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.

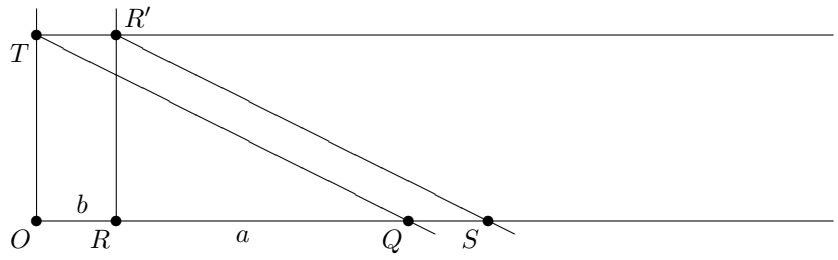
Тачке у равни можемо да видимо и као комплексне бројеве на стандардан начин.

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 $a \neq 0$.

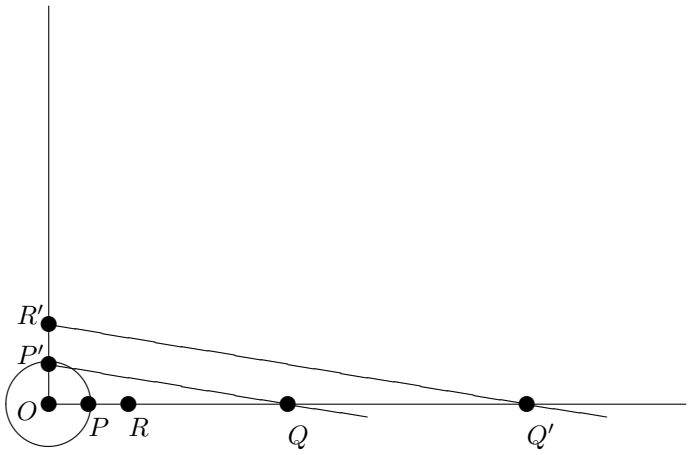
Није тешко уверити се да је довољно ово показати када имамо позитивне реалне бројеве (негативни бројеви само уводе више случајева). Конструкција броја $a + b$ дата је следећим цртежом.



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).



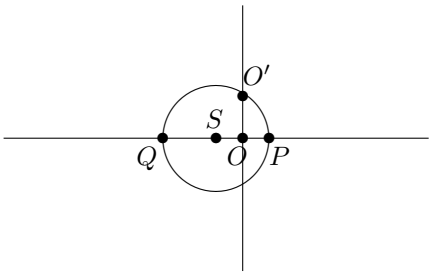
Постављамо кругове са центром у O који пролазе кроз тачке P (која одговара броју 1) и тачку R (која одговара броју b). У пресеку добијамо тачке P' и R' на вертикалној оси. Права кроз R' паралелна правој кроз тачке P' и Q сече хоризонталну осу у тачки Q' и та тачка одговара тачки $a \cdot b$. Наиме, правоугли 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 $p = \mu_{\alpha_1} \cdots \mu_{\alpha_n}$. □

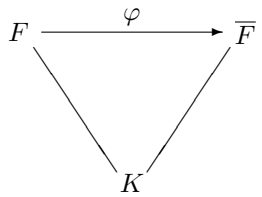
Дефиниција 22 Ако је L раширење поља K, онда је НОРМАЛНО ЗАТВОРЕЊЕ поља L најмање раширење $\overline{L}$ поља L тако да је раширење $\overline{L}/K$ нормално.

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,

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

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

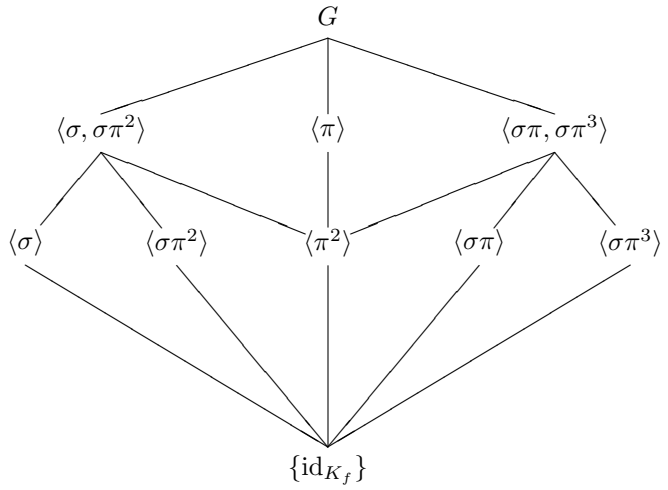
$$\pi^4(\sqrt[4]{2}) = \pi(-i\sqrt[4]{2}) = -\pi(i)\pi(\sqrt[4]{2}) = -i \cdot i\sqrt[4]{2} = \sqrt[4]{2}.$$

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

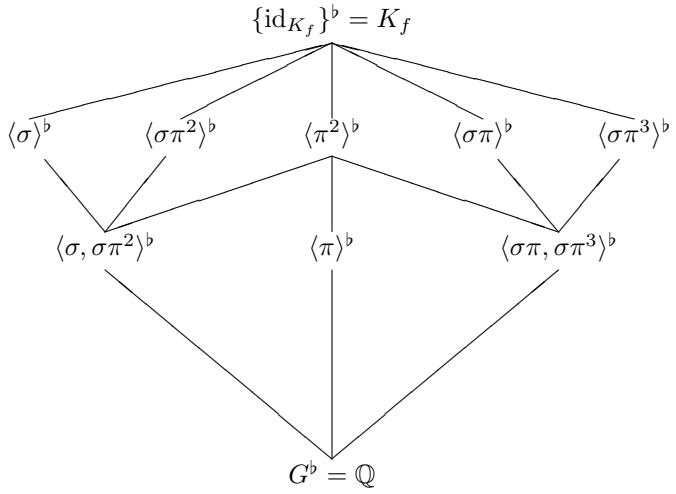
$$i \overset{\pi}{\longmapsto} i \overset{\sigma}{\longmapsto} -i, \quad \sqrt[4]{2} \overset{\pi}{\longmapsto} i\sqrt[4]{2} \overset{\sigma}{\longmapsto} -i\sqrt[4]{2},$$

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

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:

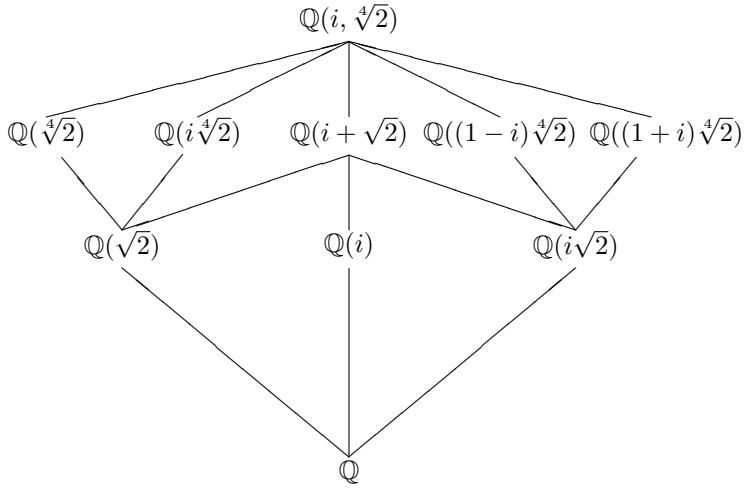
$$\langle \sigma\pi^2 \rangle^\flat = \mathbb{Q}(x_2) = \mathbb{Q}(i\sqrt[4]{2}).$$

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:

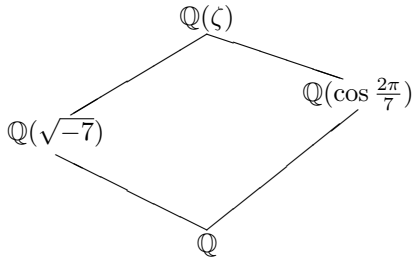
$$a = a - d, \quad b = e - d, \quad c = b - d, \quad d = f - d, \quad e = c - d, \quad f = -d.$$

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 $\sigma^k\tau^2\sigma^{-k}$.

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

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

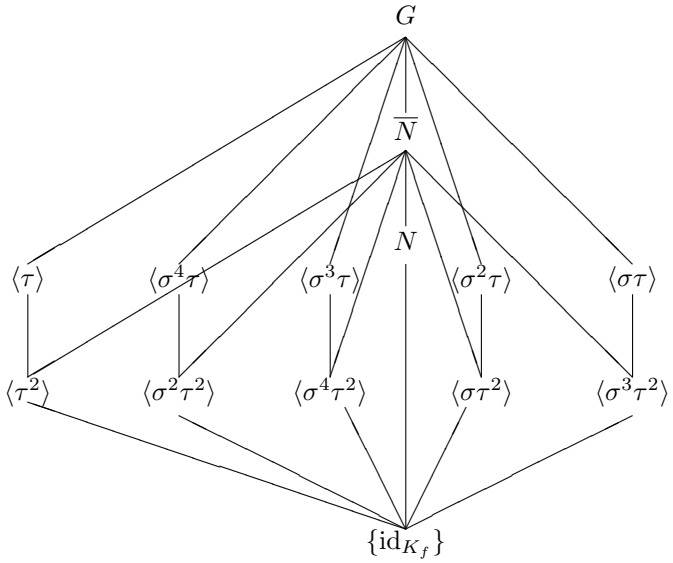
$$\sigma^3\tau^2\sigma^{-3} = (\sigma^3\tau\sigma^{-3})^2 = (\sigma^2\tau)^2 = \sigma^2\tau\sigma^2\tau = \sigma^2\sigma^4\tau\tau = \sigma\tau^2;$$

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

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

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

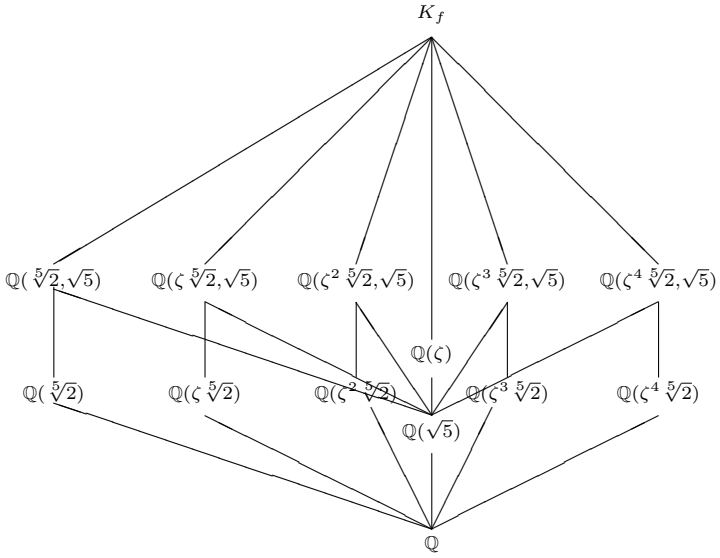
Одавде је $\xi \in \{\frac{-1\pm\sqrt{5}}{2}\}$. Дакле, $\overline{N}^\flat = \mathbb{Q}(\xi) = \mathbb{Q}(\sqrt{5})$.

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 $G_f = \mathbb{S}_3$. ♣

8.2 Полиноми степена 4

Нека је f сепарабилан полином степена 4. Тада је $G_f \leq \mathbb{S}_4$. Са V означимо (Клајнову) подгрупу: $V = \{(1), (12)(34), (13)(24), (14)(23)\}$. Она је нормална подгрупа од $\mathbb{S}_4$, те је $G_f \cap V \triangleleft G_f$. Нека су корени од f: $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Тада је у $K_f[X]$: $f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4)$. Посматрајмо елементе $\alpha, \beta, \gamma \in K_f$ задате са:

$$\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4, \quad \beta = \alpha_1\alpha_3 + \alpha_2\alpha_4, \quad \gamma = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

Јасно је да подгрупа V мотивише разматрање ових елемената. Ови су елементи различити. На пример: $\alpha - \beta = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3) \neq 0$. Како је $\mathbb{S}_4 \cong \mathbb{S}_{\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}}$ можемо сматрати да $\mathbb{S}_4$ дејствује на скупу свих корена, а тиме и на скупу $\{\alpha, \beta, \gamma\}$. Приметимо да је то дејство транзитивно:

$$(13) \cdot \alpha = \alpha_3\alpha_2 + \alpha_1\alpha_4 = \gamma, \quad (14) \cdot \alpha = \alpha_4\alpha_2 + \alpha_3\alpha_1 = \beta.$$

Због тога су подгрупе $\Sigma_\alpha, \Sigma_\beta, \Sigma_\gamma$ реда 8 и све су конјуговане међусобно, као стабилизатори елемената из исте орбите (оне су конјуговане и као Силовљеве 2-подгрупе од $\mathbb{S}_4$).

Покажимо да је Σ_α изоморфна са $\mathbb{D}_4$. Приметимо да $(12), (1324) \in \Sigma_\alpha$. Наиме,

$$(12) \cdot \alpha = \alpha_2\alpha_1 + \alpha_3\alpha_4 = \alpha, \quad (1324) \cdot \alpha = \alpha_3\alpha_4 + \alpha_2\alpha_1 = \alpha.$$

Но,

$$(12)(1324) = (13)(24), (1324)^3(12) = (1423)(12) = (13)(24),$$

те можемо да закључимо да је $\Sigma_\alpha = \langle (12), (1324) \rangle \cong \mathbb{D}_4$. Подгрупа V је као 2-подгрупа садржана у некој Силовљевој 2-подгрупи, али како је она и нормална, она је садржана у свакој Силовљевој 2-подгрупи, тј. $V \subseteq \Sigma_\alpha \cap \Sigma_\beta \cap \Sigma_\gamma$. Но, како је $|V| = 4$, а $|\Sigma_\alpha| = |\Sigma_\beta| = |\Sigma_\gamma| = 8$, то мора заправо бити $V = \Sigma_\alpha \cap \Sigma_\beta \cap \Sigma_\gamma$. Приметимо да је

$$\Phi^{-1}\left[\Sigma_\alpha \cap \Sigma_\beta \cap \Sigma_\gamma\right] = \Phi^{-1}\left[\operatorname{Im}\Phi \cap \Sigma_\alpha \cap \Sigma_\beta \cap \Sigma_\gamma\right] = \Phi^{-1}\left[G_f \cap V\right]$$

заправо подгрупа, која фиксира потпоље $K(\alpha, \beta, \gamma)$ (подсетимо се да смо са Φ означили утапање групе $G(K_f/K)$ у $\mathbb{S}_n$), тј. $\Phi^{-1}\left[\Sigma_\alpha \cap \Sigma_\beta \cap \Sigma_\gamma\right] = K(\alpha, \beta, \gamma)^\sharp$. Стога нам ова анализа практично доказује следећу лему.

Лема 49 $\left(\Phi^{-1}\left[G_f \cap V\right]\right)^\flat = K(\alpha, \beta, \gamma)$. Раширење $K(\alpha, \beta, \gamma)/K$ је Галоаово и $G(K(\alpha, \beta, \gamma)/K) \cong G_f/_{G_f \cap V}$.

Доказ. При Галоаовој кореспонденцији потпољу $K(\alpha, \beta, \gamma)$ одговара подгрупа $\Phi^{-1}\left[G_f \cap V\right]$, $G(K_f/K(\alpha, \beta, \gamma)) \cong G_f \cap V$, а, како је $G_f \cap V \triangleleft G_f$, то је и раширење $K(\alpha, \beta, \gamma)/K$ Галоаово са Галоаовом групом $G(K(\alpha, \beta, \gamma)/K) \cong G_f/_{G_f \cap V}$. □

Посматрајмо сада поље $M = K(\alpha, \beta, \gamma)$ и полином

$$g(X) = (X - \alpha)(X - \beta)(X - \gamma) \in M[X].$$

Но, за свако $\sigma \in G(K_f/K)$ је $\sigma[\{\alpha, \beta, \gamma\}] = \{\alpha, \beta, \gamma\}$, па је

$$\widetilde{\sigma}(g(X)) = (X - \sigma(\alpha))(X - \sigma(\beta))(X - \sigma(\gamma)) = g(X).$$

Стога је заправо $g(X) \in K[X]$, а $M = K_g$. Овај полином $g(X)$ зове се и РАЗРЕШАВАЈУЋА КУБИКА за полином f.

Лема 50 Разрешавајућа кубика за $f = X^4 + bX^3 + cX^2 + dX + e$ је $g = X^3 - cX^2 + (bd - 4e)X - b^2e + 4ce - d^2$. При томе је $D(f) = D(g)$.

Доказ. Пре свега,

$$\begin{aligned} f &= (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4) \\ &= X^4 - (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)X^3 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4)X^2 \\ &\qquad - (\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4)X + \alpha_1\alpha_2\alpha_3\alpha_4, \end{aligned}$$

те је

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = -b, \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 = c \\ \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4 = -d, \alpha_1\alpha_2\alpha_3\alpha_4 = e. \end{aligned}$$

Имамо и

$$g = (X-\alpha)(X-\beta)(X-\gamma) = X^3 - (\alpha+\beta+\gamma)X^2 + (\alpha\beta+\alpha\gamma+\beta\gamma)X - \alpha\beta\gamma.$$

Подсетимо се да је

$$\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4, \quad \beta = \alpha_1\alpha_3 + \alpha_2\alpha_4, \quad \gamma = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

Дакле,

$$\alpha + \beta + \gamma = \alpha_1\alpha_2 + \alpha_3\alpha_4 + \alpha_1\alpha_3 + \alpha_2\alpha_4 + \alpha_1\alpha_4 + \alpha_2\alpha_3 = c.$$

$$\begin{aligned} \alpha\beta+\alpha\gamma+\beta\gamma &= (\alpha_1\alpha_2+\alpha_3\alpha_4)(\alpha_1\alpha_3+\alpha_2\alpha_4)+(\alpha_1\alpha_2+\alpha_3\alpha_4)(\alpha_1\alpha_4+\alpha_2\alpha_3)+(\alpha_1\alpha_3+\alpha_2\alpha_4)(\alpha_1\alpha_4+\alpha_2\alpha_3) \\ &= \alpha_1^2\alpha_2\alpha_3+\alpha_1\alpha_2^2\alpha_4+\alpha_1\alpha_3^2\alpha_4+\alpha_2\alpha_3\alpha_4^2+\alpha_1^2\alpha_2\alpha_4+\alpha_1\alpha_2^2\alpha_3+\alpha_1\alpha_3\alpha_4^2+\alpha_2\alpha_3^2\alpha_4 \\ &\qquad +\alpha_1^2\alpha_3\alpha_4+\alpha_1\alpha_2\alpha_3^2+\alpha_1\alpha_2\alpha_4^2+\alpha_2^2\alpha_3\alpha_4 \\ &= \alpha_1\alpha_2\alpha_3(\alpha_1+\alpha_2+\alpha_3)+\alpha_1\alpha_2\alpha_4(\alpha_1+\alpha_2+\alpha_4)+\alpha_1\alpha_3\alpha_4(\alpha_1+\alpha_3+\alpha_4)+\alpha_2\alpha_3\alpha_4(\alpha_2+\alpha_3+\alpha_4) \\ &= \alpha_1\alpha_2\alpha_3(-b-\alpha_4)+\alpha_1\alpha_2\alpha_4(-b-\alpha_3)+\alpha_1\alpha_3\alpha_4(-b-\alpha_2)+\alpha_2\alpha_3\alpha_4(-b-\alpha_1) \\ &= (-b)(\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\alpha_1\alpha_3\alpha_4+\alpha_2\alpha_3\alpha_4)-4\alpha_1\alpha_2\alpha_3\alpha_4 = (-b)(-d)-4e = bd-4e. \end{aligned}$$

$$\alpha\beta\gamma=(\alpha_1\alpha_2+\alpha_3\alpha_4)(\alpha_1\alpha_3+\alpha_2\alpha_4)(\alpha_1\alpha_4+\alpha_2\alpha_3)=(\alpha_1^2\alpha_2\alpha_3+\alpha_1\alpha_2^2\alpha_4+\alpha_1\alpha_3^2\alpha_4+\alpha_2\alpha_3\alpha_4^2)(\alpha_1\alpha_4+\alpha_2\alpha_3)$$
$$=\alpha_1^3\alpha_2\alpha_3\alpha_4+\alpha_1^2\alpha_2^2\alpha_3^2+\alpha_1^2\alpha_2^2\alpha_4^2+\alpha_1\alpha_2^3\alpha_3\alpha_4+\alpha_1^2\alpha_3^2\alpha_4^2+\alpha_1\alpha_2\alpha_3^3\alpha_4+\alpha_1\alpha_2\alpha_3\alpha_4^3+\alpha_2^2\alpha_3^2\alpha_4^2$$
$$=\alpha_1\alpha_2\alpha_3\alpha_4(\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_4^2)+\alpha_1^2\alpha_2^2\alpha_3^2+\alpha_1^2\alpha_2^2\alpha_4^2+\alpha_1^2\alpha_3^2\alpha_4^2+\alpha_2^2\alpha_3^2\alpha_4^2$$
$$=e((\alpha_1+\alpha_2+\alpha_3+\alpha_4)^2-2(\alpha_1\alpha_2+\cdots+\alpha_3\alpha_4))+(\alpha_1\alpha_2\alpha_3+\cdots+\alpha_2\alpha_3\alpha_4)^2-2(\alpha_1^2\alpha_2^2\alpha_3\alpha_4+\cdots+\alpha_1\alpha_2\alpha_3^2\alpha_4^2)$$
$$=e((-b)^2-2c)+(-d)^2-2\alpha_1\alpha_2\alpha_3\alpha_4(\alpha_1\alpha_2+\cdots+\alpha_3\alpha_4)=eb^2-2ce+d^2-2ec=b^2e+d^2-4ce.$$

Дакле, $g = X^3 - cX^2 + (bd - 4e)X - b^2e + 4ce - d^2$.

Провера $D(g) = D(f)$ није толико сложена:

$$D(g)=(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$$
$$=((\alpha_1\alpha_2+\alpha_3\alpha_4-\alpha_1\alpha_3-\alpha_2\alpha_4)(\alpha_1\alpha_2+\alpha_3\alpha_4-\alpha_1\alpha_4-\alpha_2\alpha_3)(\alpha_1\alpha_3+\alpha_2\alpha_4-\alpha_1\alpha_4-\alpha_2\alpha_3))^2$$
$$=((\alpha_1(\alpha_2-\alpha_3)-\alpha_4(\alpha_2-\alpha_3))(\alpha_1(\alpha_2-\alpha_4)-\alpha_3(\alpha_2-\alpha_4))(\alpha_1(\alpha_3-\alpha_4)-\alpha_2(\alpha_3-\alpha_4)))^2$$
$$=((\alpha_1-\alpha_4)(\alpha_2-\alpha_3)(\alpha_1-\alpha_3)(\alpha_2-\alpha_4)(\alpha_1-\alpha_2)(\alpha_3-\alpha_4))^2=D(f).$$

Наведимо једну кратку таблицу.

G_f	$V \cap G_f$	$G(K_g/K) \cong G_f/_{G_f \cap V}$
$\mathbb{S}_4$	V	$\mathbb{S}_3$
$\mathbb{A}_4$	V	$\mathbb{C}_3$
V	V	$\{1\}$
$\mathbb{D}_4$	V	$\mathbb{C}_2$
$\mathbb{C}_4$	$\mathbb{C}_2$	$\mathbb{C}_2$

Овде је коришћен и резултат да је $\mathbb{S}_4/V \cong \mathbb{S}_3$.

Пример 51 Нека је $f = X^4 - 4X + 2 \in \mathbb{Q}[X]$. Одредити G_f.

Овај је полином нерастављив по Ајзенштајновом критеријуму – посматрамо прост број $p = 2$. Његова разрешавајућа кубика је $g = X^3 - 8X - 16 \in \mathbb{Q}[X]$. Овај полином је нерастављив над $\mathbb{Q}$. У ту сврху, довољно је проверити да нема нулу облика $\pm 2^k$ за $0 \leq k \leq 4$. Но, лакше је приметити следеће. Ако је g растављив над $\mathbb{Q}$, растављив је и над $\mathbb{Z}$, па тиме и над свим пољима $\mathbb{Z}_p$, где је p прост број.

Поље $\mathbb{Z}_2$ није од користи пошто се добија растављив полином X^3, као ни поље $\mathbb{Z}_3$ пошто полином $X^3 + X + 2 \in \mathbb{Z}_3[X]$ има нулу у $\mathbb{Z}_3$: $2^3 + 2 + 2 = 0$. Но, за $p = 5$ добијамо полином $X^3 + 2X + 4$ који јесте нерастављив над $\mathbb{Z}_5$ пошто ту нема нулу (а то је свакако лакше проверити него за почетни полином). Дискриминанта кубике $g \in \mathbb{Q}[X]$ је $D(g) = (-4)(-8)^3 - 27(-16)^2 = 2^{11} - 27 \cdot 2^8 = 2^8 \cdot (8 - 27) < 0$ што није квадрат у $\mathbb{Q}$. Стога следи да је $G(K_g/K) \cong \mathbb{S}_3$, те је (видети таблицу) $G_f = \mathbb{S}_4$. ♣

Пример 52 Нека је $f = X^4 + 4X^2 + 2 \in \mathbb{Q}[X]$. Одредити G_f.

Најпре можемо да констатујемо да је f нерастављив над $\mathbb{Q}$ по Ајзенштајновом критеријуму — посматра се наравно прост број $p = 2$. Разрешавајућа кубика је $g = X^3 - 4X^2 - 8X + 32$. Но, овај полином јесте растављив над $\mathbb{Q}$: $g(X) = X^2(X-4) - 8(X-4) = (X^2-8)(X-4)$. Заправо даљим растављањем добијамо да је $g(X) = (X - 2\sqrt{2})(X + 2\sqrt{2})(X-4)$ па је његово коренско поље $K_g = \mathbb{Q}(\sqrt{2})$. Дакле, $G(K_g/\mathbb{Q}) \cong \mathbb{C}_2$. Да бисмо одредили да ли је $G_f = \mathbb{D}_4$ или $G_f = \mathbb{C}_4$, испитајмо да ли је f нерастављив као полином из $\mathbb{Q}(\sqrt{2})[X]$. Наиме, према ставу **46** полином је нерастављив **акко** Галоаова група дејствује транзитивно на коренима. С обзиром на чињеницу да група реда 2 не може транзитивно да дејствује на скупу од 4 елемента, нерастављивост ће нам у потпуности разрешити дилему (ради се о групи $V \cap G_f$ – погледајте таблицу и доказ леме **49**). Но,

$$f = X^4 + 4X^2 + 2 = (X^2+2)^2 - 2 = (X^2 + 2 - \sqrt{2})(X^2 + 2 + \sqrt{2}).$$

Како је полином растављив, добијамо да је $G_f = \mathbb{C}_4$. ♣

Пример 53 Нека је $f = X^4 - 10X^2 + 4 \in \mathbb{Q}[X]$. Одредити G_f.

Да бисмо утврдили да ли је f нерастављив над $\mathbb{Q}$ овај пут поступимо директно. Најпре се можемо уверити да нема нула у $\mathbb{Z}$ (а нуле у $\mathbb{Q}$ би морале заправо бити у $\mathbb{Z}$) пошто редукција по модулу 3 даје полином $X^4 - X^2 + 1 \in \mathbb{Z}_3[X]$, а он нема нула у $\mathbb{Z}_3$ што се лако провери. Остаје да се види да ли је f растављив над $\mathbb{Q}$ у облику производа два квадратна тринома. Претпоставимо да је то тако, тј. да постоје $a, b, c, d \in \mathbb{Q}$ тако да је

$$X^4 - 10X^2 + 4 = (X^2 + aX + b)(X^2 + cX + d).$$

Стога мора бити

$$a + c = 0, \quad b + ac + d = -10, \quad ad + bc = 0, \quad bd = 4.$$

Дакле, $c = -a$ и

$$b - a^2 + d = -10, \quad a(d-b) = 0, \quad bd = 4.$$

1) $a = 0$. Тада је $b + d = -10$, $bd = 4$. Ако ставимо да је

$$b = -5 + t, d = -5 - t,$$

добијамо да је

$$25 - t^2 = 4,$$

те је $t^2 = 21$, а свакако тада t не може бити рационалан број: t би био корен полинома $X^2 - 21 \in \mathbb{Q}[X]$, а према добро познатом резултату тада мора заправо бити цео број који је делилац од 10.

2) $a \neq 0$. Тада је $b = d$ и $2b - a^2 = -10$, $b^2 = 4$. Добијамо да је $b = \pm 2$. Дакле, $a^2 \in \{6, 14\}$ и опет a не може бити рационалан број.

Дакле, заиста је f нерастављив над $\mathbb{Q}$. Разрешавајућа кубика за f је $g = X^3 + 10X^2 - 16X - 160$, но имамо да је

$$g = X^2(X+10) - 16(X+10) = (X^2-16)(X+10) = (X-4)(X+4)(X+10),$$

те је $K_g = \mathbb{Q}$ и из табеле видимо да је $G_f = V$. ♣

Пример 54 Нека је $f = X^4 - 2 \in \mathbb{Q}[X]$. Одредити G_f.

Полином је наравно нерастављив над $\mathbb{Q}$ на основу Ајзенштајновог критеријума. Разрешавајућа кубика је

$$g = X^3 + 8X = X(X^2+8) = X(X - 2\sqrt{-2})(X + 2\sqrt{-2}),$$

па је $K_g = \mathbb{Q}(\sqrt{-2})$. Треба још проверити да ли је f нерастављив над $\mathbb{Q}(\sqrt{-2})$. Знамо корене од f и они нису у $\mathbb{Q}(\sqrt{-2})$. Проверимо да ли постоји растав на производ квадратних тринома. Како недостаје члан уз X^3 такав растав би био облика (погледајте и претходни пример):

$$X^4 - 2 = (X^2 + aX + b)(X^2 - aX + d),$$

где су $a, b, d \in \mathbb{Q}(\sqrt{-2})$. Добијамо:

$$b - a^2 + d = 0, \quad a(d-b) = 0, \quad bd = -2.$$

$a = 0$. Тада је $b + d = 0$, $bd = -2$, што нам даје $b^2 = 2$, те је $b = \pm\sqrt{2}$. Но, $\sqrt{2} \notin \mathbb{Q}(\sqrt{-2})$. Ово се може проверити директно, или се може констатовати да би из $\sqrt{2} \in \mathbb{Q}(\sqrt{-2})$ следило и да $i \in \mathbb{Q}(\sqrt{-2})$ те би имали да је $[\mathbb{Q}(\sqrt{-2}) : \mathbb{Q}] = 4$, што није тачно.

$a \neq 0$. Добијамо да је $b = d = \pm\sqrt{-2}$. Дакле, $a^2 = 2b = \pm 2\sqrt{-2}$. Но, $a \in \mathbb{Q}(\sqrt{-2})$, па је $a = p + q\sqrt{-2}$, за неке $p, q \in \mathbb{Q}$. Тада је $a^2 = p^2 - 2q^2 + 2pq\sqrt{-2}$ и из $a^2 = \pm 2\sqrt{-2}$ бисмо добили да је $p^2 - 2q^2 = 0$, тј. да је $\sqrt{2}$ рационалан број.

Дакле, f је нерастављив над $\mathbb{Q}(\sqrt{-2})$, те је стога $G_f = \mathbb{D}_4$. ♣

Напомена 55 Сваки полином f из $\mathbb{Q}[X]$ облика $f = X^4 + pX^2 + qX + d$ има такву факторизацију $f = (X^2+aX+b)(X^2-aX+d)$, за неке $a, b, d \in \mathbb{C}$ (на овоме је базиран Декартов метод за решавање једначина четвртог степена), овде је поента да тражимо факторизацију у неком конкретном потпољу од $\mathbb{C}$. ♠

8.3 Случај када је $G_f = \mathbb{S}_p$

Подсетимо се најпре корисне формуле о пермутацијама. Ако је $\pi \in \mathbb{S}_n$ и $(a_1 \dots a_k)$ један k-цикл у $\mathbb{S}_n$, онда је $\pi(a_1 \dots a_k)\pi^{-1} = (\pi(a_1) \dots \pi(a_k))$.

Лема 56 Нека је p прост број. Тада је група $\mathbb{S}_p$ генерисана двочланим скупом који чине ма која транспозиција и ма који p-цикл.

Доказ. Нека је τ нека транспозиција и σ један p-цикл. Знамо да траспозиције $(12), (13), \ldots, (1p)$ генеришу $\mathbb{S}_p$. Наравно, и транспозиције (ks), за $s \neq k$ такође генеришу $\mathbb{S}_p$ за ма које k.

Нека је $\tau = (kl)$, а $\sigma = (ki_2 \ldots i_p)$. Јасно је да је $\sigma^r(k) = l$ за неки r, тако да имамо и цикл $\sigma_0 = (klj_3 \ldots j_p)$ (приметимо да је σ^r увек p-цикл за $p \nmid r$ пошто је p прост број). Добијамо:

$$\sigma_0\tau\sigma_0^{-1} = (lj_3), \quad \sigma_0^2\tau\sigma_0^{-2} = (j_3j_4) \quad , \ldots, \quad \sigma_0^{p-2}\tau\sigma_0^{2-p} = (j_{p-1}j_p).$$

Но, имамо да је

$$\tau(lj_3)\tau^{-1}{=}(kj_3),(kj_3)(j_3j_4)(kj_3)^{-1}{=}(kj_4),\ldots,(kj_{p-1})(j_{p-1}j_p)(kj_{p-1})^{-1}{=}(kj_p).$$

Дакле, у групи генерисаној елементима τ и σ су све транспозиције (ks) за $s \neq k$ и како оне генеришу $\mathbb{S}_p$, то и τ и σ генеришу $\mathbb{S}_p$. □

Став 57 Нека је $f \in \mathbb{Q}[X]$ нерастављив полином степена p, где је p прост број. Ако f у $\mathbb{C}$ има тачно два корена који нису реални бројеви, онда је $G_f = \mathbb{S}_p$.

Доказ. Нека је α корен полинома f. Ако је K_f коренско поље овог полинома, онда је $\alpha \in K_f$ и $\mathbb{Q}(\alpha) \subseteq K_f$. Како је f нерастављив, то је $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$ те $p \mid [K_f : \mathbb{Q}]$. Но, $[K_f : \mathbb{Q}] = G(K_f/\mathbb{Q}) \cong G_f$, те $p \mid |G_f|$, те у G_f постоји елемент реда p на основу Кошијеве теореме. Како је $G_f \leq \mathbb{S}_p$ и p прост број, тај елемент мора бити неки p-цикл.

Нека су β и $\overline{\beta}$ ти једини конјуговано комплексни корени од f. Нека је $\tau(z) = \overline{z}$. Тада је $\tau(\beta) = \overline{\beta}$, $\tau(\overline{\beta}) = \beta$, а $\tau(\gamma) = \gamma$ за све остале корене γ полинома f. Тако добијамо да је $\tau \in G(K_f/\mathbb{Q})$ и да τ одговара једној транспозицији из $\mathbb{S}_p$. На основу леме **56** закључујемо да је $G_f = \mathbb{S}_p$. □

Пример 58 Нека је $p > 2$ прост број. Одредити G_f, где је $f = X^5 - p^2X - p$.

Приметимо најпре да је овај полином нерастављив по Ајзенштајновом критеријуму. Одредимо колико он има реалних нула.

У ту сврху, може се посматрати одговарајућа полиномска функција $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^5 - p^2x - p$ и одредити број њених реалних нула. Ово је задатак из Анализе 1. Урадите то за вежбу. Алтернативно, ми ћемо искористити Декартово правило знака да бисмо одредили број реалних нула.

Ако је $f = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{R}[X]$, при чему је $a_0 \neq 0$, онда је број позитивних корена полинома f једнак броју $z - 2k$, где је са z означен број ПРОМЕНА ЗНАКОВА у низу коефицијената овог полинома почев од a_n па до a_0 при чему се коефицијенти једнаки 0 не узимају у обзир, а k је неки природан број.

Ово ће бити јасно чим применимо на наш случај. Наиме, овде је низ коефицијената који нису једнаки 0: $1, -p^2, -p$, па је низ знакова:

$+,-,-$. Видимо да имамо само једну промену знака, те овај полином има један позитиван реални корен.

За одређивање броја негативних нула посматрамо $f(-X)$. Наиме, број негативних корена полинома $f(X)$, једнак је броју позитивних корена полинома $f(-X)$. У нашем случају имамо да је $f(-X) = -X^5 + p^2X - p$. Овде су коефицијенти: $-1, p^2, -p$ а знаци: $-,+,-$. Дакле, овај полином има или два негативна корена или ниједан (ово је наравно мана овог метода). Дакле, само треба да проверимо да ли полином има неки негативан корен. Што није тешко видети, пошто је $f(-1) = -1 + p^2 - p > 0$, а $f(0) = -p < 0$. Дакле, како он има негативних корена, закључујемо да их има два и укупно има три реална корена. На основу става **57**, добијамо да је $G_f = \mathbb{S}_5$. ♣

Пример 59 Нека је $p > 2$ прост број. Одредити G_f, где је

$$f = (X^2 + 4m)(X-2)(X-4)\cdots(X-2(p-2)) - 2,$$

а m веома велики природан број.

Приметимо најпре да је број линеарних фактора у овом производу једнак $p-2$, тако да је $\deg f = p$. Полином је нерастављив по Ајзенштајновом критеријуму за прост број 2. Наиме, редукцијом по модулу 2 добијамо полином X^p што значи да су сви коефицијенти, сем водећег. дељиви са 2. Треба само установити да слободни члан није дељив са 4. Но, слободни члан је једнак $f(0) = 4m \cdot (-2)^{p-2}(p-2)! - 2$, те је $f(0) \equiv -2 \pmod 4$, те није дељив са 4.

Остаје да се види колико има реалних нула. Немогуће је не приметити да је $f(2) = f(4) = \cdots = f(2(p-2)) = -2$. Дакле, овде имамо негативне вредности полинома у $p-2$ тачке. Потражимо позитивне вредности. Природно је гледати тачке између ових, а имамо целобројне тачке $3, 5, \ldots, 2p-5$. Но, $f(3) > 0$, $f(5) < 0$, $f(7) > 0$, итд. Наиме,

$$\begin{aligned} f(3) &= (9+4m)\cdot 1\cdot(-1)\cdots(-1-2(p-2)) - 2 \\ &= (9+4m)\cdot(-1)^{p-3}(2p-3)!! - 2 = (9+4m)(2p-3)!! - 2 > 0. \end{aligned}$$

С друге стране,

$$\begin{aligned} f(5) &= (25+4m)\cdot 3\cdot 1\cdot(-1)\cdot(-3)\cdots(5-2(p-2)) - 2 \\ &= (25+4m)\cdot 3\cdot(-1)^{p-4}(2p-9)!! - 2 = -(25+4m)\cdot 3\cdot(2p-9)!! - 2 < 0. \end{aligned}$$

Није много ни важно који се тачно бројеви ту добијају, битно је да када имамо 3, 7, 11, ... добијамо позитивне бројеве, а за 5, 9, 13, ... негативне, јер сваки следећи има један негативан фактор мање од претходног.

Да резимирамо. Имамо да је

$$f(2) < 0, f(3) > 0, f(6) < 0, f(7) > 0, \ldots, f(2(p-2)) < 0), f(2p-3) > 0.$$

То значи да имамо један корен између 2 и 3, између 3 и 6, између 6 и 7, итд. Ово је боље организовати овако: у интервалу $(2, 6)$ два корена, у интервалу $(6, 10)$ два корена, $\ldots$, у интервалу $(2(p-4), 2(p-2))$ два корена и један корен у интервалу $(2(p-2), +\infty)$. У интервалу $(-\infty, 2)$ нема корена. У крајњим тачкама одговарајућих одсечака смо констатовали да су вредности -2. Број интервала у којима имамо два корена једнак је $(p-3)/2$. Наиме, то су интервали облика $(2+4k, 6+4k)$, где је $k = \overline{0, (p-5)/2}$. Дакле, ту имамо укупно $p-3$ корена. И додајмо још један корен у интервалу $(2(p-2), +\infty)$ што нам даје укупно $p-2$.

Покажимо да су преостала два корена конјуговано-комплексна. Нека су сви корени $\alpha_1, \ldots, \alpha_p$, а та додатна два су прва два, тј. α_1, α_2. Вијетове формуле нам дају:

$$\sum_{i=1}^{p} \alpha_i = \sum_{k=1}^{p-2} 2k, \qquad \sum_{1 \leq i < j \leq p} \alpha_i \alpha_j = 4 \sum_{1 \leq k < l \leq p-2} kl + 4m.$$

Дакле,

$$\sum_{i=1}^{p} \alpha_i^2 = \left(\sum_{i=1}^{p} \alpha_i \right)^2 - 2 \sum_{1 \leq i < j \leq p} \alpha_i \alpha_j = 2^2 + 4^2 + \cdots + (2(p-2))^2 - 8m.$$

Уколико је m довољно велики број, добијамо да је сума квадрата корена негативан број, па не могу сви бити реални. Стога су ти додатни корени конјуговано-комплексни и на основу става **57** добијамо да је $G_f = \mathbb{S}_p$. ♣

9 Циклотомична раширења

Овај одељак почињемо једном дефиницијом.

Дефиниција 60 Нека је K поље. Примитивни n-ти корен из јединице је елемент реда n у мултипликативној групи $K^\times (= K \setminus \{0\})$.

Наравно, за произвољно поље и произвољно n, примитивни n-ти корен из јединице не мора постојати. На пример, у пољу $\mathbb{F}_9$ не постоји примитивни трећи корен из јединице. Наиме, $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$, где је $\alpha \in F_9$ корен неког нерастављивог полинома из $\mathbb{F}_3[X]$ степена 2. Један такав је полином $a = X^2 + 1$ — лако је проверити да он нема корен у $\mathbb{F}_3$, па је нерастављив. Уколико би у $\mathbb{F}_9$ постојао примитивни трећи корен из јединице, онда би постојали $a, b \in \mathbb{F}_3$ такви да је $(a + b\alpha)^3 = 1$. Но, како је карактеристика овог поља 3 и како $a, b \in \mathbb{F}_3$ то је $(a + b\alpha)^3 =$

$a^3+b^3\alpha^3 = a-b\alpha$, јер је $\alpha^2 = -1$. Но, из $a-b\alpha = 1$ следи да је $a = 1, b = 0$, те је $a+b\alpha = 1$, а то је неутрал, а не елемент реда 3 у $U(\mathbb{F}_9)$. Наравно, могли смо да ово констатујемо и тако што бисмо приметили да је $U(\mathbb{F}_9)$ група реда 8 и онда сигурно не садржи елемент реда 3, али није лоше видети и мало рачунице у $\mathbb{F}_9$ ☺.

Следећа теорема разматра један важан случај, када такав корен постоји.

Теорема 61 Нека је K поље карактеристике 0, или карактеристике p, где $p \nmid n$, а L коренско поље полинома $X^n - 1 \in K[X]$.

а) Постоји примитивни n-ти корен из јединице у L.

б) Ако је ζ примитивни n-ти корен из јединице у L, онда је $L = K(\zeta)$.

в) L је Галоаово над K и постоји мономорфизам $G(L/K) \to U(\mathbb{Z}_n)$, те је $G(L/K)$ Абелова група.

а) Нека је $f = X^n - 1$. Како је $f'(X) = nX^{n-1} \neq 0$, на основу услова за карактеристику поља K, то је 0 једини корен од f', што свакако није корен од f, те је f сепарабилан. Стога је L/K Галоаово раширење. Нека је $E = \{\alpha \in L : \alpha^n = 1\}$. Дакле, E се састоји од корена полинома f у L, а како је он сепарабилан, то је $|E| = n$. Приметимо да је $(E, \cdot)$ подгрупа групе $(K^\times, \cdot)$. Како знамо да је свака коначна подгрупа мултипликативне групе поља нужно циклична, то је E циклична група реда n. Сваки њен генератор је стога примитивни n-ти корен из јединице, тако да их L заиста садржи.

б) Нека је $\zeta \in L$ ма који од примитивних корена из јединице. Тада је $E = \{\zeta^k : 0 \leqslant k < n\}$. Како је L коренско поље полинома f, а сви корени тог полинома су степени од ζ, то је свакако $L = K(\zeta)$.

в) Већ смо констатовали да је раширење L/K Галоаово. Посматрајмо групу $G = G(L/K) = G(K(\zeta)/K)$, где је ζ неки од примитивних корена из јединице. Сваки елемент $\sigma \in G$ потпуно је одређен вредношћу у ζ. Но, како је σ и изоморфизам групе $L^\times$, то је $\omega(\zeta) = \omega(\sigma(\zeta))$, где смо са $\omega(x)$ означили ред елемента x у групи $L^\times$. Но, $\sigma(\zeta) = \zeta^i$, за неко $1 \leqslant i \leqslant n-1$, а $\omega(\zeta^i) = n$ **акко** је $\mathrm{NZD}(i, n) = 1$. Знамо и да је $U(\mathbb{Z}_n) = \Phi(n)(= \{k : 1 \leqslant k < n, \mathrm{NZD}(k, n) = 1\})$. Стога имамо пресликавање $\Psi\colon G \to U(\mathbb{Z}_n)$ дефинисано са:

$$\Psi(\sigma) = i \overset{\text{def}}{\iff} \sigma(\zeta) = \zeta^i.$$

Уверимо се да је Ψ мономорфизам. Нека су $\sigma, \tau \in G$ и нека је $\sigma(\zeta) = i$, $\sigma(\tau) = j$. Тада је

$$(\sigma \circ \tau)(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^j) = (\sigma(\zeta))^j = (\zeta^i)^j = \zeta^{i \cdot j} = \zeta^{i \cdot_n j}.$$

Последња једнакост је тачна, јер је $\zeta^n = 1$. Стога је

$$\Psi(\sigma \circ \tau) = i \cdot_n j = \Psi(\sigma) \cdot_n \Psi(\tau),$$

те је Ψ заиста хомоморфизам група. Но, јасно је да је Ψ мономорфизам: ако је $\Psi(\sigma) = 1$, онда је $\sigma(\zeta) = \zeta^1 = \zeta$, па је $\sigma = \mathrm{id}_L$. □

Напомена 62 а) Ψ не мора бити „на". На пример, ако је $K = \mathbb{C}$, онда је $L = K$, без обзира на $n > 1$ и слика је тривијална подгрупа. Слично, ако је $K = \mathbb{R}$ и $n > 1$, онда је $L = \mathbb{C}$ и слика је подгрупа реда 2. Но, ако је $K = \mathbb{Q}$, $n = p$, где је p прост број, онда смо раније видели да је $[L : K] = p - 1$ и добијамо изоморфизам. Видећемо да је ово тачно за све n ако је $K = \mathbb{Q}$.

б) Ако је $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ факторизација на просте бројеве, онда је

$$U(\mathbb{Z}_n) \cong U(\mathbb{Z}_{p_1^{\alpha_1}}) \times \cdots \times U(\mathbb{Z}_{p_k^{\alpha_k}}).$$

Осим тога, $U(\mathbb{Z}_p) \cong \mathbb{C}_{p-1}$, а за $\alpha > 1$:

$$U(\mathbb{Z}_{p^\alpha}) \cong \begin{cases} \mathbb{C}_{p^{\alpha-1}(p-1)}, & p \text{ непаран прост број}, \\ \mathbb{C}_2 \times C_{2^{\alpha-2}}, p = 2, \alpha \geqslant 3, \\ \mathbb{C}_2, & p = 2, \alpha = 2. \end{cases}$$

Доказ, ко жели, може погледати у књизи *Алгебра за информатичаре*. ♠

Раширења $K(\zeta)$ описана претходном теоремом зовемо и ЦИКЛОТОМИЧНИМ РАШИРЕЊИМА, јер су у случају $K = \mathbb{Q}$ у вези са поделом круга на n једнаких делова.

Фокусирајмо се сада на случај $K = \mathbb{Q}$. Имамо да је

$$X^n - 1 = \prod_{\zeta^n = 1} (X - \zeta).$$

Сваки ζ који се појављује у овом производу је елемент цикличне групе $\mathbb{C}_n$ и има свој ред. Ако скупимо заједно елементе реда n (примитивне n-те корене из јединице) добијамо ЦИКЛОТОМИЧНИ ПОЛИНОМ Φ_n:

$$\Phi_n(X) = \prod_{\omega(\zeta) = n} (X - \zeta).$$

Ако се заједно скупе елементи реда d, за све d који деле n, добијамо

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X). \tag{24}$$

Како знамо да је број елемената реда n у цикличној групи са n елемената једнак $\varphi(n)$, имамо да је $\deg \Phi_n(X) = \varphi(n)$. С обзиром да

сваки $\mathbb{Q}$-аутоморфизам циклотомичног раширења чува ред сваког елемента из групе $\mathbb{Q}(\zeta)^\times$, он пермутује n-те корене из јединице, те је стога $\Phi_n(X) \in \mathbb{Q}[X]$. Но, из **(24)** следи да су заправо сви ови полиноми из $\mathbb{Z}[X]$. Погледајмо пар примера.

$$\Phi_1(X) = X - 1,$$
$$\Phi_2(X) = X + 1,$$
$$\Phi_3(X) = \left(X - \left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)\right)\left(X - \left(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}\right)\right) = X^2 + X + 1,$$
$$\Phi_4(X) = (X - i)(X + i) = X^2 + 1.$$

Ови полиноми се заправо добијају на једноставан рекурентни начин:

$$\Phi_n(X) = \frac{X^n - 1}{\prod\limits_{d|n, d\neq n} \Phi_d(X)}.$$

Дакле,

$$\Phi_5(X) = \frac{X^5 - 1}{X - 1} = X^4 + X^3 + X^2 + X + 1,$$
$$\Phi_6(X) = \frac{X^6 - 1}{\Phi_1(X)\Phi_2(X)\Phi_3(X)} = \frac{X^6 - 1}{(X-1)(X+1)(X^2+X+1)} = X^2 - X + 1,$$
$$\Phi_7(X) = \frac{X^7 - 1}{X - 1} = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1,$$
$$\Phi_8(X) = \frac{X^8 - 1}{\Phi_1(X)\Phi_2(X)\Phi_4(X)} = \frac{X^8 - 1}{(X-1)(X+1)(X^2+1)} = X^4 + 1,$$
$$\Phi_9(X) = \frac{X^9 - 1}{\Phi_1(X)\Phi_3(X)} = \frac{X^9 - 1}{(X-1)(X^2+X+1)} = X^6 + X^3 + 1,$$
$$\begin{aligned}\Phi_{10}(X) &= \frac{X^{10} - 1}{\Phi_1(X)\Phi_2(X)\Phi_5(X)} = \frac{X^{10} - 1}{(X-1)(X+1)(X^4+X^3+X^2+X+1)} \\ &= X^4 - X^3 + X^2 - X + 1.\end{aligned}$$

Наравно, могу се ове рачунице скратити како се примећују додатне правилности. На пример, јасно је да је $\Phi_p(X) = X^{p-1} + \cdots + X + 1$, ако је p прост број. Наведимо још нека својства.

1. Ако је p прост број и $r \geqslant 1$, онда је:

$$\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}}). \tag{25}$$

Ово се лако показује. Најпре, приметимо да је

$$\Phi_p(X^{p^{r-1}}) = \frac{\left(X^{p^{r-1}}\right)^p - 1}{X^{p^{r-1}} - 1} = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1}. \tag{26}$$

Но,

$$X^{p^{r-1}} - 1 = \prod_{0 \leqslant k \leqslant r-1} \Phi_{p^k}(X), \tag{27}$$

јер су $1, p, \ldots, p^{r-1}$ једини делитељи од p^r. Такође је

$$X^{p^r} - 1 = \prod_{0 \leqslant k \leqslant r} \Phi_{p^k}(X), \tag{28}$$

Но, из **(27)** и **(28)** директно следи **(25)**. ♠

2. Ако је $n > 1$ непаран број, онда је

$$\Phi_{2n}(X) = \Phi_n(-X). \tag{29}$$

Приметимо да важи једноставна чињеница: ако је $\{\zeta_1, \ldots, \zeta_{\varphi(n)}\}$ скуп свих примитивних n-тих корена из јединице, онда је $\{-\zeta_1, \ldots, -\zeta_{\varphi(n)}\}$ скуп свих примитивних $2n$-тих корена из јединице. Пре свега, како је n непаран, имамо да је $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$ и $\varphi(n)$ је паран број. Како -1 и ζ_i комутирају и имају узајамно просте редове, то је ред њиховог производа производ њихових редова, те је $\omega(-\zeta_i) = 2n$ и $-\zeta_i$ је примитиван $2n$-ти корен из јединице. Узимајући ово у обзир имамо да је

$$\begin{aligned}\Phi_n(-X) &= \prod_{\omega(\zeta)=n} (-X - \zeta) = (-1)^{\varphi(n)} \prod_{\omega(\zeta)=n} (X + \zeta) \\ &= \prod_{\omega(\zeta)=n} (X - (-\zeta)) = \prod_{\omega(\eta)=2n} (X - \eta) = \Phi_{2n}(X). \quad ♠\end{aligned}$$

3. Ако је p прост број такав да $p \nmid n$, онда је

$$\Phi_{pn}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}.$$

Кажу да не треба мењати победнички тим, па ћемо и овде користити сличну идеју као и у претходном својству. Наиме, нека је η примитивни p-ти корен из јединице. Но, тада су сви примитивни (pn)-ти корени из јединице облика $\eta^k\zeta_i$, за $1 \leqslant k \leqslant p-1$, $1 \leqslant i \leq \varphi(n)$, где су ζ_i, за $1 \leqslant i \leq \varphi(n)$ сви примитивни n-ти корени из јединице. Наиме, $\omega(\eta^k) = p$ за све наведене k, а такође је и $\omega(\eta^k\zeta_i) = pn$ из истих разлога као и горе. А број примитивних (pn)-тих корена из јединице је $\varphi(pn) = \varphi(p)\varphi(n) = (p-1)\varphi(n)$, те су заиста сви у наведеном списку. Корисно је приметити и следеће: $\omega(\zeta_i^p) = n$. Наравно, за $i \neq j$ је $\zeta_i^p \neq \zeta_j^p$. Наиме, како $p \nmid n$, постоје $a, b \in \mathbb{Z}$ такви да је $pa + nb = 1$. Стога би из једнакости $\zeta_i^p = \zeta_j^p$ следило:

$$\zeta_i = \zeta_i^1 = \zeta_i^{pa+nb} = (\zeta_i^p)^a(\zeta_i^n)^b = (\zeta_i^p)^a = (\zeta_j^p)^a = (\zeta_j^p)^a(\zeta_j^n)^b = \zeta_j^{pa+nb} = \zeta_j^1 = \zeta_j.$$

Дакле, и скуп $\{\zeta_1^p, \ldots, \zeta_{\varphi(n)}^p\}$ јесте скуп свих примитивних n-тих корена из јединице. Имајући то у виду, имамо да је

$$\Phi_n(X^p) = \prod_{\omega(\zeta)=n} (X^p - \zeta^p).$$

Но,

$$X^p - \zeta^p = \prod_{k=0}^{p-1} (X - \eta^k \zeta).$$

Дакле, добили смо

$$\Phi_n(X^p) = \prod_{\omega(\zeta)=n} \prod_{k=0}^{p-1} (X - \eta^k \zeta). \tag{30}$$

Но,

$$\Phi_{pn}(X) = \prod_{\omega(\zeta)=n} \prod_{k=1}^{p-1} (X - \eta^k \zeta). \tag{31}$$

Обратите пажњу на малу, али битну разлику, између производа у **(30)** и **(31)** — у другом производу k иде од 1, а у првом од 0. Како је $\Phi_n(X) = \prod_{\omega(\zeta)=n}(X - \zeta)$ важи једнакост:

$$\Phi_n(X^p) = \Phi_n(X)\Phi_{pn}(X),$$

из које следи тражено. ♠

4. Ако $p \mid n$, онда је $\Phi_{pn}(X) = \Phi_n(X^p)$.

И овде ћемо искористити сличну идеју као пре. Наиме, покажимо да, ако је $\{\zeta_1, \ldots, \zeta_{\varphi(n)}\}$ скуп свих примитивних n-тих корена из јединице и ако су, за $i = \overline{1, \varphi(n)}$, $\zeta_{i1}, \ldots, \zeta_{ip}$ p-ти корени елемента ζ_i, онда је $\{\zeta_{11}, \ldots, \zeta_{1p}, \ldots, \zeta_{\varphi(n)1}, \ldots, \zeta_{\varphi(n)p}\}$ скуп свих примитивних (pn)-тих корена из јединице. Наравно, како је $\zeta_{ij}^{pn} = (\zeta_{ij}^p)^n = \zeta_i^n = 1$, ово су свакако (pn)-ти корени из јединице. Треба проверити да ли су ово примитивни корени из јединице. То је вежбица из Алгебре 1. Наиме, претпоставимо да у некој групи имамо елемент x који је реда n, при чему $p \mid n$ и елемент y такав да је $y^p = x$. Треба одредити ред елемента y. Ако је $\omega(y) = m$, онда имамо да је $\omega(y^p) = m/\mathrm{NZD}(m, p)$, тј. да је $n = m/\mathrm{NZD}(m, p)$. Уколико $p \nmid m$, онда је $n = m$, но ту имамо контрадикцију, јер $p \mid n$. Стога $p \mid m$, те је $n = m/p$, односно $m = np$. Наравно да се ово може и другачије доказати. Дакле, наведени елементи су заиста примитивни (pn)-ти корени из јединице. Како $p \mid n$, имамо да је $\varphi(pn) = p\varphi(n)$ (покажите да је то тачно). Стога тај скуп заиста садржи све примитивне (pn)-те корене из јединице. Важи следеће:

$$X^p - \zeta_i = \prod_{j=1}^{p} (X - \zeta_{ij}),$$

пошто су ζ_{ij}, $j=\overline{1,p}$, сви корени полинома $X^p-\zeta_i$. Сада радимо као и пре.

$$\Phi_n(X^p)=\prod_{i=1}^{\varphi(n)}(X^p-\zeta_i)=\prod_{i=1}^{\varphi(n)}\prod_{j=1}^{p}(X-\zeta_{ij})=\prod_{\omega(\xi)=pn}(X-\xi)=\Phi_{np}(X).$$

Пошто се аутор ових редова већ уморио од силног куцања (видети лекције из Историје и филозофије математике — део посвећен Декарту), читаоцима се за вежбу остављају још два својства.

5. Ако је $n=p_1^{r_1}\cdots p_k^{r_k}$ факторизација n у производ простих бројева, показати да је

$$\Phi_n(X)=\Phi_{p_1\cdots p_k}(X^{p_1^{r_1-1}\cdots p_k^{r_k-1}}).$$

6.

$$\Phi_n(X)=\prod_{d|n}(X^{n/d}-1)^{\mu(d)},$$

где је μ Мебијусова функција дефинисана са:

$$\mu(n)=\begin{cases}0, & \text{ако је } n \text{ дељив квадратом неког простог броја}\\ (-1)^k, & \text{ако је } n \text{ производ } k \text{ различитих простих бројева}\\ 1, & \text{ако је } n=1.\end{cases}$$

Осим овога, као лакшу вежбу би било добро да читаоци одреде још циклотомичних полинома нижег степена користећи доказана својства. Гледајући те примере, може се констатовати да су сви коефицијенти ових полинома једнаки или -1, или 0, или 1. То није увек тачно. Но, први полином који има коефицијент различит од ових је полином Φ_{105}. Приметимо да је 105 најмањи број који је производ три непарна проста броја.

$$\begin{aligned}\Phi_{105}(X)&=X^{48}+X^{47}+X^{46}-X^{43}-X^{42}-2X^{41}-X^{40}-X^{39}+X^{36}+X^{35}\\&+X^{34}+X^{33}+X^{32}+X^{31}-X^{28}-X^{26}-X^{24}-X^{22}-X^{20}+X^{17}+X^{16}\\&+X^{15}+X^{14}+X^{13}+X^{12}-X^9-X^8-2X^7-X^6-X^5+X^2+X+1.\end{aligned}$$

Веома је мистериозно понашање тих коефицијената и њихова величина је доста истраживана, али то наравно превазилази теме које ми обрађујемо.

Вратимо се сада ономе што смо најавили — разматрању циклотомичног полинома над пољем $\mathbb{Q}$.

Теорема 63 а) $\Phi_n(X)$ је нерастављив над $\mathbb{Q}$.

б) Ако је $\zeta\in\mathbb{C}$ било који примитивни n-ти корен из јединице, онда је $[\mathbb{Q}(\zeta):\mathbb{Q}]=\varphi(n)$.

в) Ако је ζ као у делу под б), онда је $G(\mathbb{Q}(\zeta)/\mathbb{Q})\cong U(\mathbb{Z}_n)$.

Доказ. а) Нека је ζ примитивни корен из јединице и $f(X) \in \mathbb{Q}[X]$ његов минимални полином. Како је $\Phi_n(\zeta) = 0$, то $f(X) \mid \Phi_n(X)$ и пошто је $\Phi_n(X)$ моничан полином у $\mathbb{Z}[X]$, а и $f(X)$ је моничан, онда је $\Phi_n(X) = f(X)g(X)$, где $f(X), g(X) \in \mathbb{Z}[X]$. Да бисмо доказали нерастављивост полинома $\Phi_n(X)$ доказаћемо да је $\Phi_n(X) = f(X)$.

Претпоставимо да је $\deg g(X) > 0$. Покажимо да је за свако i које је узајамно просто са n: $f(\zeta^i) = 0$. Ако ово докажемо показаћемо да су сви примитивни n-ти корени из јединице корени полинома $f(X)$, па мора бити $f(X) = \Phi_n(X)$. За ово је довољно доказати да ако је $f(\eta) = 0$ за неки примитивни n-ти корен из јединице η, онда је $f(\eta^p) = 0$ за сваки прост број p такав да $p \nmid n$. Наиме, сваки i који је узајамно прост са n је производ таквих простих бројева, а ако је η примитивни n-ти корен из јединице, онда је и η^p, за такво p, такође примитивни n-ти корен из јединице.

Претпоставимо да ово није тачно, тј. нека постоји неки прост p, и примитивни n-ти корен из јединице η такав да $p \nmid n$, да је $f(\eta) = 0$ и да је $f(\eta^p) \neq 0$. Но, како су сви примитивни n-ти корени из јединице корени полинома $\Phi_n(X)$, то мора бити: $0 = \Phi_n(\eta^p) = f(\eta^p)g(\eta^p)$. Добијамо да је $g(\eta^p) = 0$. Посматрајмо полиноме $f(X), g(X^p) \in \mathbb{Z}[X]$. Они имају заједнички корен η, па је $\mathrm{NZD}(f(X), g(X^p)) \neq 1$. Посматрајмо сада све по модулу p, и нека су $\overline{f(X)}, \overline{g(X^p)} \in \mathbb{F}_p[X]$ одговарајуће редукције. Дакле, у $\mathbb{F}_p$ имамо да је $\mathrm{NZD}(\overline{f(X)}, \overline{g(X^p)}) \neq 1$. Но, у $\mathbb{F}_p[X]$ је $\overline{g(X^p)} = \overline{g(X)}^p$. Како је $\mathbb{F}_p[X]$ прстен са једнозначном факторизацијом, из $\mathrm{NZD}(\overline{f(X)}, \overline{g(X)}^p) \neq 1$, следи да је $\mathrm{NZD}(\overline{f(X)}, \overline{g(X)}) \neq 1$. Но, тада из факторизације

$$\overline{\Phi_n(X)} = \overline{f(X)} \cdot \overline{g(X)}$$

следи да $\overline{\Phi_n(X)} \in \mathbb{F}_p[X]$ има двоструку нулу у свом коренском пољу ($\overline{f(X)}$ и $\overline{g(X)}$ имају ту заједничку нулу). Но, то није могуће, јер полином $\overline{\Phi_n(X)}$ дели полином $X^n - 1$ у $\mathbb{F}_p[X]$, а $(X^n - 1)' = \overline{n}X^{n-1} \neq 0$, пошто $p \nmid n$, па полином $X^n - 1$ нема двоструку нулу нигде, јер је једина нула његовог извода једнака 0, а то свакако није нула самог полинома. Стога ни његов делилац $\overline{\Phi_n(X)}$ не може имати двоструку нулу. Ова контрадикција нам завршава доказ.

Тврђења под б) и в) непосредно следе. Наиме, како је $\Phi_n(X)$ нерастављив, он је минимални полином за сваки примитивни n-ти корен из јединице ζ, те је стога $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \Phi_n(X) = \varphi(n)$. Знамо да постоји мономорфизам групе $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ у групу $U(\mathbb{Z}_n)$, но како у овом случају групе имају исти број елемената ($\varphi(n)$) онда је овде у питању један изоморфизам. □

10 Завршетак приче о конструктибилности

Доказали смо: ако је α конструктибилан број, онда је $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^s$ за неки природан број s. Видели смо да обрат у општем случају не важи, али ипак важи став.

Став 64 Ако је L потпоље од $\mathbb{C}$ такво да је $L/\mathbb{Q}$ Галоаово раширење степена 2^r за неко r и $\alpha \in L$, онда је α конструктибилан.

Доказ. Дакле, $|G| = |G(L/\mathbb{Q})| = 2^r$. Знамо да је свака p-група, за прост број p, решива, па је и G решива. Стога постоји низ подгрупа

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} \rhd G_r = \{\mathrm{id}_L\},$$

за које је $G_i/G_{i+1} \cong \mathbb{C}_2$, за $i = \overline{0, r-1}$, односно низ потпоља

$$\mathbb{Q} = L_0 \subset L_1 \subset \cdots \subset L_{r-1} \subset L_r = L,$$

за које је $[L_{i+1} : L_i] = 2$ за $i = \overline{0, r-1}$. Стога је $L_{i+1} = L_i(\alpha_i)$ за неко α_i које задовољава квадратну једначину $\alpha_i^2 + p_i\alpha_i + q_i = 0$. Но, знамо како се решава квадратна једнначина, па је $L_{i+1} = L_i(\sqrt{\beta_i})$ за неко $\beta_i \in L_i$. Стога је сваки елемент из L конструктибилан. □

Сада можемо и да коначно заокружимо причу о конструкцији правилног n-тоугла.

Теорема 65 Правилни n-тоугао је могуће конструисати ако и само ако је $n = 2^k p_1 \cdots p_s$, за неко $k \geqslant 0$, где су p_i различити Фермаови прости бројеви.

Доказ. Правилни n-тоугао је могуће конструисати акко је могуће конструисати примитивни n-ти корен из јединице $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Знамо да је раширење $\mathbb{Q}(\zeta)/\mathbb{Q}$ Галоаово и за конструкцију је потребно и довољно да је степен овог раширења степен броја 2, тј. да је број $\varphi(n)$ степен двојке. Нека је $n = 2^k p_1^{r_1} \cdots p_l^{r_s}$ факторизација броја n. Тада је

$$\varphi(n) = \varphi(2^k p_1^{r_1} \cdots p_l^{r_l}) = 2^{k-1} p_1^{r_1-1}(p_1 - 1) \cdots p_l^{r_l-1}(p_s - 1)$$

(наравно, у случају да је $k = 0$, првог фактора и нема). Да би ово био степен двојке, видимо да мора бити $r_1 = \cdots = r_s = 1$ и морају сви бројеви $p_i - 1$ бити степени броја 2. Но, ако је $p_i = 2^t + 1$ прост број, онда мора бити и $t = 2^u$ за неко $u \geqslant 0$, као што смо видели раније. Дакле, сви непарни прости бројеви који се појављују у факторизацији броја n морају имати изложилац 1 и морају бити Фермаови прости бројеви, а то се и тражило. □

11 Решивост у радикалима

11.1 Решивост у радикалима и решиве групе

Следећи став нам описује циклична раширења поља K. Видећемо да су то раширења која се добијају додавањем n-тог корена неког елемента из тог поља. Наводимо га без доказа.

Став 66 Нека је K поље које садржи примитивни n-ти корен из јединице, $L = K(\alpha)$, где је α такво да $\alpha^n \in K$, а $\alpha^s \notin K$ за $1 \leqslant s < n$. Тада је L Галоаво раширење од K са цикличном Галоаовом групом реда n.

Обратно, ако је L циклично раширење од K степена n, онда је $L = K(\alpha)$ за неко α такво да $\alpha^n \in K$, а $\alpha^s \notin K$ за $1 \leqslant s < n$.

Најпре основна дефиниција.

Дефиниција 67 Нека је K поље и $f \in K[X] \setminus \{0\}$. Кажемо да је једначина

$$f(x) = 0$$

РЕШИВА У РАДИКАЛИМА уколико се њена решења могу добити операцијама сабирања, одузимања, множења, дељења и налажења n-тих корена (за разне n). Прецизније, ако постоји растући низ поља

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m,$$

тако да:

1. $K_i = K_{i-1}(\alpha_i)$ при чему $\alpha_i^{r_i} \in K_{i-1}$ за неко r_i;

2. K_m садржи коренско поље K_f полинома f.

За раширења K_i/K кажемо и да су радикалска раширење од K пошто се добијају поновљеним додавањем корена (радикала).

Можемо да приметимо сличност са појмом конструктибилности елемената; за конструктибилност полазимо од $\mathbb{Q}$ и додајемо квадратне корене.

Теорема 68 (Галоа, 1831) Нека је K поље карактеристике 0, $f \in K[X]$. Тада је једначина $f(x) = 0$ решива у радикалима **акко** је група $G(K_f/K)$ решива.

Да бисмо се припремили за доказ ове теореме, доказујемо пар резултата.

Лема 69 Нека је K поље, $f \in K[X]$ сепарабилан полином степена n и $\widetilde{K}$ раширење поља K. Полином f можемо посматрати и као полином из $\widetilde{K}[X]$; означимо га тада са $\widetilde{f}$. Тада је група $G(K_{\widetilde{f}}/\widetilde{K})$ изоморфна подгрупи групе $G(K_f/K)$.

Доказ. Наравно, са $K_{\widetilde{f}}$ смо означили коренско поље полинома $\widetilde{f}$. Нека су $\alpha_1, \ldots, \alpha_n$ корени полинома $\widetilde{f}$ у $K_{\widetilde{f}}$. Дакле $K_{\widetilde{f}} = \widetilde{K}(\alpha_1, \ldots, \alpha_n)$. Можда су неки од тих корена у $\widetilde{K}$, али то не мења ништа. Тада је $K_f = K(\alpha_1, \ldots, \alpha_n)$. За свако $\sigma \in G(K_{\widetilde{f}}/\widetilde{K})$, $\sigma(\alpha_i) \in \{\alpha_1, \ldots, \alpha_n\}$, те $\sigma[K_f] \subseteq K_f$. Како је σ потпуно одређено вредностима у α_i, то сужење σ на K_f задаје мономорфизам $G(K_{\widetilde{f}}/\widetilde{K})$ у $G(K_f/K)$. □

Наравно, са ζ_n означавамо примитивни n-ти корен из јединице.

Лема 70 Нека је p прост број. Тада је $G(\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}(\zeta_{p-1})) \cong G(\mathbb{Q}(\zeta_p)/\mathbb{Q})$.

Доказ. Нека је $\sigma \in G(\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}(\zeta_{p-1}))$. Јасно је да је свакако $\sigma(\zeta_p) = \zeta_p^k$ за неко $1 \leqslant k \leqslant p-1$. То значи да је $\sigma[\mathbb{Q}(\zeta_p)] \subseteq \mathbb{Q}(\zeta_p)$, те можемо дефинисити сужење овог аутоморфизма $\underline{\sigma} \in G(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Дакле, имамо хомоморфизам $\sigma \mapsto \underline{\sigma}$. Но, како је σ потпуно одређено са $\sigma(\zeta)$ и како је ова вредност произвољан (примитивни) p-ти корен из јединице, то је овај хомоморфизам заправо изоморфизам. □

Теорема 71 За свако $n \geqslant 2$, једначина $x^n = 1$ је решива у радикалима.

Доказ. Доказ се наравно изводи индукцијом по n. База индукције је јасна ☺. Приметимо да је довољно показати да је сваки примитивни n-ти корен изразив у радикалима, пошто су остали корени његови степени.

Претпоставимо да су сви примитивни корени ζ_k за $k < n$ изразиви у радикалима и посматрајмо ζ_n. Разликујемо три случаја.

1. $n = p^s$, за неки прост број p и $s > 1$. По индуктивној хипотези је $\zeta_{p^{s-1}}$ изразив у радикалима, а $\zeta_{p^s} = \sqrt[p]{\zeta_{p^{s-1}}}$ (наравно, узимамо неки од p-тих корена, свеједно је који).

2. $n = ab$, где су $a, b > 1$ узајамно прости. По индуктивној хипотези су ζ_a и ζ_b изразиви у радикалима, а имамо да је $\zeta_n = \zeta_a \zeta_b$ (која се теорема из Алгебре 1 користи да би се доказало да је $\omega(\zeta_a \zeta_b) = n$?).

3. $n = p$, где је p прост број. Посматрамо раширење $\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}$. По леми **70** имамо да је раширење $\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}(\zeta_{p-1})$ циклично (подсетимо се да је $G(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{C}_{p-1}$) реда $p-1$. Како $\mathbb{Q}(\zeta_{p-1})$ садржи примитивни $(p-1)$-ви корен из јединице, на основу става **66** имамо да се $\mathbb{Q}(\zeta_p, \zeta_{p-1})$ добија додавањем неког $(p-1)$-вог корена елемента из $\mathbb{Q}(\zeta_{p-1})$. По индуктивној хипотези је $\mathbb{Q}(\zeta_{p-1})/\mathbb{Q}$ радикалско раширење, па тако добијамо да је и $\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}$ радикалско. □

Подсетимо се да је свака подгрупа решиве групе такође решива, као и да је свака количничка група решиве групе решива.

Пређимо сада на...

Доказ теореме 68.

$\Longleftarrow$: Претпоставимо да f има решиву Галоаову групу $G_f = G(K_f/K)$. Проширимо K свим потребним коренима из јединице. То можемо извести додавањем примитивног n-тог корена из јединице за n довољно велико. Узмимо да је $n = (\deg f)!$. Посматрајмо раширење $\widetilde{K} = K(\zeta_n)$. На основу леме **69** имамо да је $G_{\widetilde{f}}$ изоморфна подгрупи од G_f. Дакле, $G_{\widetilde{f}}$ је такође решива. То значи да постоји низ подгрупа

$$G_{\widetilde{f}} = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_{m-1} \rhd G_m = \{\mathrm{id}_{\widetilde{K}_f}\}$$

тако да је $G_i \lhd G_{i-1}$ и G_{i-1}/G_i је циклична. Нека је $L = K_{\widetilde{f}}$ и $K_i = G_i^\flat$. Тада имамо низ поља

$$K \subset K(\zeta_n) = \widetilde{K} = K_0 \subset K_1 \subset \cdots \subset K_{m-1} \subset K_m = L$$

при чему је K_i циклично раширење од K_{i-1}. На основу става **66**, имамо да је $K_i = K_{i-1}(\alpha_i)$, при чему $\alpha_i^{[K_i:K_{i-1}]} \in K_{i-1}$. На основу теореме **71** је раширење $K(\zeta_n)/K(\zeta)$ радикалско (ми смо радили над $\mathbb{Q}$, али то не мења ствар, додатне елементе из K и не користимо да бисмо корене јединице представили у радикалима). Дакле, добили смо да је раширење K_m/K радикалско, те је једначина $f(x) = 0$ решива у радикалима.

$\Longrightarrow$: Довољно је показати да је G_f количничка група неке решиве групе. Знамо да постоји низ поља

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m,$$

тако да је $K_i = K_{i-1}(\alpha_i)$, где $\alpha_i^{r_i} \in K_{i-1}$ и да K_m садржи коренско поље K_f од f. Нека је $n = r_1 r_2 \cdots r_m$ и $\gamma \in K_m$ такво да је $K_m = K(\gamma)$. Ако је $\mu_\gamma \in K[X]$ минимални полином елемента γ, посматрајмо коренско поље K_g полинома $g(X) = \mu_\gamma(X)(X^n - 1)$. Дакле, K_g је раширење поља K које садржи све потребне корене из јединице. Нека је $G = G(K_g/K) = \{\sigma_1, \sigma_2, \ldots, \sigma_N\}$, где је $\sigma_1 = \mathrm{id}_K$ и L нормално затворење од $K_m(\zeta)$ у K_g, где је ζ примитивни n-ти корен из јединице. Заправо је

$$L = K(\zeta, \alpha_1, \ldots, \alpha_n, \sigma_2(\alpha_1), \ldots, \sigma_2(\alpha_n), \ldots, \sigma_N(\alpha_1), \ldots, \sigma_N(\alpha_n)).$$

Наиме, уз сваки елемент α_i морамо додати и његове слике при аутоморфизмима из G да би раширење било нормално, јер су и те слике нуле њихових минималних полинома над K. И једино су то нуле тих минималних полинома (имали смо овакве аргументе раније — ако је β_i нека нула минималног полинома μ_{α_i} онда се придруживање $\alpha_i \mapsto \beta_i$ продужава до K-аутоморфизма од K_g, тј. до елемента из G). Додајемо ове елементе један по један да добијемо низ поља

$$K \subseteq K(\zeta) \subseteq K(\zeta, \alpha_1) \subseteq \cdots \subseteq K' \subseteq K'' \subseteq \cdots \subseteq L.$$

Свако следеће поље (K'') добија се од претходног (K') додавањем неког корена, па је свако од тих раширења Абелово (заправо циклично

сем првог). За ово нам је важно да су ту сви потребни корени из јединице (видети став **66**). То значи да су одговарајуће количничке групе $(K')^\sharp/(K'')^\sharp$ Абелове, те је група $G(L/K)$ решива. Но, с обзиром да је K_f садржано у L, група $G_f = G(K_f/K)$ је количничка група решиве групе $G(L/K)$, по Основној теореми коначне теорије Галоа, па је тиме и сама група G_f решива. □

11.2 Симетрични полиноми

Наравно, требало би да нам је познат појам симетричних полинома. Но, за сваки случај...

Дефиниција 72 Нека је R комутативан прстен са јединицом. Полином $p(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$ је симетричан уколико за свако $\sigma \in \mathbb{S}_n$ важи:

$$p(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = p(X_1, \ldots, X_n).$$

Следећи полиноми су од централног значаја; то су такозвани ЕЛЕМЕНТАРНИ симетрични полиноми.

$$\begin{aligned}
e_1 &= \sum_{i=1}^{n} X_i = X_1 + X_2 + \cdots + X_n;\\
e_2 &= \sum_{1\leqslant i<j\leqslant n} X_iX_j = X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n;\\
e_3 &= \sum_{1\leqslant i<j<k\leqslant n} X_iX_jX_k = X_1X_2X_3 + X_1X_2X_4 + \cdots + X_{n-2}X_{n-1}X_n;\\
&\vdots\\
e_n &= X_1X_2\cdots X_n.
\end{aligned}$$

При раду са полиномима са више неодређених корисно је имати поредак међу производима неодређених. Поредак задајемо са:

$$X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n} \succ_{grlex} X_1^{j_1}X_2^{j_2}\cdots X_n^{j_n} \overset{\text{def}}{\Longleftrightarrow} i_1 + i_2 + \cdots + i_n > j_1 + j_2 + \cdots + j_n$$
$$\text{или}$$
$$i_1 + i_2 + \cdots + i_n = j_1 + j_2 + \cdots + j_n$$
$$\text{и } (\exists k)(i_1 = j_1, \ldots, i_{k-1} = j_{k-1}, i_k > j_k).$$

Овде је и $X_1 \succ_{grlex} X_2 \succ_{grlex} \cdots \succ_{grlex} X_n$. Овај поредак се назива СТЕПЕНОВАНИ ЛЕКСИКОГРАФСКИ ПОРЕДАК. Када је задат поредак онда можемо сваки полином p написати тако да производи неодређених у његовим мономима опадају. Моном у коме је највећи производ при овом поретку зове се водећи моном и означава са $LM(p)$, док је коефицијент

уз њега водећи коефицијент и означава се са $LC(p)$. Приметимо да је $LM(e_i) = X_1X_2\cdots X_i$. Овако задат поредак има два важна својства.

1. Ако $\mathbf{X} \mid \mathbf{Y}$ за производе $\mathbf{X}$ и $\mathbf{Y}$, онда је $\mathbf{X} \preceq_{grlex} \mathbf{Y}$.

2. На производима неодређених је ово линеарно уређење.

Посебно се добија да не постоји бесконачан опадајући ланац производа.

Следећа теорема упућује на важност елементарних симетричних полинома.

Теорема 73 За сваки симетричан полином $p(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$ постоји тачно један полином $q(X_1, \ldots, X_n)$ такав да је

$$p(X_1, \ldots, X_n) = q(e_1, \ldots, e_n).$$

Доказ. Одредимо водећи моном за $e_1^{d_1}\cdots e_n^{d_n}$. Он је заправо производ степена водећих монома полинома e_i:

$$LM(e_1^{d_1}e_2^{d_2}\cdots e_n^{d_n}) = X_1^{d_1}(X_1X_2)^{d_2}\cdots(X_1X_2\cdots X_n)^{d_n} = X_1^{d_1+\cdots+d_n}X_2^{d_2+\cdots+d_n}X_n^{d_n}.$$

Доказ егзистенције полинома q. Нека је p симетрични полином и $LM(p) = cX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$. Како је p симетричан он у себи садржи све мономе који се добијају пермутацијом неодређених. Стога мора бити $i_1 \geqslant i_2 \geq \cdots \geqslant i_n$. Наиме, ако се, на пример, моном $cX_1^2X_2^3$ садржи у p, ту мора бити и моном $cX_1^3X_2^2$, добијен од претходног заменом X_1 и X_2. Но, тада је $LM(ce_1^{i_1-i_2}e_2^{i_2-i_3}\cdots e_n^{i_n}) = cX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n} = LM(p)$. Стога је $LM(p - ce_1^{i_1-i_2}e_2^{i_2-i_3}\cdots e_n^{i_n}) < LM(p)$, а $p - ce_1^{i_1-i_2}e_2^{i_2-i_3}\cdots e_n^{i_n}$ је такође симетричан полином. Поступак настављамо док не дођемо до 0 и тако изражавамо p у облику полинома по $e_1, \ldots, e_n$.

Доказ јединствености полинома q. Довољно је показати да из једнакости $q(e_1, e_2, \ldots, e_n) = 0$ у $R[X_1, X_2, \ldots, X_n]$ следи да је q нула полином. Но, $q(e_1, e_2, \ldots, e_n)$ је сума неких монома облика $ce_1^{d_1}e_2^{d_2}\cdots e_n^{d_n}$. Ако је $(d_1, d_2, \ldots, d_n) \neq (d_1', d_2', \ldots, d_n')$, онда је

$$LM(e_1^{d_1}e_2^{d_2}\cdots e_n^{d_n}) \neq LM(e_1^{d_1'}e_2^{d_2'}\cdots e_n^{d_n'}).$$

Наиме, као што смо видели:

$$LM(e_1^{d_1}e_2^{d_2}\cdots e_n^{d_n}) = X_1^{d_1+\cdots+d_n}X_2^{d_2+\cdots+d_n}X_n^{d_n},$$

а

$$LM(e_1^{d_1'}e_2^{d_2'}\cdots e_n^{d_n'}) = X_1^{d_1'+\cdots+d_n'}X_2^{d_2'+\cdots+d_n'}X_n^{d_n'}.$$

Ако би они били једнаки добили бисмо да је

$$d_1 + d_2 + \cdots + d_n = d_1' + d_2' + \cdots + d_n', \quad d_2 + \cdots + d_n = d_2' + \cdots + d_n',$$
$$\ldots, d_{n-1} + d_n = d_{n-1}' + d_n', \quad d_n = d_n'.$$

Но јасно је да из ових једнакости следи да је

$$(d_1, d_2, \ldots, d_n) = (d'_1, d'_2, \ldots, d'_n).$$

Из овога следи да се различити ненула чланови у развоју $q(e_1, e_2, \ldots, e_n)$ никако не могу скратити. Стога, је једнакост $q(e_1, e_2, \ldots, e_n) = 0$ једино могућа ако су сви чланови једнаки 0, тј. сам q је нула полином. □

Пример 74 Изразимо полином $p = X_1^3 + X_2^3 + X_3^3$ преко елементарних симетричних полинома.

Јасно је да је $LP(p) = X_1^3$. Дакле, овде је $(i_1, i_2, i_3) = (3, 0, 0)$ па од p одузимамо e_1^3:

$$\begin{aligned} &p - e_1^3 = X_1^3 + X_2^3 + X_3^3 - (X_1 + X_2 + X_3)^3 \\ &= -3X_1^2X_2 - 3X_1X_2^2 - 3X_1^2X_3 - 3X_1X_3^2 - 3X_2^2X_3 - 3X_2X_3^2 - 6X_1X_2X_3. \end{aligned}$$

Како је $LM(p - e_1^3) = -3X_1^2X_2$, имамо тројку $(2, 1, 0)$, те одузимамо $-3e_1e_2$:

$$\begin{aligned} p - e_1^3 + 3e_1e_2 = &-3X_1^2X_2 - 3X_1X_2^2 - 3X_1^2X_3 - 3X_1X_3^2 - 3X_2^2X_3 - 3X_2X_3^2 - 6X_1X_2X_3 \\ &+3(X_1 + X_2 + X_3)(X_1X_2 + X_1X_3 + X_2X_3) = 3X_1X_2X_3 = 3e_3. \end{aligned}$$

Дакле, $p = e_1^3 - 3e_1e_2 + 3e_3$. ♣

11.3 Симетричне функције и општи полином

Нека је K поље. Група $\mathbb{S}_n$ дејствује на прстену $K[X_1, \ldots, X_n]$ са:

$$\sigma \cdot p(X_1, \ldots, X_n) := p(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Ово се дејство продужава на поље рационалних функције $K(X_1, \ldots, X_n)$ на природан начин.

Теорема 75 Нека је K поље. Тада је $K(X_1, \ldots, X_n)^{\mathbb{S}_n} = K(e_1, \ldots, e_n)$.

Доказ. Знамо из става **73** да је $K[X_1, \ldots, X_n]^{\mathbb{S}_n} = K[e_1, \ldots, e_n]$; наиме, симетрични полином није ништа друго до фиксна тачка при горенаведеном дејству групе $\mathbb{S}_n$. Нека је

$$f(X_1, \ldots, X_n) = \frac{g(X_1, \ldots, X_n)}{h(X_1, \ldots, X_n)} \in K(X_1, \ldots, X_n)^{\mathbb{S}_n},$$

где су $g, h \in K[X_1, \ldots, X_n]$. Из чињенице да је њихов количник симетричан, не следи наравно да су и они симетрични, но то се лако може поправити. Нека је

$$H = \prod_{\sigma \in \mathbb{S}_n} \sigma \cdot h.$$

Јасно је (ово смо имали много пута) да је H симетричан полином, тј. $H \in K[X_1, \ldots, X_n]^{\mathbb{S}_n}$, па је и $Hf \in K[X_1, \ldots, X_n]^{\mathbb{S}_n}$ (Hf је и полином и симетрична функција, јер су и H и f симетричне). Стога је $Hf = a(e_1, \ldots, e_n)$ и $H = b(e_1, \ldots, e_n)$ за неке полиноме a, b те је

$$f = \frac{Hf}{H} = \frac{a(e_1, \ldots, e_n)}{b(e_1, \ldots, e_n)} \in K(e_1, \ldots e_n). \qquad \square$$

Последица 76 Нека је K поље.

1. Раширење $K(X_1, \ldots, X_n)/K(e_1, \ldots, e_n)$ је Галоаово са Галоаовом групом $\mathbb{S}_n$.
2. Базу за $K(X_1, \ldots, X_n)$ као векторски простор над $K(e_1, \ldots, e_n)$ чине производи $X_1^{r_1} \cdots X_n^{r_n}$, при чему је $0 \leqslant r_i \leqslant n - i$ за све $i = \overline{0, n}$.

Доказ. 1. Како је $K(e_1, \ldots, e_n) = K(X_1, \ldots, X_n)^{\mathbb{S}_n}$, из теореме **32** добијамо да је $K(X_1, \ldots, X_n)/K(e_1, \ldots, e_n)$ Галоаово раширење, а из теореме **??** да је Галоаова група баш $\mathbb{S}_n$.

2. Нека је $\widetilde{K} = K(e_1, \ldots, e_n)$ и

$$f(T) = (T - X_1)(T - X_2) \cdots (T - X_n) \in \widetilde{K}[T].$$

Јасно је да су коефицијенти овог полинома у наведеном пољу на основу Вијетових формула. Посматрамо низ раширења:

$$\widetilde{K} \subset \widetilde{K}(X_1) \subset \widetilde{K}(X_1, X_2) \subset \cdots \subset \widetilde{K}(X_1, X_2, \ldots, X_n) = K(X_1, X_2, \ldots, X_n).$$

Како је X_1 нула полинома $f(T)$, то је $[\widetilde{K}(X_1) : \widetilde{K}] \leqslant n$ и $1, X_1, \ldots, X_1^{n-1}$ је једна генератриса за $\widetilde{K}(X_1)$ над $\widetilde{K}$. То је и база уколико је полином $f(T) \in \widetilde{K}[T]$ нерастављив. Како је X_2 нула полинома $f(T)/(T - X_1)$ из $\widetilde{K}(X_1)[T]$, који је степена $n - 1$, то је $[\widetilde{K}(X_1, X_2) : \widetilde{K}(X_1)] \leqslant n - 1$ и генератриса за $\widetilde{K}(X_1, X_2)$ над $\widetilde{K}(X_1)$ је $1, X_2, \ldots, X_2^{n-2}$. Настављајући даље добијамо: $[K(X_1, \ldots, X_n) : K(e_1, \ldots, e_n] \leqslant n(n-1) \cdots 1$ и једну генератрису чине производи $X_1^{r_1} \cdots X_n^{r_n}$, при чему је $r_i \leqslant n - i$ за све i. Но, на основу дела под **1.** имамо да је $[K(X_1, \ldots, X_n) : K(e_1, \ldots, n)] = n!$ и стога горњи производи чине једну базу. $\square$

У овом тренутку корисно је подсетити се да група $\mathbb{S}_n$ није решива за $n \geqslant 5$. То следи из тога што је, за $n \geqslant 5$: $\mathbb{S}_n' = \mathbb{A}_n$, а $\mathbb{A}_n' = \mathbb{A}_n$, где смо са G' означили комутаторску подгрупу $[G, G]$.

Дефиниција 77 Општи полином степена n по T је полином

$$f(T) = T^n - t_1 T^{n-1} + t_2 T^{n-2} - + \cdots + (-1)^n t_n \in K[t_1, \ldots, t_n][T].$$

Наравно, није ово нека посебно дубока дефиниција, то смо имали и у средњој школи када смо разматрали опште квадратне триноме облика ax^n+bx+x, за $a \neq 0$. Уместо a, b, c смо увели неодређене и поставили да је полином моничан, да бисмо сигурно имали полином степена n без додатних услова на неодређене. Знаци су тако одабрани да t_i буду баш симетричне функције корена овог полинома.

Теорема 78 Галоаова група општег полинома изоморфна је са $\mathbb{S}_n$.

Доказ. Посматрамо f као полином са коефицијентима у пољу $\widetilde{K} = K(t_1, \ldots, t_n)$: $f \in \widetilde{K}[T]$. Нека је $K_f = \widetilde{K}(X_1, \ldots, X_n)$ коренско поље овог полинома. Имамо да је

$$f(X) = X^n - t_1X^{n-1} + t_2X^{n-2} - + \cdots + (-1)^n t_n = (X-X_1)(X-X_2)\cdots(X-X_n),$$

те за све $1 \leqslant i \leqslant n$: $t_i = e_i(X_1, \ldots, X_n)$. Тражени резултат следи из последице **76**. □

Како знамо да $\mathbb{S}_n$ није решива за $n \geqslant 5$, то знамо да ако је K поље карактеристике нула, није свака полиномијална једначина степена већег од 4 решива у радикалима, тј. не постоје формуле аналогне формули коју смо у средњој школи учили за квадратну једначину, нити Кардановој формули за једначину трећег степена, као ни формули за једначину четвртог степена (која се своди на једначину трећег). То наравно не значи да ма која једначина степена већег од 4 није решива у радикалима. Већ смо видели неке које то јесу; у наредном одељку бавимо се важним специјалним случајем када једначине степена већег од 4 ЈЕСУ решиве у радикалима.

11.4 Решиве једначине простог реда

До резултата о решивости једначина простог реда, Галоа је дошао 1829. године.

Подсетимо се да смо показали да ако имамо нерастављив и сепарабилан полином, онда Галоаова група тог полинома дејствује транзитивно на његовим коренима. У вези са транзитивним дејством, докажимо следећи став о дејству група.

Став 79 Нека коначна група G транзитивно дејствује на коначном скупу X који има p елемената, где је p прост број. Ако је $H \triangleleft G$ и $X^H \neq X$, онда и H дејствује транзитивно на X.

Доказ. Преставимо X као унију орбита при дејству подгрупе H:

$$X = H \cdot x_1 \sqcup \cdots \sqcup H \cdot x_k. \tag{32}$$

Нека је $i \neq 1$ произвољно. Како G дејствује транзитивно, имамо да је $g \cdot x_1 = x_i$ за неко $g \in G$. Тада је

$$H \cdot x_i = H \cdot (g \cdot x_1) = (Hg) \cdot x_1 = (gg^{-1}Hg) \cdot x_1 = g \cdot ((g^{-1}Hg) \cdot x_1) = g \cdot (H \cdot x_1).$$

Но, како је $x \mapsto g \cdot x$ бијекција $X \to X$ за свако $g \in G$ (инверз је пресликавање $x \mapsto g^{-1} \cdot x$), то имамо да је $|H \cdot x_i| = |H \cdot x_1|$. Стога из **(32)** добијамо: $p = |X| = k|H \cdot x_1|$. Како је p прост, следи да или су све орбите једночлане ($k = p$) или је дејство транзитивно ($k = 1$). Но, ако би све орбите биле једночлане, то би значило да $(\forall x \in X)(x \in X^H)$, те би било $X = X^H$, што противречи претпоставци. Стога је дејство H на X транзитивно. □

Последица 80 Нека је $G \leqslant \mathbb{S}_{\{0,1,\ldots,p-1\}}$ подгрупа групе $\mathbb{S}_{\{0,1,\ldots,p-1\}}$ и нека G транзитивно дејствује на скупу $\{0, 1, \ldots, p-1\}$ и $\{\mathrm{id}\} \neq H \lhd G$. Тада и H дествује транзитивно на $\{0, 1, \ldots, p-1\}$.

Доказ. Како се у H налази и нека неидентична пермутација σ, сигурно је $\sigma(i) \neq i$ за неко $i \in \{0, \ldots, p-1\}$ те резултат директно следи из претходног става. □

Формулишимо и докажимо Галоаову теорему.

Теорема 81 Нека је $f \in K[X]$, где је K поље карактеристике 0, нерастављив полином простог степена p са решивом Галоаовом групом G. Ако корене полинома f идентификујемо са $0, \ldots, p-1$, а групу G са подгрупом групе пермутација скупа $\{0, 1, \ldots, p-1\}$, онда је сваки елемент $\sigma \in G$ облика:

$$\sigma(k) = a \cdot_p k +_p b, \tag{33}$$

за неки $a \in \{1, \ldots, p-1\}$ и $b \in \{0, 1, \ldots, p-1\}$.

Доказ. Дакле, имамо низ подгрупа

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{m-2} \rhd G_{m-1} \rhd G_m = \{\mathrm{id}\},$$

при чему су $[G_{i-1} : G_i]$ прости бројеви. Доказаћемо тврђење полазећи од подгрупе G_{m-1}. Најпре приметимо да, на основу последице **80**, све подгрупе G_i дејствују транзитивно на $\{0, 1, \ldots, p-1\}$. Дакле, и G_{m-1} је таква, а она је простог реда. Како је број елемената у орбити, овде је то p, једнак индексу стабилизатора ма ког елемента, добијамо да је стабилизатор тривијалан и да је $|G_{m-1}| = p$. На основу онога што знамо о групама пермутација, закључујемо да је група G_{m-1} генерисана једним p-циклом. Пренумерацијом корена можемо за тај генератор узети баш цикл $\theta = (0\,1\,\ldots\,p-1)$. За θ важи:

$$\theta(k) = k +_p 1,$$

а за његове степене $\theta^r(k) = k +_p r$. Дакле, заиста су сви аутоморфизми из G_{m-1} траженог облика.

Приметимо да, уколико је $\sigma \in G$ такав да је $a \neq 1$ у **(33)**, онда σ има фиксну тачку. Наиме, $a \cdot_p k +_p b = k$ је еквивалентно са $(a-1) \cdot_p k = p -_p b$, а свакако, пошто је $a - 1 \in \{1, \ldots, p-1\}$, постоји c такав да је $(a-1) \cdot_p c = 1$,

па се за k може узети: $k = c \cdot_p (p -_p b)$. Како ниједан p-цикл нема фиксну тачку, закључујемо да аутоморфизми за које је $a \neq 1$ свакако нису p-цикли. Но, за $a = 1$ имамо степене од θ.

Посматрајмо сада G_{m-2}. Ако је $\tau \in G_{m-2}$, онда је $\tau G_{m-1}\tau^{-1} = G_{m-1}$, пошто је $G_{m-1} \lhd G_{m-2}$. Посебно је $\tau \circ \theta \circ \tau^{-1} = \theta^a$ за неко a. Из ове једнакости можемо заправо потпуно одредити τ. Приметимо најпре да из ње следи: $\tau \circ \theta^k \circ \tau^{-1} = (\theta^a)^k = \theta^{a \cdot_p k}$, те је $\tau \circ \theta^k = \theta^{a \cdot_p k} \circ \tau$.

$$\tau(k) = \tau(\theta^k(0)) = (\tau \circ \theta^k)(0) = (\theta^{a \cdot_p k} \circ \tau)(0) = \theta^{a \cdot_p k}(\tau(0)) = \tau(0) +_p (a \cdot_p k) = a \cdot_p k +_p \tau(0).$$

Дакле, сваки $\tau \in G_{m-2}$ је заиста траженог облика: a је такво да је $\tau \circ \theta \circ \tau^{-1} = \theta^a$, а $b = \tau(0)$.

При преласку на G_{m-3}, користимо чињеницу да су сви елементи из G_{m-2} траженог облика. Узмимо $\sigma \in G_{m-3}$. Како $\theta \in G_{m-2}$, а како је $G_{m-2} \lhd G_{m-3}$, то је $\sigma \circ \theta \circ \sigma^{-1} \in G_{m-2}$. Но, $\sigma \circ \theta \circ \sigma^{-1}$ је такође p-цикл, па према горњој анализи је он заправо степен од θ. И настављамо као у претходном случају. Дакле, видимо да се можемо „пењати" по овом ланцу група без икаквих проблема и добијамо да је сваки аутоморфизам из G заиста траженог облика. □

Напомена 82 У претходној теореми се не тврди да је група полинома f, за који је једначина $f(x) = 0$ решива у радикалима, једнака подгрупи групе $\mathbb{S}_n$ коју чине СВИ аутоморфизми наведеног облика. Сви аутоморфизми наведеног облика свакако чине подгрупу групе $\mathbb{S}_n$ реда $p(p-1)$, али сама група датог полинома је нека подгрупа те групе. ♠

Последица 83 Нека је $f \in K[X]$ нерастављив полином полином простог степена над пољем карактеристике 0. Ако је једначина $f(x) = 0$ решива у радикалима, онда је коренско поље овог полинома генерисано ма којим паром корена.

Доказ. Нека је $\deg f = p$ и $K_f = K(\alpha_0, \alpha_1, \ldots, \alpha_{p-1})$. Нека је $0 \leqslant i < j \leqslant p-1$ и $\Omega = K(\alpha_i, \alpha_j) \subseteq K_f$. Тада је

$$G(K_f/\Omega) = \{\sigma \in G(K_f/K) : \sigma(\alpha_i) = \alpha_i, \sigma(\alpha_j) = \alpha_j\}.$$

Нека је $\sigma \in G(K_f/\Omega) \leqslant G(K_f/K)$. На основу претходне теореме, идентификујући α_k са k, добијамо да је $\sigma(k) = a \cdot_p k +_p b$ за неке a, b као горе, при чему је још

$$a \cdot_p i +_p b = i, \qquad a \cdot_p j +_p b = j. \tag{34}$$

Добијамо да је

$$a \cdot_p (j - i) = j - i. \tag{35}$$

Како је $j - i \in \{1, \ldots, p-1\}$ то постоји $c \in \{1, \ldots, p-1\}$ такво да је $(j-i) \cdot_p c = 1$. Из **(35)** множењем са c добијамо да је $a = 1$. Заменом $a = 1$ у **(34)** добијамо да је $i +_p b = i$, па је $b = 0$. Дакле, $\sigma = \mathrm{id}$. Следи да је $G(K_f/\Omega)$ тривијална група, те је $K(\alpha_i, \alpha_j) = \Omega = K_f$. □

Из ове последице директно следи следеће.

Последица 84 Нека је $K = \mathbb{Q}$ и f као у последици **83**. Тада, ако f има бар два реална корена, онда су и сви остали корени од f реални.

Доказ. Ако $\alpha, \beta \in \mathbb{R}$, онда је $K_f = \mathbb{Q}(\alpha, \beta) \subset \mathbb{R}$. □

Из ове последице, непосредно следи и следећа.

Последица 85 Нека је $K = \mathbb{Q}$ и $f \in K[X]$ полином простог степена већег од 3. Ако једначина $f(x) = 0$ има тачно три реална решења, онда она није решива у радикалима. □

11.5 Casus irreducibilis

Када користимо Карданове формуле, односно Тартаљин метод, за решавање једначине трећег степена, у случају да једначина има три различита реална решења, наилазимо на необичну ситуацију. Мада су решења реална, ми их морамо изражавати преко израза при чијем се израчунавању обавезно појављују комплексна решења (која нису реална). То је тај „несводљиви случај" из наслова пододељка. Да ли је то само мана тог метода, или је у питању суштински проблем?

Дефиниција 86 За једначину $f(x) = 0$ са коефицијентима у пољу $K \subseteq \mathbb{R}$, кажемо да је решива у РЕАЛНИМ РАДИКАЛИМА уколико постоји радикалско раширење (видети дефиницију **67**) K_m такво да је $K_f \subseteq K_m \subseteq \mathbb{R}$. Такво раширење називамо и реално радикалско раширење.

Теорема 87 Нека је $f(x) = 0$ као у претходној дефиницији, при чему је f нерастављив полином степена 3 над K, који има три (различита) реална корена. Тада ова једначина НИЈЕ решива у реалним радикалима.

Доказ. Претпоставимо да то није тако, тј. да постоји растући низ поља

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m \subseteq \mathbb{R},$$

тако да:

1. $K_i = K_{i-1}(\alpha_i)$ при чему $\alpha_i^{r_i} \in K_{i-1}$ за неки прост r_i;

2. K_m садржи коренско поље K_f полинома f.

На основу досадашњих резултата, знамо да можемо претпоставити да су сва раширења простог степена. Нека је $K_f = K(x_1, x_2, x_3)$ и нека је i најмањи индекс за који поље K_i садржи неки од x_j. То значи да је $K_{i-1} \subset K_{i-1}(x_j) \subseteq K_{i-1}(\alpha_i) = K_i$. Како је $[K_{i-1}(x_j) : K_{i-1}] = 3$, то $3 \mid r_i$, а како је r_i прост, то је $r_i = 3$ и $K_i = K_{i-1}(x_j)$. Дакле, $\alpha_i \in K_i \subseteq K_{i-1}(x_1, x_2, x_3)$. Како је $K_{i-1}(x_1, x_2, x_3)$ коренско поље полинома f посматраног као полином из $K_{i-1}[X]$, то је $K_{i-1}(x_1, x_2, x_3)/K_{i-1}$ нормално раширење. Но, оно садржи један корен α_i полинома $X^3 - \alpha_i^3 \in K_{i-1}$.

Стога оно мора да садржи и остале корене: $\alpha_i, \zeta_3\alpha_i, \zeta_3^2\alpha_i$, па бисмо добили да и $\zeta_3 \in K(x_1, x_2, x_3) \subseteq \mathbb{R}$ и ова контрадикција завршава наш доказ. □

За сам крај ове теме један забаван 'прилог'.

Није тешко извести алгебарску формулу за налажење квадратног корена из ма ког комплексног броја. Можемо претпоставити да је комплексан број јединичног модула (ако је модул различит од 1 имамо само још један квадратни корен). Дакле, треба наћи c и s тако да је $(c+is)^2 = a+ib$, при чему је $a^2+b^2 = 1$ и $ab \neq 0$. Добија се:

$$c + is = \pm\frac{1}{\sqrt{2}}\left(\sqrt{a+1} + ib\frac{1}{\sqrt{a+1}}\right). \tag{36}$$

То није тешко добити. Стога можемо изразити на овај начин и четврти, осми, итд. корен ма ког комплексног броја. Но, шта се дешава када покушамо да нађемо општу формулу за трећи корен?

Дакле, решавамо једначину $(c+is)^3 = a+ib$ уз претпоставку да је $a^2+b^2 = 1$ и $ab \neq 0$. Следи да је и $c^2+s^2 = 1$ и $cs \neq 0$. Добијамо да је $c^3 - 3cs^2 = a$, а из $s^2 = 1-c^2$ следи $4c^3 - 3c - a = 0$. Није тешко проверити да ова једначина има три различита реална решења за свако $a \in \mathbb{R}\setminus\{0\}$.

Остаје да видимо да ли је $f(X) = 4X^3 - 3X - a \in \mathbb{Q}(a)[X]$ растављив полином. Пошто тражимо ОПШТУ ФОРМУЛУ. претпоставићемо да a и b нису алгебарски бројеви (сетимо се како смо показали да проблем трисекције угла у ОПШТЕМ СЛУЧАЈУ није могуће извести помоћу лењира и шестара). У том случају је $\mathbb{Q}[a]$ је заправо прстен полинома над $\mathbb{Q}$, са НЕОДРЕЂЕНОМ a. Те је и $\mathbb{Q}(a)$ поље рационалних функција. Уколико би $f(X)$ био растављив над $\mathbb{Q}(a)$, то би значило да је растављив и над $\mathbb{Q}[a]$ (Алгебра 2), те би ту имао нулу, тј. постојао би полином $p(a) \in \mathbb{Q}[a]$ такав да је

$$4p(a)^3 - 3p(a) - a = 0 \in \mathbb{Q}[a].$$

Уколико $p(a)$ није константан полином, онда је степен полинома $4p(a)^3 - 3p(a) - a$ једнак $3\deg p(a)$ те то не може бити нула полином. А ако је $p(a) \in \mathbb{Q}$, онда би и a било из $\mathbb{Q}$, што није тачно.

Стога се, на основу теореме **87**, c не може добити у облику који укључује само реалне корене, тако да формула за трећи корен комплексног броја аналогна формули **(36)** за квадратни корен не постоји.

Прости и максимални идеали у прстенима

Сада почињемо да се бавимо новом темом у овом курсу, а то је растављање (факторизација) полинома и налажење највећег заједничког делиоца. Но, нећемо се задовољити само полиномима једне неодређене, нити само полинома са коефицијентима у пољу, него ћемо се позабавити и полиномима са више неодређених и са коефицијентима у $\mathbb{Z}$. То се заправо појављује имплицитно и школској математици, у делу о сређивању алгебарских израза. Наравно, тамо се то ради интуитивно, али овде ћемо видети како се то највећи заједнички делилац може наћи чак и кад није видљиво како се дати полиноми могу факторисати. Но, најпре ћемо морати да радимо општије ствари у прстенима, што тако ђе није лоше, јер ћемо видети како се неки резултати, које знамо из основне школе, мењају када уместо прстена $\mathbb{Z}$ посматрамо прстене који се од овог добијају додавањем неких елемената.

Започнимо ову тему следећим ставом.

Став 88 Нека је A комутативан прстен са јединицом и $P \triangleleft A$ ($P \neq A$). Следећи услови су еквивалентни.

1. За $I, J \triangleleft A$ важи: ако је $I \cdot J \subseteq P$, онда је $I \subseteq P$ или је $J \subseteq P$.
2. За $a, b \in A$ важи: ако $ab \in P$, онда $a \in P$ или $b \in P$.
3. Прстен A/P је област целих (домен).

Доказ. Подсетимо се најпре да се област целих дефинише као комутативан прстен са јединицом у коме нема правих делитеља нуле, тј. у коме важи: ако је $ab = 0$, онда је $a = 0$ или $b = 0$.

$1 \Longrightarrow 2$. Уочимо идеале $I = \langle a \rangle$, $J = \langle b \rangle$. Како је $I \cdot J = \langle ab \rangle$ и $ab \in P$, то $I \cdot J \subseteq P$. На основу 1. следи да $I \subseteq P$, или $J \subseteq P$, тј. $a \in P$, или $b \in P$.

$2 \Longrightarrow 3$. Претпоставимо да за елементе $x, y \in A/P$ важи: $xy = 0_{A/P}$. Наравно, $0_{A/P} = P$. Како су x и y елементи из количничког прстена, то постоје $a, b \in A$ такви да је $x = a + P$ и $y = b + P$ и да важи: $(a+P)(b+P) = P$. Ова једнакост се своди на $ab + P = P$, тј. на $ab \in P$. На основу 2. добијамо да $a \in P$, или $b \in P$, односно $a + P = P$ или $b + P = P$, тј. $x = 0$, или $y = 0$.

$3 \Longrightarrow 1$. Нека су идеали I, J прстена A такви да је $I \cdot J \subseteq P$, а да $I \not\subseteq P$ и $J \not\subseteq P$. То значи да постоји $a \in I \setminus P$ и $b \in J \setminus P$. Но, $ab \in I \cdot J \subseteq P$, па је $(a + P)(b + P) = ab + P = P$. Како је A/P област целих, следи да је $a + P = P$, или $b + P = P$, односно $a \in P$ или $b \in P$. Ова контрадикција завршава доказ. □

Дефиниција 89 Идеал $P \triangleleft A$ је прост уколико испуњава неко од претходна три еквивалентна својства.

Пример 90 Идеал $\langle 2, 1-\sqrt{-5}\rangle \lhd \mathbb{Z}[\sqrt{-5}]$ је прост идеал.

Покажимо да је $\mathbb{Z}[\sqrt{-5}]/\langle 2, 1-\sqrt{-5}\rangle \cong \mathbb{Z}_2$. Приметимо да је сваки елемент у прстену $\mathbb{Z}[\sqrt{-5}]$ облика $m+n\sqrt{-5}$ за неке целе бројеве m и n. Дефинишимо пресликавање $f\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}_2$ са:

$$f(m+n\sqrt{-5}) = \rho(m+n, 2).$$

Покажимо да је ово пресликавање хомоморфизам прстена.

$$\begin{aligned} &f((m+n\sqrt{-5})+(r+s\sqrt{-5})) = f((m+n)+(r+s)\sqrt{-5}) \\ &= \rho((m+n)+(r+s), 2) = \rho(m+n, 2) +_2 \rho(r+s, 2) = f(m+n\sqrt{-5}) +_2 f(r+s\sqrt{-5}). \end{aligned}$$

$$\begin{aligned} &f((m+n\sqrt{-5})(r+s\sqrt{-5})) = f(mr-5ns+(ms+nr)\sqrt{-5}) \\ &= \rho(mr-5ns+ms+nr, 2) = \rho(mr+ns+ms+nr, 2) = \rho((m+n)(r+2), 2) \\ &\qquad = \rho(m+n, 2) \cdot_2 \rho(r+s, 2) = f(m+n\sqrt{-5}) \cdot_2 f(r+s\sqrt{-5}). \end{aligned}$$

Наравно, $f(1) = 1$. Јасно је да је f „на". Треба одредити језгро овог хомоморфизма. Но, $m+n\sqrt{-5} \in \operatorname{Ker} f$ **акко** $2 \mid (m+n)$. Но,

$$m+n\sqrt{-5} = m-n(-\sqrt{-5}) = m-n(1-\sqrt{-5}-1) = (m+n)-n(1-\sqrt{-5}).$$

Стога, ако је $m+n$ паран број, онда је $m+n = 2t$ за неко $t \in \mathbb{Z}$ и на основу горње једнакости $m+n\sqrt{-5} \in \langle 2, 1-\sqrt{-5}\rangle$. Обратно, ако $m+n\sqrt{-5} \in \langle 2, 1-\sqrt{-5}\rangle$, онда је

$$\begin{aligned} &m+n\sqrt{-5} = (a+b\sqrt{-5})\cdot 2 + (c+d\sqrt{-5})\cdot(1-\sqrt{-5}) \\ &= 2a+2b\sqrt{-5}+c-c\sqrt{-5}+d\sqrt{-5}+5d = (2a+c+5d)+(2b-c+d)\sqrt{-5}, \end{aligned}$$

за неке $a, b, c, d \in \mathbb{Z}$. Тада је

$$m+n = 2a+c+5d+2b-c+d = 2a+2b+6d,$$

па је $m+n$ паран број. Добили смо да је $\operatorname{Ker} f = \langle 2, 1-\sqrt{-5}\rangle$ и на основу теореме о изоморфизму прстена добијамо тражени изоморфизам. Како је $\mathbb{Z}_2$ област целих, закључујемо да је идеал $\langle 2, 1-\sqrt{-5}\rangle$ прост. ♣

Приметимо да, уколико је P прост идеал, а $a_1, \ldots, a_n \in A$, онда из $a_1 \cdots a_n \in P$ следи да $a_i \in P$ за неко $i \in \{1, \ldots, n\}$ (што се лако доказује индукцијом по n).

Пређимо сада на појам максималног идеала.

Дефиниција 91 Идеал M прстена A је максималан, уколико не постоји идеал I прстена A за који важи: $M \subset I \subset A$.

Дакле, максималан идеал је прави идеал за који не постоји прави идеал, различит од њега, који га садржи као свој подскуп.

Став 92 Нека је M прави идеал прстена A. Тада је M максималан идеал ако и само ако је A/M поље.

Доказ. Претпоставимо да је M максималан идеал и $a+M \neq M$. Треба показати да $a+M$ има инверз у прстену A/M. Посматрамо идеал $\langle a\rangle + M$. Како $a \notin M$, то је M прави подскуп од $\langle a\rangle + M$. Но, с обзиром да је M максималан идеал, мора бити $\langle a\rangle + M = A$. То значи да постоје $b \in A$ и $m \in M$ за које је $ab + m = 1$. Дакле, $ab - 1 = m \in M$, па је $ab + M = 1 + M$, те је $b + M$ тражени инверз елемента $a + M \in M$.

Обратно, претпоставимо да је A/M поље. Нека је M прави подскуп идеала I. Дакле, постоји $a \in I \setminus M$. Стога је $a + M \neq M$ у количничком прстену A/M. Како је овај прстен по претпоставци поље, то постоји $b \in M$ тако да је $(a+M)(b+M) = 1+M$, односно, $ab-1 \in M$. Дакле, за неко $m \in M$ важи: $ab - 1 = m$, тј. $1 = ab - m$. Како и a и m припадају идеалу I, то и $1 \in I$, па мора бити $I = A$. Закључујемо да је M заиста максималан идеал у A. □

Напомена 93 Видимо да из овог става следи да је сваки максималан идеал уједно и прост идеал, пошто знамо у пољу нема правих делитеља нуле. ♢

У основној школи смо научили да је природан број прост уколико нема других делилаца сем 1 и њега самог (ово такође важи и за број 1, али се он не сматра простим бројем). Но, у произвољној области целих разликује се појам простог и нерастављивог елемента. Подсетимо се да са $U(A)$ означавамо скуп свих инвертибилних елемената у прстену A.

Дефиниција 94 Нека је A област целих (домен), тј. комутативни прстен са јединицом у коме је производ два елемента једнак нули ако и само ако је један од њих једнак нули. Елемент $p \in A \setminus (U(A) \cup \{0\})$ је

- ПРОСТ, уколико за $a, b \in A$ важи: ако $p \mid ab$, онда $p \mid a$, или $p \mid b$;
- НЕРАСТАВЉИВ (АТОМ) уколико за $a, b \in A$ важи: ако је $p = ab$, онда је $a \in U(A)$, или $b \in U(A)$.

Веза између простих и нерастављивих елемената у произвољном прстену дата је следећим ставом.

Став 95 Нека је A домен. Тада је сваки прост елемент у A нерастављив.

Доказ. Претпоставимо да је p прост и да је $p = ab$. Посебно то значи да p дели производ ab. Како је p прост, то $p \mid a$, или $p \mid b$. Нека, на пример, $p \mid a$. То значи да постоји $c \in A$ за који је $a = pc$. Како је $p = ab$, то је $p = pcb$, тј. $p(1 - cb) = 0$, па мора бити $1 - cb = 0$, пошто је A област целих. Дакле, $cb = 1$, те је елемент b инвертибилан. □

У произвољном домену, прости и нерастављиви елементи се разликују. Размотримо следећи пример.

Пример 96 У прстену $\mathbb{Z}\left[\sqrt{-5}\right]$ елемент 3 је нерастављив, али није прост.

Пре свега,

$$\mathbb{Z}\left[\sqrt{-5}\right] := \{p(\sqrt{-5}) : p \in \mathbb{Z}[X]\}.$$

Но, није тешко уверити се да из дефиниције следи да је

$$\mathbb{Z}\left[\sqrt{-5}\right] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

Уверимо се најпре да је 3 нерастављив. Претпоставимо да је $3 = uv$. Уведимо ознаку $N(z) := z\overline{z}$, за $z \in \mathbb{Z}\left[\sqrt{-5}\right]$ (наравно да је $N(z)$ квадрат модула комплексног броја z). Јасно је да је $N(z_1 z_2) = N(z_1)N(z_2)$ за све z_1, z_2. Добијамо да је $N(3) = N(u)N(v)$, односно $9 = N(u)N(v)$. Ово је факторизација природног броја 9 у скупу природних бројева, то имамо две могућности:

1) један од $N(u)$, $N(v)$ једнак је 1, а други 9;

2) $N(u) = N(v) = 3$.

1) Претпоставимо, на пример, да је $N(u) = 1$. Уколико је $u = a+b\sqrt{-5}$, добијамо да је $1 = N(u) = u\overline{u} = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2$. С обзиром да $a, b \in \mathbb{Z}$, ово је могуће једино ако је $b = 0$ и $a \in \{-1, 1\}$, тј. $u \in \{-1, 1\}$, те следи да је u инвертибилан (било би добро да читаоци сами покажу, за вежбу, да је $U\left(\mathbb{Z}\left[\sqrt{-5}\right]\right) = \{-1, 1\}$ користећи функцију N).

2) Поступамо на сличан начин. Уколико је $u = a + b\sqrt{-5}$, добијамо да је $3 = N(u) = a^2 + 5b^2$. С обзиром да $a, b \in \mathbb{Z}$, мора бити $b = 0$ и добијамо да је $3 = a^2$, за неко $a \in \mathbb{Z}$. Ово наравно није могуће, те закључујемо да се случај 2) и не појављује.

Дакле, из чињенице да је $3 = uv$, добијамо да је један од фактора инвертибилан, а то заправо значи да је 3 нерастављив.

Остаје да покажемо да 3 није прост. Посматрајмо факторизацију броја 9 у $\mathbb{Z}\left[\sqrt{-5}\right]$:

$$9 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Како је $9 = 3 \cdot 3$, то

$$3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Покажимо да 3 не дели ниједан од ових фактора. Из те чињенице ће следити да 3 није прост.

Нека $3 \mid (2 + \sqrt{-5})$ (аналогно се разматра и други случај). Дакле, за неки елемент $u \in \mathbb{Z}\left[\sqrt{-5}\right]$:

$$3 \cdot u = 2 + \sqrt{-5}.$$

Применом функције N добијамо

$$9 \cdot N(u) = 9.$$

Добијамо да је $N(u) = 1$, те је $u \in \{-1, 1\}$, тј. $3 = 2 + \sqrt{-5}$, или $3 = -(2 + \sqrt{-5})$. Ова контрадикција нам показује да 3 не дели $2 + \sqrt{-5}$, тј. 3 заиста није прост. ♣

Напомена 97 Приметимо да једнакост $3 \cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5})$ даје две различите факторизације броја 9 у производ нерастављивих. То је нешто са чиме се нисмо срели у случају целих бројева. Више ћемо о овоме рећи у наредним предавањима. ♢

Следећи став је помало и очекиван.

Став 98 Елемент је прост ако и само ако је идеал генерисан тим елементом прост идеал.

Доказ. Нека је p прост елемент у прстену A и $\langle p\rangle$ идеал генерисан тим елементом. Уколико $ab \in \langle p\rangle$, онда је $ab = pc$ за неки $c \in A$, тј. $p \mid ab$. Како је елемент p прост, то $p \mid a$, или $p \mid b$, односно, $a \in \langle p\rangle$, или $b \in \langle p\rangle$, те закључујемо да је $\langle p\rangle$ прост идеал.

Обратно, претпоставимо да је $\langle p\rangle$ прост идеал и нека $p \mid ab$. То значи да $ab \in \langle p\rangle$, те следи да $a \in \langle p\rangle$, или $b \in \langle p\rangle$, односно $p \mid a$, или $p \mid b$. □

Напомена 99 Као што смо доказали да 3 није прост, можемо доказати да ни 2 није прост. Стога идеал $\langle 2\rangle$ није прост. Но, важи једнакост

$$\langle 2\rangle = \langle 2, 1-\sqrt{-5}\rangle\langle 2, 1+\sqrt{-5}\rangle.$$

Наиме, лако је видети да је генерално тачно да је $\langle a, b\rangle\langle c, d\rangle = \langle ac, ad, bc, bd\rangle$. Стога је

$$\langle 2, 1-\sqrt{-5}\rangle\langle 2, 1+\sqrt{-5}\rangle = \langle 4, 2+2\sqrt{-5}, 2-2\sqrt{-5}, 6\rangle,$$

но, 2 припада овом идеалу као разлика $6-4$, а сви остали елементи су умношци од 2. Стога је тај идеал заправо $\langle 2\rangle$. Као што смо доказали да је идеал $\langle 2, 1-\sqrt{-5}\rangle$ прост идеал, може се доказати да је то и идеал $\langle 2, 1+\sqrt{-5}\rangle$. Дакле, мада идеал $\langle 2\rangle$ није прост, он ипак има факторизацију на производ простих идеала. Заправо, тачно је, мада ми нећемо то овде доказивати, да сваки идеал у прстену $\mathbb{Z}[\sqrt{-5}]$ има јединствену, до на редослед фактора, факторизацију у облику простих идела! Према томе, мада елементи немају јединствену факторизацију, преласком на идеале добијамо јединствену факторизацију. Посебно то важи за главне идеале. Видимо сада зашто нам је корисна аритметика идеала. ♢

Веза између нерастављивих елемената и максималних идеала дата је следећим ставом.

Став 100 Елемент $a \in A$ је нерастављив ако и само ако је идеал $\langle a\rangle$ максималан у скупу свих главних идеала прстена A.

Доказ. Претпоставимо да је $a \in A$ нерастављив и нека је $\langle a\rangle \subseteq \langle b\rangle$. Треба да покажемо да је $\langle a\rangle = \langle b\rangle$ или $\langle b\rangle = A$. Како је $\langle a\rangle \subseteq \langle b\rangle$, то $a \in \langle b\rangle$, па постоји $c \in A$ тако да је $a = bc$. Како је a нерастављив,

то $b \in U(A)$, или $c \in U(A)$. Уколико $b \in U(A)$, онда је $\langle b \rangle = A$, а ако $c \in U(A)$, онда је $\langle a \rangle = \langle b \rangle$.

Обратно, претпоставимо да је $\langle a \rangle$ максималан у скупу свих главних идеала прстена A. Нека је $a = bc$ и претпоставимо да $c \notin U(A)$. То значи да је $a \in \langle b \rangle$, али да $b \notin \langle a \rangle$ (зашто?), тј. да је $\langle a \rangle$ прави подскуп идеала $\langle b \rangle$. Како је $\langle a \rangle$ максималан у скупу свих главних идеала, то мора бити $\langle b \rangle = A$, тј. постоји $c \in A$ тако да је $bc = 1$, те закључујемо да је b инвертибилан. □

Максималан идеал у сваком комутативном прстену са јединицом постоји. Заправо, важи следећа теорема, коју нећемо доказивати.

Теорема 101 Нека је I прави идеал у комутативном прстену са јединицом A. Тада постоји максималан идеал M за који је $I \subseteq M$.

Посебно је занимљив случај прстена у којима постоји тачно један максимални идеал.

Став 102 У комутативном прстену са јединицом A постоји тачно један максималан идеал ако и само ако је $A \setminus U(A)$ идеал.

Доказ. Приметимо да важи следеће. Идеал $I \lhd A$ је прави акко I не садржи ниједан инвертибилан елемент (видети пример **??**).

Претпоставимо да у прстену постоји тачно један максималан идеал M. Према претходном је $U(A) \subseteq A \setminus M$. Но, ако постоји $a \in A \setminus M$ који није инвертибилан, онда је идеал $\langle a \rangle$ прави, па је према теореми **101** $\langle a \rangle$ садржиан у неком максималном, а како је M једини такав, то је $\langle a \rangle \subseteq M$, што није могуће, јер $a \notin M$.

Обратно, нека у прстену A сви неинвертибилни елементи чине идеал M: $A \setminus U(A) = M$. Но, тада је и сваки други идеал I садржан у M, јер је $I \cap U(A) = \emptyset$, као што смо горе приметили. Стога је M максималан идеал и то једини такав. □

Дефиниција 103 Комутативан прстен са јединицом у коме постоји тачно један максимални идеал назива се ЛОКАЛНИ ПРСТЕН.

Пример 104 Нека је $p \in \mathbb{N}$ прост број. Тада је прстен $\mathbb{Z}_{(p)}$ дефинисан са:

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} : p \nmid b \right\}$$

локални.

Треба само показати да неинвертибилни елементи чине идеал. Приметимо да $\frac{a}{b} \in U(\mathbb{Z}_{(p)})$ **акко** $p \nmid a$. Дакле, $\frac{a}{b} \notin U(\mathbb{Z}_{(p)})$ **акко** $p \mid a$. Но, то управо значи да је скуп свих неинвертибилних елемената у овом прстену скуп свих умножака броја p, тј. идеал генерисан са p. ♣

Пример 105 Нека је A задат са:

$$A = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a, b \in \mathbb{Q} \right\}.$$

Показати да је A комутативни прстен са јединицом у односу на множење и сабирање матрица и да је A пример локалног прстена.

Није тешко проверити да је A комутативан прстен са јединицом, као и да је матрица из $\left[\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right] \in A$ инвертибилна **акко** је $a \neq 0$. Дакле,

$$A \setminus U(A) = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} : b \in \mathbb{Q} \right\}.$$

Но,

$$\left\langle \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{Q} \right\} = \left\{ \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{Q} \right\} = A \setminus U(A).$$

Дакле, неинвертибилни елементи чине главни идеал генерисан матрицом $\left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$. ♣

Факторизација; локализација

Подсетимо се да је област целих (домен) комутативан прстен са јединицом у коме нема правих делитеља нуле, тј. у којима важи: за све $a, b \in A$ из $ab = 0$ следи $a = 0$, или $b = 0$. Сви прстени којима ћемо се бавити у овој лекцији биће домени.

Дефиниција 106 Два елемента $a, b \in A$ су ПРИДРУЖЕНА уколико постоји елемент $u \in U(A)$ такав да је $a = ub$.

Јасно је да је придруженост елемената једна релација еквиваленције. Приметимо да ако је p нерастављив онда је то и сваки њему придружен елемент. Исто то важи и за просте елементе у домену.

Дефиниција 107 Домен A је домен са једнозначном факторизацијом уколико су испуњени следећи услови.

1. За сваки елемент из $a \in A \setminus (U(A) \cup \{0\})$ постоје нерастављиви елементи $p_1, \ldots, p_r$ такви да је $a = p_1 p_2 \cdots p_r$.

2. Ако је за нерастављиве елементе p_i, q_j:

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

онда је $r = s$ и постоји пермутација $\sigma \in \mathbb{S}_r$ тако да је за све $i = \overline{1, r}$ елемент p_i придружен елементу $q_{\sigma(i)}$.

Другим речима у домену са јединственом факторизацијом, сваки елемент може се на јединствен начин, до на придруженост и редослед фактора, приказати у облику производа нерастављивих елемената.

Став 108 Домен A је домен са јединственом факторизацијом акко се сваки елемент $a \in A \setminus (U(A) \cup \{0\})$ може приказати у облику производа простих елемената. Посебно, то значи да је сваки нерастављив елемент прост.

Доказ. Претпоставимо да се сваки неинвертибилан, ненула елемент може приказати у облику производа простих. Како су прости нерастављиви, потребно је само доказати да је приказ у облику производа јединствен (у горенаведеном смислу). Докажимо најпре да је, у овом случају, сваки нерастављив елемент прост.

Нека је q нерастављив елемент. По претпоставци, он се може написати у облику производа простих елемената: $q = p_1 \cdots p_r$, где су p_i прости. Но, како је q нерастављив, мора бити $r = 1$, тј. и сам q је прост.

Докажимо сада јединственост разлагања у облику производа нерастављивих елемената. Нека је

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

Доказ изводимо индукцијом по r. Случај $r = 1$ је тривијалан. Претпоставимо да је у горњој једнакости $r > 1$ и да су су p_i, q_j нерастављиви. Према доказаном, p_1 је прост, па постоји $j_1 \in \{1, \ldots, s\}$ тако да $p_1 \mid q_{j_1}$. Како је q_{j_1} нерастављив, добијамо да су p_1 и q_{j_1} придружени, тј. да постоји $u_1 \in U(A)$ за који је $q_{j_1} = u_1 p_1$. Горњу једнакост можемо скратити са p_1 и добити

$$p_2 \cdots p_r = q_2' q_3 \cdots q_s,$$

где је $q_2' = q_2 u_1$, који је такође нерастављив. Индуктивна хипотеза завршава доказ.

Обратно, претпоставимо да је A домен за јединственом факторизацијом. Довољно је показати да је сваки нерастављив елемент прост. Нека је p нерастављив и нека $p \mid ab$. Треба показати да $p \mid a$, или $p \mid b$. Претпоставимо да p не дели ни a ни b. Нека је $a = p_1 \cdots p_r$ факторизација a на нерастављиве елементе и $b = q_1 \cdots q_s$ факторизација b на нерастављиве. Тада је

$$ab = p_1 \cdots p_r q_1 \cdots q_s$$

факторизација ab на нерастављиве. Како p дели ab, то је $ab = pc$ за неко c. И c има факторизацију на нерастављиве елементе, па је $c = z_1 \cdots z_l$ за неке нерастављиве $z_1, \ldots, z_l$. Добијамо да је

$$p_1 \cdots p_r q_1 \cdots q_s = p z_1 \cdots z_l,$$

где су сви p_i, q_j, z_k и p нерастављиви. Како је, по претпоставци, A домен са једнозначном факторизацијом, то је p придружен неком од елемената из скупа $\{p_1, \ldots, p_r, q_1, \ldots, q_s\}$. Уколико је p придружен елементу p_i (за неко i), добијамо да $p \mid a$, а ако је p придружен неком q_j онда $p \mid b$. Наиме, лако се показује да важи следеће: ако је p придружен елементу q и ако $q \mid c$, онда и $p \mid c$. Овим је доказ завршен. □

Знамо да је $\mathbb{Z}$ домен за једнозначном факторизацијом. Показаћемо сада да је сваки главноидеалски домен уједно и домен са једнозначном факторизацијом.

Став 109 Доказати да у сваком главноидеалском домену за свака два елемента постоји њихов највећи заједнички делилац.

Доказ. Нека A један главноидеалски домен и $a, b \in A$. Уочимо идеал $\langle a, b\rangle$ генерисан елементима a и b. Како је у A сваки идеал главни, то је и $\langle a, b\rangle = \langle d\rangle$, за неки $d \in A$. Докажимо да је d један највећи заједнички делилац елемената a и b (највећи заједнички делилац није једнозначно одређен, али су свака два највећа заједничка делиоца придружени један другом).

Најпре, $a, b \in \langle d\rangle$. То значи да постоје a_1, b_1 за које је $a = da_1$ и $b = db_1$, тј. $d \mid a$ и $d \mid b$, те d јесте заједнички делилац од a и b.

Претпоставимо да $d_1 \mid a$ и $d_1 \mid b$, тј. да је d_1 неки заједнички делилац од a и b. Треба доказати да $d_1 \mid d$. Како $d_1 \mid a$ и $d_1 \mid b$, то постоје a_1 и b_1 тако да је $a = d_1a_1$ и $b = d_1b_1$. С обзиром да $d \in \langle a, b\rangle$, постоје p, q такви да је $d = ap + bq$. Добијамо да је $d = d_1a_1p + d_1b_1q = d_1(a_1p + b_1q)$, те следи да $d_1 \mid d$. □

Заправо је у овом ставу доказано не само да свака два елемента a и b имају највећи заједнички делилац d, но и да постоје p и q за које је $d = ap + bq$ (Безуова релација). Из ове релације се, на стандардан начин, изводи следеће својство: ако $a \mid bc$ и ако је $\mathrm{NZD}(a, b)$ придружен јединици, онда $a \mid c$ (наравно, уместо да пишемо да је $\mathrm{NZD}(a, b)$ придружен јединици, писаћемо да је $\mathrm{NZD}(a, b) = 1$, имајући на уму шта то значи). Нека читаоци ово сами докажу.

Теорема 110 Сваки главноидеалски домен је и домен са једнозначном факторизацијом.

Доказ. Нека је A главноидеалски домен. Докажимо најпре да је сваки нерастављив елемент у A прост. Нека је q нерастављив и нека $q \mid ab$. Уколико q не дели a, мора бити $\mathrm{NZD}(q, a) = 1$. Наиме, ако је $d = \mathrm{NZD}(q, a)$, то значи да је $q = dz$ за неко z. Како је q нерастављив, мора бити $d \in U(A)$, или $z \in U(A)$. Но, ако је $z \in U(A)$, онда из чињенице да $d \mid a$ следи да и $q \mid a$, што противречи претпоставци. Закључујемо да $d \in U(A)$, тј. $\mathrm{NZD}(q, a) = 1$ (погледајте ранију напомену у загради).

Но, тада из горенаведеног својства следи да $q \mid b$, те закључујемо да је q прост.

Да бисмо доказали да је A домен са једнозначном факторизацијом, остаје само да покажемо да се сваки елемент из $A \setminus (U(A) \cup \{0\})$ може приказати у облику производа нерастављивих елемената (видети став **108**).

Докажимо најпре да сваки непразан скуп идеала у A има максималан елемент. Претпоставимо да то није тако и нека је $\mathcal{I}$ неки непразан скуп идеала који не садржи максималан елемент. Нека је $I_1 \in \mathcal{I}$ произвољан идеал из $\mathcal{I}$. Како он није максималан у $\mathcal{I}$, то постоји $I_2 \in \mathcal{I}$ за који је $I_1 \subset I_2$. Слично, постоји и $I_3 \in \mathcal{I}$ такав да је $I_2 \subset I_3$. Заправо добијамо стриктно растући ланац идеала

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

из $\mathcal{I}$. Унија $J = \bigcup_{i=1}^{\infty} I_i$ је идеал као што се лако може проверити (проверите!). Но, с обзиром да је A главноидеалски, то је $J = \langle x \rangle$ за неки $x \in A$. Како је $x \in \bigcup_{i=1}^{\infty} I_i$, то $x \in I_{i_0}$ за неки i_0. Но, одавде следи да је $J = I_{i_0}$, па је и $I_i = I_{i_0}$ за све $i \geq i_0$, те бесконачан стриктно растући ланац идеала и не постоји. Закључујемо да у $\mathcal{I}$ постоји максималан елемент.

Претпоставимо да у $A \setminus (U(A) \cup \{0\})$ има елемената који немају факторизацију на нерастављиве елементе. Уочимо скуп идеала $\mathcal{J}$ задат са:

$$\mathcal{J} = \{\langle a \rangle : a \in A \setminus (U(A) \cup \{0\}) \text{ и } a \text{ нема факторизацију на нерастављиве}\}.$$

Према управо доказаном резултату, у $\mathcal{J}$ постоји максималан елемент $\langle x \rangle$. Како x нема факторизацију на нерастављиве, то он сам није нерастављив, па постоје a, b такви да је $x = ab$, при чему $a, b \in A \setminus (U(A) \cup \{0\})$. Стога је $\langle x \rangle \subset \langle a \rangle$ и $\langle x \rangle \subset \langle b \rangle$ (зашто?), па a и b имају факторизацију на нерастављиве ($\langle x \rangle$ је максималан елемент у $\mathcal{J}$). Но, ако су то факторизације $a = p_1 \cdots p_r$ и $b = q_1 \cdots q_s$, онда је $x = ab = p_1 \cdots p_r q_1 \cdots q_s$ једна факторизација x на нерастављиве, што противречи избору елемента x. Ова контрадикција завршава доказ. □

Дакле, домен са једнозначном факторизацијом се карактерише тиме да се у њему прости и нерастављиви елементи подударају и да се сваки ненула, неинвертибилан елемент a може представити у облику

$$a = up_1^{\alpha_1} \cdots p_k^{\alpha_k}, \tag{37}$$

где је u инвертибилан елемент и p_i нерастављиви, при чему за $i \neq j$ елементи p_i и p_j нису придружени, док је $\alpha_i \in \mathbb{N}$. Осим тога, ако је

$$a = vq_1^{\beta_1} \cdots q_l^{\beta_l},$$

где је v инвертибилан, q_j нерастављиви и q_i, q_j нису придружени за $i \neq j$, онда је $k = l$ и за неку пермутацију $\sigma \in \mathbb{S}_k$ $\alpha_i = \beta_{\sigma(i)}$ и p_i је придружен елементу $q_{\sigma(i)}$.

Напомена 111 Читалац се можда пита зашто се појављује инвертибилан елемент u у представљању елемента a у облику производа, када се тако нешто не појављује у самој дефиницији домена са једнозначном факторизацијом. Разлог лежи у томе што нерастављиви елементи p_i нису међусобно придружени и онда је неопходно издвојити инвертибилан елемент u. На пример, елемент $-36 \in \mathbb{Z}$ се може записати у облику $-36 = (-1)2^2 3^2$, или у облику $-36 = (-1)2^2(-3)^2$, али се (-1) мора појавити у овим записима. Презентација $-36 = 2(-2)3^2$ не задовољава услов да за различите индексе прости елементи нису придружени. $\diamondsuit$

Пређимо сада на важан метод локализације којим се од датог домена прелази на нови домен, а у коме су неки изабрани елементи из почетног домена инвертибилни у новом домену (ми смо се у основној школи упознали са овим – то је увођење разломака). Почнимо следећом дефиницијом.

Дефиниција 112 Нека је A домен и $S \subseteq A \setminus \{0\}$. За S кажемо да је мултипликативан ако $1 \in S$ и ако из $s, t \in S$ следи да $st \in S$.

Пример 113 Следећи подскупови од $A \setminus \{0\}$ су мултипликативни:

1. $A \setminus \{0\}$;
2. $\{f^n : n \in \mathbb{N}\}$, за ма који елемент $f \in A \setminus \{0\}$;
3. $A \setminus P$ за ма који прост идеал $P \lhd A$.

1. Ово је јасно.

2. Подсетимо се да $0 \in \mathbb{N}$, па $1 \in S$. Осим тога, како је $f^m f^n = f^{m+n}$ и други услов је испуњен.

3. Јасно је да $1 \in A \setminus P$. Осим тога, ако $a \notin P$ и $b \notin P$, онда и $ab \notin P$, пошто је P прост идеал (појасните себи ово!). $\clubsuit$

Нека је A домен и S ма који мултипликативан подскуп од A. На скупу $A \times S$ дефинишемо релацију $\sim$ са:

$$(a, s) \sim (b, t) \overset{\text{def}}{\iff} ta = sb.$$

Докажимо да је $\sim$ једна релација еквиваленције.

Рефлексивност. Ово је јасно пошто је $sa = sa$, па је $(a, s) \sim (a, s)$.

Симетричност. И ово је јасно, јер из $(a, s) \sim (b, t)$, следи да је $ta = sb$, тј, $sb = ta$, а то управо значи да је $(b, t) \sim (a, s)$.

Транзитивност. Нека је $(a,s)\sim(b,t)$ и $(b,t)\sim(c,r)$. То значи да је $ta=sb$ и $rb=tc$. Добијамо да је

$$rta=rsb=stc.$$

Како је A домен, то је $ra=sc$, па је $(a,s)\sim(c,r)$.

Са $S^{-1}A$ означавамо скуп свих класа еквиваленције, а са $\frac{a}{s}$ класу еквиваленције елемента (a,s). Дефинишемо операције $+$ и $\cdot$ на $S^{-1}A$ са:

$$\frac{a}{s}+\frac{b}{t}:=\frac{ta+sb}{st};$$

$$\frac{a}{s}\cdot\frac{b}{t}:=\frac{ab}{st}.$$

Како је скуп S мултипликативан, то за $s,t\in S$ и $st\in S$, па ови записи имају смисла. Треба још да проверимо да су ове операције добро дефинисане.

Нека је $\frac{a}{s}=\frac{a'}{s'}$ и $\frac{b}{t}=\frac{b'}{t'}$. То заправо значи да је $(a,s)\sim(a',s')$ и $(b,t)\sim(b',t')$. Треба проверити да је $(ta+sb,st)\sim(t'a'+s'b',s't')$ и $(ab,st)\sim(a'b',s't')$. Рачунамо:

$$s't'(ta+sb)=s't'ta+s't'sb=t'tsa'+s'stb'=st(t'a'+s'b'),$$

па је заиста $(ta+sb,st)\sim(t'a'+s'b',s't')$. На сличан начин се проверава и добра дефинисаност операције множења.

Није тешко проверити да је структура $(S^{-1}A,+,\cdot)$ један комутативан прстен са јединицом (урадите то за вежбу: $0_{S^{-1}A}=\frac{0}{1}$, $1_{S^{-1}A}=\frac{1}{1}$). Овај прстен назива се локализација домена A у односу на мултипликативан скуп S. Основно својство локализације дато је следећим ставом.

Став 114 Нека је A домен и S неки мултипликативан подскуп од A.

а) Са $i(a)=\frac{a}{1}$ задат је један мономорфизам $i\colon A\to S^{-1}A$,

б) Ако је B ма који комутативан прстен и $f\colon A\to B$ хомоморфизам такав да за све $s\in S$ важи: $f(s)\in U(B)$, онда постоји тачно један хомоморфизам $\widetilde{f}\colon S^{-1}A\to B$ за који је $\widetilde{f}\circ i=f$.

Доказ.

а) Како је $i(a+b)=\frac{a+b}{1}=\frac{a}{1}+\frac{b}{1}=i(a)+i(b)$ и $i(ab)=\frac{ab}{1}=\frac{a}{1}\frac{b}{1}$, то је i заиста хомоморфизам. Но, $a\in\mathrm{Ker}(i)$ ако и само ако је $\frac{a}{1}=\frac{0}{1}$, што је еквивалентно са $a=0$, па је i мономорфизам.

б) Тражени хоморфизам $\widetilde{f}$ дефинишемо са: $\widetilde{f}(\frac{a}{s})=f(a)f(s)^{-1}$. Како је, за све $s\in S$, $f(s)$ инвертибилан, ова дефиниција има смисла. Остављамо читаоцима да провере да је ово заиста један добро дефинисан хомоморфизам и да важи: $\widetilde{f}\circ i=f$. □

Уколико је $S=A\backslash P$ за неки прост идеал P, онда се уместо $(A\backslash P)^{-1}A$ краће пише: A_P. Важи следећа теорема.

Теорема 115 За сваки прост идеал $P \triangleleft A$, прстен A_P је локални прстен.

Доказ. Доказаћемо да је скуп свих неинвертибилних елемената идеал. Одредимо најпре $U(A_P)$:

$$\frac{a}{s} \in U(A_P) \text{ акко постоје } b \in A \text{ и } t \in A \setminus P \text{ тако да је } \frac{a}{s} \cdot \frac{b}{t} = \frac{1}{1}.$$

Другим речима, $\frac{a}{s}$ је инвертибилан акко постоји $b \in A$ и $t \notin P$ за које је $ab = st$. Уколико $a \in P$, онда и $st = ab \in P$, па како је P прост идеал, следи да $s \in P$, или $t \in P$, што није могуће на основу избора s и t. А уколико $a \notin P$, онда је $\frac{s}{a} (\in A_P)$ инверз елемента $\frac{a}{s}$. Дакле,

$$A_P \setminus U(A_P) = \left\{ \frac{a}{s} \in A_P : a \in P \right\}.$$

Уверимо се да је ово заиста идеал у A_P.

Нека су x, y неинвертибилни елементи из A_P. То значи да постоје елементи $a, b \in P$ и $s, t \notin P$ за које је $x = \frac{a}{s}$ и $y = \frac{b}{t}$. Тада је $x + y = \frac{a}{s} + \frac{b}{t} = \frac{ta+sb}{st}$, но, како је P идеал, $ta + sb \in P$, па је заиста и елемент $x + y$ неинвертибилан. На сличан начин се показује да ако $x \in A_P$ нема инверз и ако је $z \in A_P$ произвољан, ни елемент zx нема инверз. Закључујемо да је $A_P \setminus U(A_P)$ заиста идеал, па је и прстен A_P локални прстен. □

За крај напоменимо да, уколико је $S = A \setminus \{0\}$, у прстену $S^{-1}A$ је сваки елемент различит од нуле инвертибилан, те је, у овом случају, $S^{-1}A$ једно поље. Ово поље се назива поље разломака домена A и означава са $Q(A)$. На овај начин смо показали да се сваки домен може утопити у неко поље. Као што видимо, ова је конструкција у потпуности аналогна конструкцији рационалних бројева као разломака над целим бројевима. Други важан пример имамо у случају прстена полинома, али ћемо се прво позабавити више овим прстеном.

Једнозначна факторизација у прстену полинома

У овом одељку, прстен A је прстен са једнозначном факторизацијом. Главни резултат у овом делу биће следећа теорема.

Теорема 116 Ако је A домен са једнозначном факторизацијом, онда је и $A[X]$ домен са једнозначном факторизацијом.

Но, ово није тако лако доказати, биће нам потребни неки припремни резултати. У даљем ћемо поље разломака домена A, тј. прстен $Q(A)$ означавати са K. То је заправо $S^{-1}A$, за $S = A \setminus \{0\}$.

Докажимо најпре следећу лему.

Лема 117 Ако је p прост елемент у A, онда је $\langle p\rangle \lhd A[X]$ прост идеал.

Доказ. Неопходно је да разликујемо идеал pA прстена A генерисан са p и идеал $pA[X]$ који је идеал у прстену $A[X]$. Овај потоњи идеал је горенаведени идеал $\langle p\rangle$. Пошто је p прост елемент у A, онда је, по ранијим резултатима, pA прост идеал у A и $A/_{pA}$ је домен. Ми треба да докажемо да је $A[X]/_{pA[X]}$ домен. Дефинишимо пресликавање $\varphi\colon A[X] \to (A/_{pA})[X]$ са:

$$\varphi(a_0 + a_1X + \cdots + a_nX^n) := \overline{a_0} + \overline{a_1}X + \cdots + \overline{a_n}X^n,$$

где са $\overline{a}$ означен елемент $a + pA$ прстена $A/_{pA}$. С обзиром да је пресликавање $a \mapsto \overline{a}$ епиморфизам (хомоморфизам који је „на" прстена A на прстен A/pA), лако се проверава да је φ такође један епиморфизам. Но, $a_0 + a_1X + \cdots + a_nX^n \in \mathrm{Ker}(\varphi)$ **акко** је $a_i = 0_{A/pA}$ за све i, тј. **акко** $p \mid a_i$ за све i. Но, у том случају је $a_i = pb_i$, за неке b_i, па је $a_0 + a_1X + \cdots + a_nX^n = p(b_0 + b_1X + \cdots + b_nX^n)$. Но, ово нам показује да је $\mathrm{Ker}(\varphi) = pA[X]$, те имамо изоморфизам $A[X]/_{pA[X]} \cong (A/_{pA})[X]$. Но, како је $A/_{pA}$ домен, то је и $(A/_{pA})[X]$ такође домен, те закључујемо да је $pA[X]$ заиста прост идеал. □

Дефиниција 118 За полином $a(X) = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ кажемо да је ПРИМИТИВАН уколико је $\mathrm{NZD}(a_0, a_1, \ldots, a_n) = 1$.

Лема 119 (Гаусова лема) Ако су $f, g \in A[X]$ примитивни, онда је и $f \cdot g$ примитиван.

Доказ. Довољно је доказати да не постоји прост елемент који дели сваки коефицијент полинома $f \cdot g$. У супротном, нека је p прост елемент који дели сваки коефицијент полинома $f \cdot g$. То значи да је онда

$$\varphi(f \cdot g) = 0 \in (A/_{pA})[X], \tag{38}$$

где је φ горенаведени епиморфизам. Но, како је f примитиван, онда p не може да дели све његове коефицијенте, тј. $\varphi(f) \neq 0$. Из истих разлога је $\varphi(g) \neq 0$. Но, како је $(A/_{pA})[X]$ домен, то је $\varphi(f) \cdot \varphi(g) \neq 0$, а $\varphi(f \cdot g) = \varphi(f) \cdot \varphi(g)$. Једначина (**38**) даје контрадикцију која завршава доказ. □

Лема 120 Нека је $f \in K[X] \setminus \{0\}$. Тада:

а) $f = c(f) \cdot f_0$, где је $f_0 \in A[X]$ примитиван полином, а $c(f) \in K$ је одређен до на инвертибилан елемент из A.

б) $c(f \cdot g) = u \cdot c(f) \cdot c(g)$, где је $u \in U(A)$.

Доказ. а) Нека је

$$f = \frac{a_0}{b_0} + \frac{a_1}{b_1}X + \cdots + \frac{a_n}{b_n}X^n,$$

где $a_i, b_i \in A$. Ако је $d = b_0 b_1 \cdots b_n$, онда је јасно да $df \in A[X]$. Како $d\frac{a_i}{b_i} \in A$, може се дефинисати

$$c = \text{NZD}\left(d\frac{a_0}{b_0}, d\frac{a_1}{b_1}, \ldots, d\frac{a_n}{b_n}\right).$$

Тада је полином $f_0 = \frac{d}{c}f \in A[X]$ примитиван полином и имамо да је $f = \frac{c}{d}f_0$. Докажимо јединственост оваквог представљања. Нека је $f = c_1 f_1 = c_2 f_2$, где су $c_1, c_2 \in K$, а f_1, f_2 примитивни. Уколико је $c_1 = \frac{p_1}{q_1}$, $c_2 = \frac{p_2}{q_2}$ онда из

$$\frac{p_1}{q_1}f_1 = \frac{p_2}{q_2}f_2,$$

множењем са $q_1 q_2$ добијамо

$$q_2 p_1 f_1 = q_1 p_2 f_2.$$

Како су f_1 и f_2 примитивни полиноми, то је $q_2 p_1$ највећи заједнички делилац коефицијената полинома $q_2 p_1 f_1$, а $q_1 p_2$ највећи заједнички делилац коефицијената полинома $q_1 p_2 f_2$. С обзиром да су ово једнаки полиноми, закључујемо да су $q_2 p_1$ и $q_1 p_2$ придружени елементи прстена A, тј. постоји $u \in U(A)$ тако да је $q_2 p_1 = u q_1 p_2$, те је $\frac{p_1}{q_1} = u\frac{p_2}{q_2}$, тј. $c_1 = u c_2$, за неки $u \in U(A)$.

б) Нека је $f = c(f)f_0$ и $g = c(g)g_0$, $h = f \cdot g = c(f \cdot g)h_0$, $f_0, g_0, h_0 \in A[X]$ примитивни полиноми. Тада је $f \cdot g = c(f)c(g)f_0 g_0$, где је $f_0 g_0$ примитиван по Гаусовој леми. Дакле,

$$c(f)c(g)f_0 g_0 = c(h)h_0.$$

На основу а) добијамо да је $c(f \cdot g) = u \cdot c(f) \cdot c(g)$, за неки $u \in U(A)$. □

Лема 121 Прости елементи у $A[X]$ су или прости елементи у A или примитивни полиноми из $A[X]$ који су нерастављиви у $K[X]$.

Доказ. Нека је $f \in A[X]$ прост елемент. Ако је $\deg f = 0$, онда је f прост елемент у A. Ако је $\deg f > 0$, онда f мора бити примитиван полином. Наиме, ако постоји p који је прост у A и који дели све коефицијенте полинома f, онда је $f = a_0 + a_1 X + \cdots + a_n X^n = p(b_0 + b_1 X + \cdots + b_n X^n)$ и f не би био нерастављив, па тиме ни прост. Поставља се питање: може ли f бити растављив у $K[X]$. Уколико би то било тако, тј. уколико би постојали неконстантни полиноми g и h тако да је $f = g \cdot h$, онда би, на основу претходне леме, важило да је $c(f) = u \cdot c(g) \cdot c(h)$, за неки $u \in U(A)$. Како је f примитиван полином,

то је $c(f) = 1$ (или је само инвертибилан у A, што не мења ништа) и имали бисмо да је $c(g) \cdot c(h) \in U(A)$. Тада је

$$f = c(g)g_0 \cdot c(h)h_0 = \underbrace{c(g) \cdot c(h)}_{\in U(A)} g_0 h_0$$

и добили бисмо да је f растављив у $A[X]$ што противречи претпоставци да је f прост елемент у $A[X]$. Тиме смо доказали да ако је f прост елемент у $A[X]$ који није константа, онда је он примитиван и нерастављив у $K[X]$.

Докажимо сада и други смер. Ако је f прост елемент у A, онда из леме **117** следи да је он прост и у $A[X]$. Претпоставимо сада да је f примитиван полином у $A[X]$ који је нерастављив у $K[X]$. Треба доказати да је он прост у $A[X]$. Претпоставимо да $f \mid g \cdot h$, за неке $g, h \in A[X]$. Како је f нерастављив у $K[X]$, а ово јесте прстен са јединственом факторизацијом и ту се прости и нерастављиви елементи подударају, онда $f \mid g$ у $K[X]$ или $f \mid h$ у $K[X]$. Нека $f \mid g$ у $K[X]$. тада је $g = k \cdot f$ за неки $k \in K[X]$. На основу леме **120** имамо да је $c(g) = c(k) \cdot c(f) \cdot u$, где је $u \in U(A)$. Како је f примитиван, то је $c(f) = 1$, па је $c(k) = c(g) \cdot u^{-1} \in A$, па је заправо $k \in A[X]$ и $f \mid g$ у $A[X]$, те је f прост елемент у $A[X]$. □

Сада најзад можемо доказати теорему **116**.

Доказ теореме 116. Знамо да је довољно доказати да се сваки елемент у $A[X] \setminus (U(A[X]) \cup \{0\})$ може приказати у облику производа простих елемената. Наравно, $U(A[X]) = U(A)$. Можемо наћи растав од f на нерастављиве у $K[X]$ за који знамо да постоји: $f = f_1 \cdots f_k$. Но, $f_i = c(f_i)g_i$ где је $c(f_i) \in K$, а g_i примитивни (а наравно да су нерастављиви у $K[X]$ јер су такви f_i). Дакле,

$$f = c(f_1) \cdots c(f_k) g_1 \cdots g_k.$$

Како су g_i примитивни у $A[X]$ и нерастављиви у $K[X]$, онда су они прости елементи у $A[X]$. Но, из горње једнакости следи да $c(f_1) \cdots c(f_k) \in A$, а како је A прстен са јединственом факторизацијом, могуће је наћи $d_1, \ldots, d_r$ који су прости у A (а тиме и прости у $A[X]$) такве да је $c(f_1) \cdots c(f_k) = d_1 \cdots d_r$ те смо најзад добили да је $f = d_1 \cdots d_r g_1 \cdots g_k$ и то је тражена факторизација од f у производ простих елемената из $A[X]$. □

Као последицу ове теореме имамо чињеницу да су прстени $\mathbb{Z}[X]$, $\mathbb{Z}[X, Y]$, $\mathbb{Z}[X, Y, Z]$ прстени са јединственом факторизацијом. Истакнимо још да смо доказали и да је примитиван полином у $\mathbb{Z}[X]$ нерастављив у $\mathbb{Z}[X]$ **акко** је нерастављив у $\mathbb{Q}[X]$

Приметимо да ако је $f \in A[X]$, онда $c(f) \in A$.

Став 122 Нека је A прстен са јединственом факторизацијом, K његово поље разломака и $f, g \in A[X]$. Тада је $\mathrm{NZD}(f, g) = \mathrm{NZD}(c(f), c(g)) \cdot d$, где је

$d \in A[X]$ примитивни полином у $A[X]$ који је највећи заједнички делилац полинома f и g у $K[X]$.

Доказ. Пре свега, знамо да је $A[X]$ прстен са једнозначном факторизацијом, те у њему свака два елемента имају највећи заједнички делилац. Докажимо најпре да је наведени полином заједнички делилац полинома f и g.

Како $d \,|\, f$ у $K[X]$, а тада и $\mathrm{NZD}(c(f), c(g)) \cdot d \,|\, f$ у $K[X]$ то је $f = \mathrm{NZD}(c(f), c(g)) \cdot d \cdot q$ за неки полином $q \in K[X]$. Добијамо да је $c(f) = \mathrm{NZD}(c(f), c(g))c(q)u$, за неки $u \in U(A)$, пошто је $c(d) = 1$, јер је d примитивни полином. Но, $\mathrm{NZD}(c(f), c(g)) \mid c(f)$, те можемо да скратимо тим елементом из A и добијамо да је $c(q) \in A$, те $q \in A[X]$ и наведени полином дели f у $A[X]$. На исти начин се показује да он дели и g у $A[X]$.

Нека је сада $D \in A[X]$ полином који дели и f и g у $A[X]$. Тада је $f = Dq_1$ у $A[X]$, те је $c(f) = c(D)c(q_1)v$ за неки $v \in U(A)$. То значи да $c(D) \mid c(f)$ у A, јер је $c(q_1)v \in A$. Такође, $c(D) \mid c(g)$ у A и добијамо да $c(D) \mid \mathrm{NZD}(c(f), c(g))$ у A. Ако искористимо приказ $D = c(D)D_0$, где је D_0 примитиван полином и чињеницу да $D \mid d$ у $K[X]$, јер је d највећи заједнички делилац ових полинома у $K[X]$, онда $D \mid \mathrm{NZD}(c(f), c(g))d$ у $K[X]$ и $\mathrm{NZD}(c(f), c(g))d = DQ$ у $K[X]$. Тада је $\mathrm{NZD}(c(f), c(g))c(d) = c(D)c(Q) \cdot w$, за неки $w \in U(A)$. Како $c(D) \mid \mathrm{NZD}(c(f), c(g))$ у A, то је $\mathrm{NZD}(c(f), c(g)) = c(D)a$, за неки $a \in A$ и добијамо да је $c(Q) = aw^{-1} \in A$. Стога је $Q \in K[X]$ и D дели наведени полином у $A[X]$. Стога он испуњава оба услова за највећи заједнички делилац и то завршава доказ овог става. □.

Уколико је A прстен са једнозначном факторизацијом, а K његово поље разломака, онда је поље разломака за прстен $A[X]$, заправо ПОЉЕ РАЦИОНАЛНИХ ФУНКЦИЈА у ознаци $K(X)$, дато са:

$$K(X) = \left\{ \frac{a(X)}{b(X)} : a(X), b(X) \in A[X], b(X) \neq 0 \right\}.$$

Наравно, овде је $\frac{a(X)}{b(X)}$ класа еквиваленције и

$$\frac{a(X)}{b(X)} = \frac{a_1(X)}{b_1(X)} \textbf{ акко је } a(X)b_1(X) = a_1(X)b(X).$$

Приметимо да је $K(X)$ истовремено и поље разломака за прстен $K[X]$. Наиме, инвертујући све не-нула полиноме из $A[X]$ ми смо инвертовали и све не-нуле елементе из A и тиме добили и K.

Илуструјмо став **122** примерима.

Пример 123 Наћи највећи заједнички делилац полинома $f(X) = 8X^5 + 8X^4 + 4X^3 + 4X^2 + 4X + 8$ и $g(X) = 18X^4 + 24X^3 + 12X^2 - 6X - 12$ у прстену $\mathbb{Z}[X]$.

Одредимо најпре $c(f)$ и $c(g)$ за наше полиноме.

$$c(f) = \text{NZD}(8,8,4,4,4,8) = 4, \quad c(g) = \text{NZD}(18,24,12,-6,-12) = 6$$

и добијамо да је $NZD(c(f), c(g)) = 2$. Следеће што треба да урадимо је да нађемо највећи заједнички делилац ових полинома, али у $\mathbb{Q}[X]$. Потом, пошто знамо да је највећи делилац одређен но на инвертибилан елемент, према ставу **122** треба да изаберемо полином који је примитиван у $\mathbb{Z}[X]$. Он наравно не мора бити моничан.

Како радимо са коефицијентима у пољу $\mathbb{Q}$, сви ненула цели бројеви су инвертибилни те је $\text{NZD}(ma(X), nb(X)) = \text{NZD}(a(X), b(X))$ за све целе бројеве m, n који нису једнаки нула. Поступак наравно изводимо Еуклидовим алгоритмом, али користећи ову идеју да бисмо поједноставили међурезултате. Како је $f(X) = 4(2X^5 + 2X^4 + X^3 + X^2 + X + 2)$, а $g(X) = 6(3X^4 + 4X^3 + 2X^2 - X - 2)$, то Еуклидов алгдеоритам можемо применити на ове примитивне полиноме у заградама. Дакле, требало би да започнемо дељењем полинома $2X^5 + 2X^4 + X^3 + X^2 + X + 2$ полиномом $3X^4 + 4X^3 + 2X^2 - X - 2$ у $\mathbb{Q}[X]$. Наравно, видимо да ћемо одмах добити разломак. Нема ничег лошег у разломцима, али ради лакше рачунице бисмо волели да их избегнемо. Видимо да то можемо ако први полином помножимо са 3. То ће свакако дати цео број као коефицијент на почетку, али се дељење не завршава у једном кораку пошто је разлика у степенима ова два полинома једнака 1. Стога се у другом кораку може појавити разломак. Зато је погодно први полином помножити са $3^2 = 9$.

Дакле, делимо полином $18X^5+18X^4+9X^3+9X^2+9X+18$ полиномом $3X^4+4X^3+2X^2-X-2$. То радимо стандардно и добијамо да је количник $6X - 2$, а остатак $5X^3 + 19X^2 + 19X + 14$. Сада полином $3X^4 + 4X^3 + 2X^2 - X - 2$ треба поделити полиномом $5X^3+19X^2+19X+14$. Да бисмо избегли разломке, први полином множимо са $5^2 = 25$.

Дакле, делимо полином $75X^4 + 100X^3 + 50X^2 - 25X - 50$ полиномом $5X^3 + 19X^2 + 19X + 14$. Добијамо количник $15X - 37$ и остатак $468X^2 + 468X + 468 = 468(X^2 + X + 1)$. Сада полином $5X^3 + 19X^2 + 19X + 14$ треба поделити полиномом $468(X^2 + X + 1)$, но наравно да ћемо га делити полиномом $X^2 + X + 1$. Када то урадимо, добијамо да је количник $5X + 14$, а остатак је једнак 0.

Еуклидов алгоритам нам за тражени највећи заједнички делилац даје последњи ненула остатак, а то је полином $468(X^2 + X + 1)$. Но, највећи заједнички делилац ће бити тада и полином $X^2 + X + 1$ и њега бирамо зато што је он примитиван полином у $\mathbb{Z}[X]$.

Коначно, $\text{NZD}(f, g) = 2(X^2 + X + 1)$ на основу става **122**. ♣

Пример 124 Наћи највећи заједнички делилац полинома $f(X, Y) = X^3 + X^2Y - 2XY^2 + XY + 2Y^2$ и $g(X, Y) = X^4 + 2X^3Y + XY^2 + X + 2Y^3 + 2Y$ у прстену $\mathbb{Z}[X, Y]$.

Да бисмо применили став **122**, представимо наше полиноме као полиноме у прстену $\mathbb{Z}[Y][X]$ (дакле, овде ће основни прстен бити $A =$

$\mathbb{Z}[Y]$) и означимо први са P, а други са Q:

$$P = X^3 + YX^2 + (-2Y^2 + Y)X + 2Y^2, Q = X^4 + 2YX^3 + (Y^2 + 1)X + 2Y^3 + 2Y.$$

Тада је $c(P) = \text{NZD}(1, Y, -2Y^2 + Y, 2Y^2) = 1$, а $c(Q) = \text{NZD}(1, 2Y, Y^1 + 1, 2Y^3 + 2Y) = 1$. Остаје да нађемо највећи заједнички делилац полинома P и Q у $\mathbb{Q}(Y)[X]$ и да изаберемо такав који је примитиван полином у $\mathbb{Z}[Y][X]$ (поље разломака прстена $\mathbb{Z}[Y]$ је поље $\mathbb{Q}(Y)$).

Поделимо полином Q полиномом P. Добијамо количник $X + Y$ и остатак $(Y^2 - Y)X^2 + (2Y^3 - 2Y^2 + 1)X + 2Y$. Сада би полином P требало поделити овим остатком. Да би се избегли разломци, као у претходном, делићемо полином $(Y^2 - Y)^2 P$ тим остатком. После доста рачунања добијамо да је количник $(Y^2 - Y)X - Y^3 + Y^2 - 1$, а остатак $(Y^5 - 2Y^4 + 2Y^3 - Y^2 + 1)X + (2Y^6 - 4Y^5 + 4Y^4 - 2Y^3 + 2Y)$. Није тешко видети да је овај полином шестог степена по Y заправо производ полинома петог степена по Y и $2Y$, те је остатак $(Y^5 - 2Y^4 + 2Y^3 - Y^2 + 1)(X + 2Y)$ и у даљем рачуну можемо користити $X + 2Y$ (пошто је сваки ненула полином по Y инвертибилан у $\mathbb{Q}(Y)$).

Остало је да се полином $(Y^2 - Y)X^2 + (2Y^3 - 2Y^2 + 1)X + 2Y$ подели полиномом $X + 2Y$. Но, добијамо да је заправо $(Y^2 - Y)X^2 + (2Y^3 - 2Y^2 + 1)X + 2Y = (X + 2Y)((Y^2 - Y)X + 1)$. Дакле, последњи ненула остатак је $X + 2Y$ и добијамо да је то заправо највећи заједнички делилац датих полинома. ♣

Докажимо на крају овог дела и познати Ајзенштајнов критеријум за нерастављивост полинома из $\mathbb{Z}[X]$ у прстену $\mathbb{Q}$.

Став 125 (Ајзенштајнов критеријум) Нека је A прстен са једнозначном факторизацијом, K његово поље разломака и $f = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ такав да постоји прост елемент $p \in A$ за који важи:

1. $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}, p \nmid a_n$;
2. $p^2 \nmid a_0$,

онда је f нерастављив у $K[X]$.

Доказ. Претпоставимо да је $f = g \cdot h$ у $K[X]$, при чему је $\deg g, \deg h < \deg f$. Тада је $c(f) = c(g)c(h)u$, за неки $u \in U(A)$. Како је $f \in A[X]$, то је $c(g)c(h) \in A$ и добијамо да је $f = c(g)g_0c(h)h_0 = g_1h_0$, при чему је $g_1 = c(g)c(h)g_0 \in A[X]$. Дакле, имамо факторизацију $f = g_1h_1$ и у $A[X]$.

Искористимо сада хомоморфизам φ из доказа леме **117**. Ако са $\overline{a}$ означимо слику елемента a у $A/_{pA}[X]$, онда имамо да је $\overline{f} = \overline{a_n}X^n$, а како је $f = g_1h_1$, онда је $\overline{a_n}X^n = \overline{g_1}\overline{h_1}$, из чега следи да је $\overline{g_1} = \overline{c}X^k$, а $\overline{h_1} = \overline{d}X^{n-k}$. Но, то значи да је сваки коефицијент полинома g_1 и f_1, сем најстаријег, дељив са p. Посебно су и слободни чланови дељиви са p, па је a_0 дељив са p^2 што противречи претпоставци. Стога закључујемо да је f нерастављив у $K[X]$. □

Пример 126 Нека је p прост број. Доказати да је полином $a(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$ нерастављив у $\mathbb{Q}[X]$.

Јасно је да је полином $a(X)$ нерастављив **акко** је нерастављив полином $a(X+1)$. Наиме, ако би полином $a(X+1)$ био растављив, онда би било $a(X+1) = b(X)c(X)$, за неке полиноме $a(X)$ и $b(X)$, но из овога следи да је $a(X) = b(X-1)c(X-1) = a_1(X)b_1(X)$. 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 $p \mid \binom{p}{k}$, а $p^2 \nmid p$ и $p \nmid 1$, то је полином $a(X+1)$ нерастављив по Ајзенштајновом критеријуму. ♣

За испитивање нерастављивости је корисна и провера да ли полином из $A[X]$ има нулу у K. Ево става који нам у томе помаже.

Став 127 Нека је $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$, где је A прстен са једнозначном факторизацијом. Уколико су $b, c \in A$ такви да је $c \neq 0$, $\mathrm{NZD}(b,c) = 1$ и $f(b/c) = 0$, онда $b \mid a_0$ и $c \mid a_n$. Посебно, ако је $f(X)$ моничан полином, онда је свака нула тог полинома која се налази у K заправо у A.

Доказ. Ако је $f(b/c) = 0$, онда имамо

$$a_n \left(\frac{b}{c}\right)^n + a_{n-1} \left(\frac{b}{c}\right)^{n-1} \cdots + a_1 \left(\frac{b}{c}\right) + a_0 = 0.$$

Множењем са c^n добијамо

$$a_n b^n + a_{n-1} b^{n-1} c + \cdots + a_1 b c^{n-1} + a_0 c^n = 0.$$

Одавде добијамо да $b \mid a_0 c^n$, а $c \mid a_n b^n$. Из чињенице да је $\mathrm{NZD}(b,c) = 1$ следи да је и $\mathrm{NZD}(b, c^n) = 1$, те, као и раније, закључујемо да $b \mid a_0$. На аналоган начин добијамо да $c \mid a_n$. Ако је $f(X)$ моничан полином, тј. ако је $a_n = 1$, онда из $c \mid a_n$ следи да је $c \in U(A)$, те је $b/c \in A$. □

– Крај курса –