^2 - 2\alpha_1\alpha_3 + \alpha_3^2)(\alpha_2^2 - 2\alpha_2\alpha_3 + \alpha_3^2) \\ &= (-b - 3\alpha_1\alpha_2)(-b - 3\alpha_2\alpha_3)(-b - 3\alpha_1\alpha_2) \\ &= -b^3 - 3b^2(\underbrace{\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3}_{=b}) - 3b\alpha_1\alpha_2\alpha_3(\underbrace{\alpha_1 + \alpha_2 + \alpha_3}_{=0}) - 27(\underbrace{\alpha_1\alpha_2\alpha_3}_{=-c})^2 \\ &= -4b^3 - 27c^2. \quad \clubsuit \end{aligned}$$

8 Галоава група полинома као група пермутација корена

Ако група G дејствује на скупу X и ако је $x \in X$, онда постоји бијекција између левог косет простора G/Σ_x и орбите $\Omega(x)$. За дејство кажемо да је ТРАНЗИТИВНО ако постоји само једна орбита при овом дејству, тј. ако је за сваки $x \in X$: $\Omega(x) = X$. Тада за СВАКО $x \in X$ постоји бијекција између G/Σ_x и X.

У случају да имамо полином $f \in K[X]$, група $G(K_f/K)$ дејствује на скупу свих корена $\{\alpha_1, \ldots, \alpha_n\}$, а група G_f на скупу $\{1, \ldots, n\}$ (користимо ознаке од пре).

Став 46 Нека је $f \in K[X]$ сепарабилан полином. Тада је он нерастављив акко $G(K_f/K)$ транзитивно дејствује на скупу корена $\{\alpha_1, \ldots, \alpha_n\}$.

Доказ. $\Longrightarrow$. Нека је $\deg(f) = n$ и $\alpha, \beta \in \{\alpha_1, \ldots, \alpha_n\}$. Како је f нерастављив, то је он минимални полином и за α и за β, па постоји K-изоморфизам $\sigma : K(\alpha) \cong K(\beta)$, такав да је $\sigma(\alpha) = \beta$. Наравно да σ можемо да проширимо до $\widetilde{\sigma} \in G(K_f/K)$ као и раније (свакако није јединствено проширење!). Дакле, дејство $G(K_f/K)$ јесте транзитивно: за свака два α, β постоји $\widetilde{\sigma}$ тако да је $\widetilde{\sigma}(\alpha) = \beta$.

$\Longleftarrow$. Нека је g нерастављив фактор од f у $K[X]$, $\alpha, \beta \in K_f$ такви да је $g(\alpha) = 0$, $f(\beta) = 0$. Како је $f = g \cdot h$ за неко h, свакако је и $f(\alpha) = 0$. По претпоставци о транзитивности дејства, постоји $\sigma \in G(K_f/K)$ тако да је $\sigma(\alpha) = \beta$. Пошто је $g \in K[X]$, то је

$$g(\beta) = g(\sigma(\alpha)) = \sigma(g(\alpha)) = \sigma(0) = 0.$$

Дакле, β је и корен од g. Тако добијамо да је сваки корен од f уједно и корен од g. Како је f сепарабилан полином и g његов нерастављив фактор, ово је могуће само ако је $f = g$, па закључујемо да је f нерастављив. □

Дакле, ако је f сепарабилан и нерастављив полином степена n и α неки корен полинома f у K_f, важи следеће:

$$\underbrace{[K(\alpha) : K)]}_{=n} \quad \Big| \quad \underbrace{[K_f : K]}_{=|G(K_f/K)|=|G_f|} \quad .$$

Добијамо да је G_f транзитивна група пермутација скупа $\{1, \ldots, n\}$ чији је ред дељив са n.

Питање. Да ли ред сваке транзитивне групе пермутација скупа $\{1, \ldots, n\}$ мора бити дељив са n?

8.1 Полиноми степена 3

Нека је $f \in K[X]$ нерастављив полином степена 3. Овај полином **није** сепарабилан **акко** је $\operatorname{char} K = 3$ и $f = X^3 - a$ за неко $a \in K$ које није трећи степен неког елемента из K. У случају да полином јесте сепарабилан, група $G_f \leq \mathbb{S}_3$ транзитивно дејствује на $\{1, 2, 3\}$ (кратко: G_f је транзитивна подгрупа од $\mathbb{S}_3$) и $3 \mid |G_f|$. Дакле, једине могућности за G_f су $\mathbb{A}_3$ и $\mathbb{S}_3$, при чему знамо да је $G_f = \mathbb{A}_3$ **акко** је $D(f)$ потпун квадрат у K.

Пример 47 Нека је $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$. Одредити G_f.

Јасно је да је f нерастављив пошто је $f(1) = f(-1) = 1 \neq 0$. Израчунајмо дискриминанту: $D(f) = -4(-3)^3 - 27(1)^2 = 81 = 9^2$. Следи да је $G_f = \mathbb{A}_3 \cong \mathbb{C}_3$. ♣

Пример 48 Нека је $f = X^3 + 3X + 1 \in \mathbb{Q}[X]$. Одредити G_f.

И овај полином је нерастављив, а $D(f) = -135$. Како $D(f)$ није потпун квадрат у $\mathbb{Q}$ закључујемо да је $G_f = \mathbb{S}_3$. ♣