АЛГЕБРА 3

ПРЕДАВАЊА

ЗОРАН ПЕТРОВИЋ

ШКОЛСКА 2023/24 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.

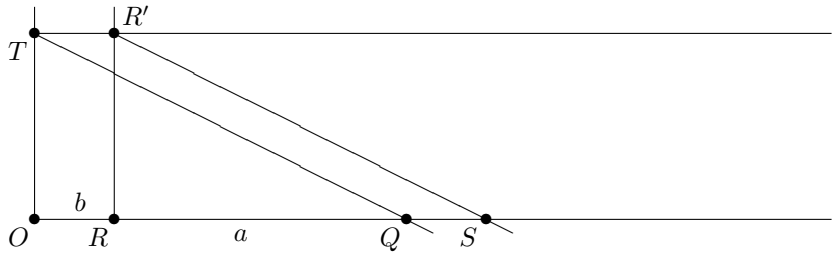
Тачке у равни можемо да видимо и као комплексне бројеве на стандардан начин.

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 $a \neq 0$.

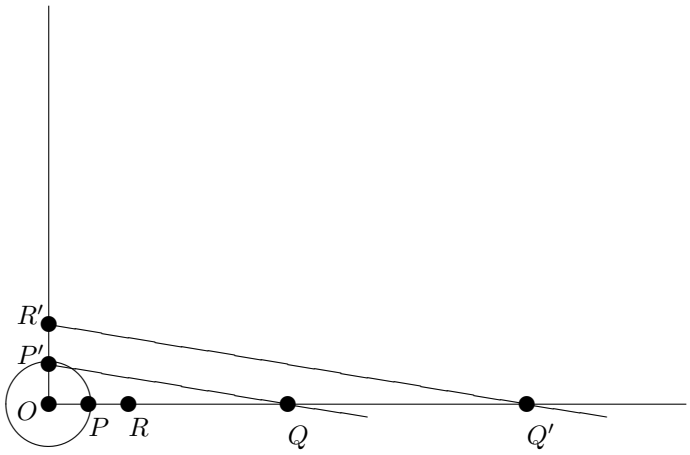
Није тешко уверити се да је довољно ово показати када имамо позитивне реалне бројеве (негативни бројеви само уводе више случајева). Конструкција броја $a + b$ дата је следећим цртежом.



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).



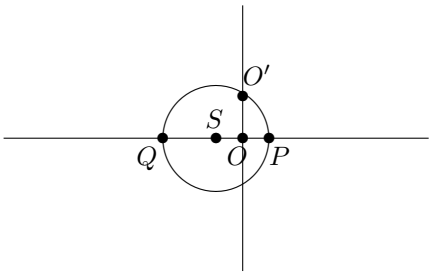
Постављамо кругове са центром у O који пролазе кроз тачке P (која одговара броју 1) и тачку R (која одговара броју b). У пресеку добијамо тачке P' и R' на вертикалној оси. Права кроз R' паралелна правој кроз тачке P' и Q сече хоризонталну осу у тачки Q' и та тачка одговара тачки $a \cdot b$. Наиме, правоугли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

Наведимо сада најважнију теорему у овом одељку.

Теорема 5 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 6 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 $s \geq 1$. ♠

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

Став 7 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 $\cos 20^\circ$. Докажимо то.

Став 8 Број $\cos 20^\circ$ 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 $\varphi = 20^\circ$ добијамо

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

Дакле,

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

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 Напредније питања

Следећи резултат је нешто тежи за доказ.

Став 9 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 10 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 11 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 12 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 13 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 14 Просто поље је поље које нема правих потпоља.

Став 15 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 јединичку 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 16 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 17 Нека је K поље карактеристике 0 и $\varphi \in \mathrm{Aut}(K)$. 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 18 Нека је $K = \mathbb{Q}(\sqrt[3]{2})$. Одредити групу $\mathrm{Aut}(K)$.

Нека је $\varphi \in \mathrm{Aut}(K)$. Знамо да по ставу **17** 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 19 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 раставља („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 20 Коначно раширење F поља K је нормално ако и само ако је оно коренско поље неког полинома p из $K[X]$.

Доказ става 20. $\Longleftarrow$: 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 $p = \mu_{\alpha_1} \cdots \mu_{\alpha_n}$. □

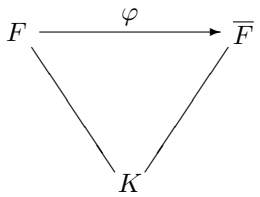
Дефиниција 21 Ако је L раширење поља K, онда је НОРМАЛНО ЗАТВОРЕЊЕ поља L најмање раширење $\overline{L}$ поља L тако да је раширење $\overline{L}/K$ нормално.

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:

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

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 22 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 23 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.

Дефиниција 24 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.

Дефиниција 25 Поље K је САВРШЕНО ако је $\operatorname{char} K = 0$ или је $\operatorname{char} K = p$ и $K^p = \{x^p : x \in K\} = K$.

Савршена поља коначне карактеристике постоје. На пример, то су сва коначна поља.

Став 26 Свако коначно поље је савршено.

Доказ. Нека је K коначно поље и $\operatorname{char} K = p$. Посматрајмо пресликавање $\varphi\colon K \to K$ задато са; $\varphi(x) = x^p$. Јасно је да је $\varphi(1_K) = 1_K^p = 1_K$ и да је $\varphi(x \cdot y) = (x \cdot y)^p = x^p \cdot y^p = \varphi(x) \cdot \varphi(y)$. Но, имамо да је и $\varphi(x + y) = (x + y)^p = x^p + y^p$, пошто су сви остали чланови у биномном развоју једнаки нули јер су ти коефицијенти сви дељиви са p, као што смо већ напоменули раније. Дакле, φ је ендоморфизам поља K, а сваки је ендоморфизам поља нужно и мономорфизам. Но, како је поље K коначно, то је φ и „на" те за свако $y \in K$ постоји $x \in K$ тако да је $\varphi(x) = y$, тј. $x^p = y$. Закључујемо да је K савршено. □

Напомена 27 Аутоморфизам $\varphi\colon K \to K$ поља карактеристике p задат са $\varphi(x) = x^p$ зове се ФРОБЕНИЈУСОВ АУТОМОРФИЗАМ поља K. Дакле, у сваком савршеном пољу постоји Фробенијусов аутоморфизам. ♠

Теорема 28 Нека је L/K алгебарско раширење савршеног поља K. Тада је то раширење сепарабилно, а поље L је и само савршено.

Доказ. Нека је L алгебарско раширење поља K карактеристике 0 и $\alpha \in L$. Ако је $\mu_\alpha \in K[X]$ његов минимални полином (за минималне полиноме ћемо увек претпостављати да су монични) степена n, онда је водећи члан полинома μ'_α једнак nX^{n-1} и он није једнак нули, јер је и L карактеристике 0. Стога је раширење L/K сепарабилно.

Нека је сада L алгебарско раширење савршеног поља K, при чему је $\operatorname{char} K = p$, $\alpha \in L$ и $\mu_\alpha \in K[X]$ његов минимални полином. Ако је $\mu_\alpha = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ и $\mu'_\alpha = 0$, онда је $ma_m = 0$ за свако $m \in \{0, \ldots, n\}$. То значи

$$\text{за свако } m \in \{0, \ldots, n\} : m1_K = 0 \text{ или } a_m = 0.$$

Дакле, ако је $a_m \neq 0$, онда $p \mid m$. Другим речима, полином μ_α је облика:

$$\mu_\alpha = X^{ps} + a_{p(s-1)}X^{p(s-1)} + \cdots + a_0.$$

Како је K савршено поље, то постоје елементи $b_i \in K$ такви да је $b_i^p = a_{pi}$ за све $0 \leq i < p$. Добијамо да је

$$\mu_\alpha = (X^s)^p + b_{s-1}^p (X^{s-1})^p + \cdots + b_0^p = \left(X^s + b_{s-1}X^{s-1} + \cdots + b_0\right)^p,$$

што није могуће, јер је μ_α нерастављив у K као минимални полином елемента $\alpha \in L$. Дакле, $\mu'_\alpha \neq 0$ те је раширење L/K сепарабилно.

Докажимо да је L савршено поље. Да бисмо то доказали, можемо да претпоставимо да је L/K коначно раширење. Наиме, пошто желимо да покажемо да је сваки елемент α облика β^p за неко β, довољно је да посматрамо раширење $K(\alpha)/K$, које је коначно. Дакле, у даљем посматрамо коначно раширење L/K.

Приметимо да је M^p потпоље од M, за свако поље M карактеристике p. Посебно је то тачно и за поље L. Такође је и L^p векторски простор над K^p (ако је L/K раширење поља карактеристике p). Докажимо да је

$$[L : K] \leq [L^p : K^p].$$

Нека је $[l_1, \ldots, l_n]$ база за L над K. Покажимо да су $l_1^p, \ldots, l_n^p$ линеарно независни над K^p. Уколико је

$$\alpha_1^p l_1^p + \cdots + \alpha_n^p l_n^p = 0,$$

онда је $(\alpha_1 l_1 + \cdots + \alpha_n l_n)^p = 0$ те добијамо да је $\alpha_1 l_1 + \cdots + \alpha_n l_n = 0$, што, из линерне независности $l_1, \ldots, l_n$, даје $\alpha_1 = \cdots = \alpha_n = 0$. Сада имамо да је

$$[L : K] \leq [L^p : K^p] \quad \overset{K \text{ је савршено}}{=\!=\!=} \quad [L^p : K] \leq [L : K].$$

Последња неједнакост важи, јер је L^p потпоље поља L. Закључујемо да је $[L : K] = [L^p : K]$, а како је L/K коначно раширење и L^p потпоље од L, то мора бити $L^p = L$, те је поље L савршено. □

Неки аутори дефинишу савршена поља као она поља чија су сва алгебарска раширења сепарабилна. Следећи став, уз све што је до сада речено, оправдава ту алтернативну дефиницију.

Став 29 Нека је K поље карактеристике p такво да је свако алгебарско раширење L/K сепарабилно. Тада је K савршено поље.

Доказ. Нека је $\alpha \in K$. Посматрајмо полином $f(X) = X^p - \alpha \in K[X]$. Нека је L коренско поље полинома $f(X)$ и $\beta \in L$ један корен овог полинома. Тада је $\beta^p - \alpha = 0$. Добијамо да је

$$f(X) = X^p - \alpha = X^p - \beta^p = (X - \beta)^p.$$

Како је, по претпоставци, L/K сепарабилно раширење, то је минимални полином елемента β, $\mu_\beta \in K[X]$ сепарабилан, тј. све његове нуле

су просте. Но, како $\mu_\beta \mid (X-\beta)^p$, закључујемо да је $\mu_\beta = X - \beta$, па $\beta \in K$ и $\alpha \in K^p$. Како је α био произвољан елемент из K закључујемо да је $K^p = K$ и поље K је савршено. □

Наравно, нису сва поља савршена.

Пример 30 Поље $\mathbb{F}_p(X) = \left\{ \frac{a(X)}{b(X)} : a(X), b(X) \in \mathbb{F}_p[X], b(X) \neq 0 \right\}$ је пример несавршеног поља.

Покажимо да у овом пољу једначина $x^p = X$ нема решења. Доказ је практично идентичан доказу да $\sqrt{2}$ није рационалан број. Наиме, ако би постојали узајамно прости полиноми $a(X), b(X) \in \mathbb{F}_p[X]$ такви да је

$$\left(\frac{a(X)}{b(X)}\right)^p = X,$$

онда би следило да је

$$(a(X))^p = (b(X))^p X \tag{12}$$

у $\mathbb{F}_p[X]$ и, како је X нерастављив, па тиме и прост, добили бисмо да $X \mid a(X)$. Дакле, $a(X) = a_1(X)X$. Заменом у **(12)** добијамо

$$(a_1(X))^p X^p = (b(X))^p X. \tag{13}$$

После скраћивања добијамо

$$(a_1(X))^p X^{p-1} = (b(X))^p, \tag{14}$$

одакле следи и да $X \mid b(X)$, што противречи претпоставци да су $a(X)$ и $b(X)$ узајамно прости. ♣

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 31 Ако је у коначном раширењу $L = K(\alpha_1, \ldots, \alpha_n)$ сваки елемент α_i сепарабилан над K, онда постоји $\lambda \in L$ такав да је $L = K(\lambda)$. Посебно, свако коначно раширење савршеног поља је просто.

Доказ. 1) Нека је K коначно поље. У том случају је и L, као његово коначно раширење, такође коначно поље и група $(L\setminus\{0\}, \cdot)$ је циклична. Дакле, постоји $\lambda \in L$ такав да је $L \setminus \{0\} = \{\lambda^k : 0 \leq k \leq |L| - 2\}$. Јасно је да је онда $L = K(\lambda)$.

2) Нека 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

$$f_c(\beta_r) = 0 \text{ акко } \mu_\alpha(\alpha + c(\beta - \beta_r)) = 0 \tag{15}$$

$$\text{акко } \alpha + c(\beta - \beta_r) = \alpha_s \text{ за неко } s \geq 2 \tag{16}$$

$$\text{акко } c = \frac{\alpha_s - \alpha}{\beta - \beta_r} \text{за неко } s \geq 2. \tag{17}$$

Посматрајмо скуп

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

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

$$\mathrm{NZD}(f_{c_0}, \mu_\beta) \in E_{c_0}[X]. \tag{18}$$

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 **(18)** 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 $\lambda = \alpha + c_0\beta$. □

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 32 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 33 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 $G(L/K) \leq \operatorname{Aut} L$. Ако је пак $\Pi \leq \operatorname{Aut} L$, 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 34 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 $\Pi \leq \operatorname{Aut} L$.

(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 $p = c_0 + c_1 X + \cdots + c_{n-1}X^{n-1} \in K[X]$: $a = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$. 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 35 За коначно раширење L поља K кажемо да је Галоаово уколико је $K = L^{G(L/K)}$.

Дакле, доказали смо следећу теорему.

Теорема 36 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 37 (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

$$\begin{aligned} \big[L : F\big] &= \big|F^{\sharp}\big| \qquad (19) \\ \big[L : \Pi^{\flat}\big] &= \big|\Pi\big|. \qquad (20) \end{aligned}$$

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 **(19)** 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:

$$|\Pi| \leq \deg M_\alpha. \qquad (21)$$

Посматрајмо сад полином

$$q(X) = \prod_{\pi\in\Pi}(X - \pi(\alpha)). \qquad (22)$$

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

$$\deg M_\alpha \leq \deg q(X) = |\Pi|. \tag{23}$$

Из **(21)** и **(23)** добијамо да је $\deg M_\alpha = |\Pi|$, а како је $\deg M_\alpha = [L : \Pi^\flat]$ доказали смо **(20)**.

Коришћењем **(19)** и **(20)** није тешко доказати да је $\Pi = \Pi^{\flat\sharp}$ и $F = F^{\sharp\flat}$. Наиме:

$$\big|\Pi\big| \overset{\textbf{(20)}}{=\!=} \big[L : \Pi^\flat\big] \overset{\textbf{(19)}}{=\!=} \big|\Pi^{\flat\sharp}\big|.$$

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

$$\big[L : F\big] \overset{\textbf{(19)}}{=\!=} \big|F^\sharp\big| \overset{\textbf{(20)}}{=\!=} \big[L : F^{\sharp\flat}\big].$$

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 **(22)**. 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 38 (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 **(20)**, 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 39 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,

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

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

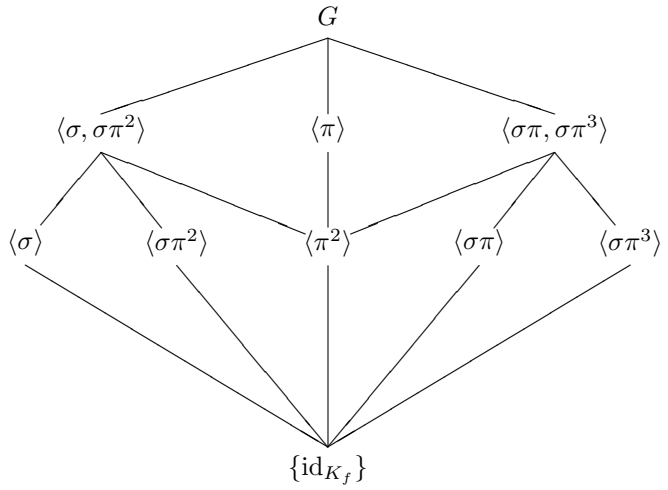
$$\pi^4(\sqrt[4]{2}) = \pi(-i\sqrt[4]{2}) = -\pi(i)\pi(\sqrt[4]{2}) = -i \cdot i\sqrt[4]{2} = \sqrt[4]{2}.$$

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

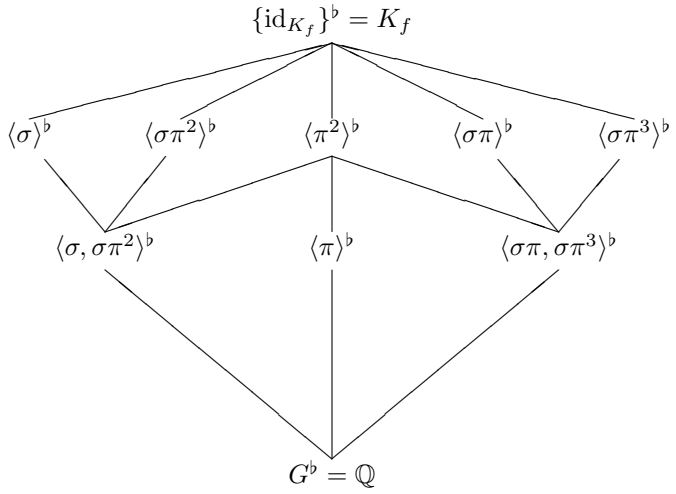
$$i \overset{\pi}{\longmapsto} i \overset{\sigma}{\longmapsto} -i, \quad \sqrt[4]{2} \overset{\pi}{\longmapsto} i\sqrt[4]{2} \overset{\sigma}{\longmapsto} -i\sqrt[4]{2},$$

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

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 **(20)** 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:

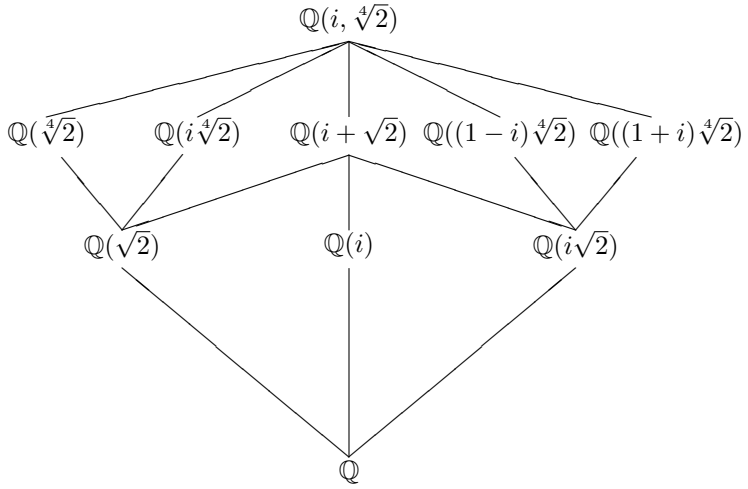
$$\langle \sigma\pi^2 \rangle^\flat = \mathbb{Q}(x_2) = \mathbb{Q}(i\sqrt[4]{2}).$$

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 40 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:

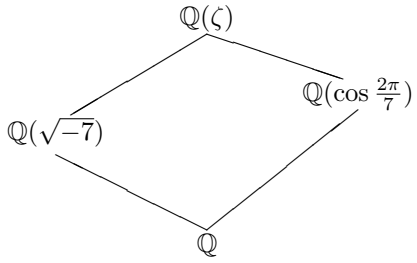
$$a = a - d, \quad b = e - d, \quad c = b - d, \quad d = f - d, \quad e = c - d, \quad f = -d.$$

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 41 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

$$\tau\sigma = \sigma^2\tau. \tag{24}$$

Из **(24)** индукцијом се лако показује да је

$$\tau\sigma^k = \sigma^{2k}\tau. \tag{25}$$

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

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

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

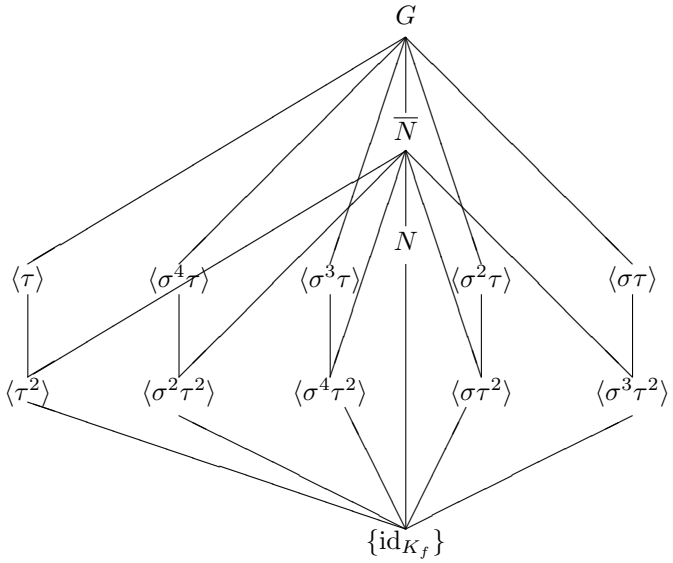
$$\sigma^3\tau^2\sigma^{-3} = (\sigma^3\tau\sigma^{-3})^2 = (\sigma^2\tau)^2 = \sigma^2\tau\sigma^2\tau = \sigma^2\sigma^4\tau\tau = \sigma\tau^2;$$

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

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:

$$\zeta^2 + \zeta + 1 + \frac{1}{\zeta} + \frac{1}{\zeta^2} = 0. \tag{26}$$

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 **(26)** добијамо да је

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

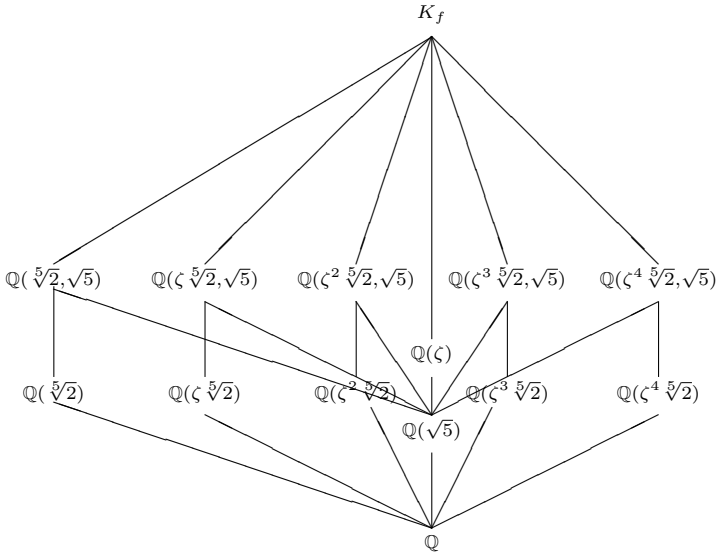
Одавде је $\xi \in \{\frac{-1\pm\sqrt{5}}{2}\}$. Дакле, $\overline{N}^\flat = \mathbb{Q}(\xi) = \mathbb{Q}(\sqrt{5})$.

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]:

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

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

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



♣

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

7 Независност карактера и Артинова лема

Дефиниција 42 Нека је G група и F поље. Карактер групе G је хомоморфизам $\chi\colon G \to F^\times$.

Наравно, $F^\times = F \setminus \{0\}$ и то је мултипликативна група. Алтернативна ознака, која се користи и за опште комутативне прстене R са јединицом је $U(R)$.

Напомена 43 Приметимо да карактери „не виде" некомутативност у групи, јер је за сваки карактер χ и групу G: $\chi([G,G]) = 1_F$, пошто је поље F комутативно. ♠

Теорема 44 Нека је G група и F поље. Сваки коначан скуп карактера $\{\chi_1, \ldots, \chi_m\}$, где $\chi_i \colon G \to F^\times$, је линеарно независан над F као скуп функција из G у F.

Доказ. Нека су $a_i \in F$ такви да је

$$a_1\chi_1 + \cdots + a_m\chi_m = 0 \colon G \to F.$$

Треба доказати да је $a_i = 0_F$ за све i. Доказ радимо индукцијом по m. Уколико је $m = 1$, онда имамо да је $a_1\chi_1$ заправо нула функција те је $a_1\chi_1(g) = 0$ за све $g \in G$. Посебно, $a_1\chi_1(e) = 0$, где је e неутрал групе G. Но, свакако је $\chi_1(e) = 1_F$ и добијамо да је $a_1 = 0_F$.

Претпоставимо да је тврђење доказано за скупове са m карактера и посматрамо скуп $\{\chi_1, \ldots, \chi_m, \chi_{m+1}\}$. Нека је, дакле,

$$a_1\chi_1 + \cdots + a_m\chi_m + a_{m+1}\chi_{m+1} = 0. \tag{27}$$

То значи да је за свако $g \in G$:

$$a_1\chi_1(g) + \cdots + a_m\chi_m(g) + a_{m+1}\chi_{m+1}(g) = 0_F. \tag{28}$$

Како је $\chi_1 \neq \chi_{m+1}$, то постоји $g_0 \in G$ тако да је $\chi_1(g_0) \neq \chi_{m+1}(g_0)$. Нека је $g \in G$ произвољан елемент групе. Тада је

$$a_1\chi_1(g_0g) + \cdots + a_m\chi_m(g_0g) + a_{m+1}\chi_{m+1}(g_0g) = 0_F. \tag{29}$$

С обзиром да су χ_i хомоморфизми, добијамо:

$$a_1\chi_1(g_0)\chi_1(g) + \cdots + a_m\chi_m(g_0)\chi_m(g) + a_{m+1}\chi_{m+1}(g_0)\chi_{m+1}(g) = 0_F. \tag{30}$$

Множењем **(28)** са $\chi_{m+1}(g_0)$ добијамо

$$a_1\chi_{m+1}(g_0)\chi_1(g) + \cdots + a_m\chi_{m+1}(g_0)\chi_m(g) + a_{m+1}\chi_{m+1}(g_0)\chi_{m+1}(g) = 0_F. \tag{31}$$

Одузимањем **(31)** од **(30)**добијамо

$$a_1(\chi_1(g_0) - \chi_{m+1}(g_0))\chi_1(g) + \cdots + a_m(\chi_m(g_0) - \chi_{m+1}(g_0))\chi_m(g) = 0_F. \tag{32}$$

Ако уведемо ознаке $b_i = a_i(\chi_i(g_0) - \chi_{m+1}(g_0))$ онда имамо да је за све $g \in G$:

$$b_1\chi_1(g) + \cdots + b_m\chi_m(g) = 0_F, \tag{33}$$

односно

$$b_1\chi_1 + \cdots + b_m\chi_m = 0_F, \tag{34}$$

пошто једнакост **(33)** важи за све $g \in G$. На основу индуктивне хипотезе, закључујемо да је $b_i = 0_F$ за све i. Посебно је $b_1 = 0$, а онда из чињенице да је $\chi_1(g_0) \neq \chi_{m+1}(g_0)$ следи да је $a_1 = 0_F$. Заменом у **(27)** добијамо

$$a_2\chi_2 + \cdots + a_{m+1}\chi_{m+1} = 0, \tag{35}$$

а онда поновном применом индуктивне хипотезе, добијамо да је и $a_2 = \cdots = a_{m+1} = 0$, што и завршава доказ. □

Последица 45 Нека су F и E поља и $\sigma_1, \ldots, \sigma_m \colon F \to E$ различити хомоморфизми. Тада су они линеарно независни као функције из F у E.

Доказ. Рестрикција хомоморфизма $\sigma_i \colon F \to E$ на $F^\times$ задаје карактер $\chi_i \colon F^\times \to E^\times$. Применом претходне теореме резултат следи. □

Претходни део је за први колоквијум.

Последица 46 Нека је L коначно раширење поља K степена m и Ω произвољно раширење поља K. Ако је $[\alpha_1, \ldots, \alpha_m]$ база за векторски простор L над K, а $\sigma_1, \ldots, \sigma_m \colon L \to \Omega$ различити K-хомоморфизми, онда је матрица $A = [\sigma_i(\alpha_j)]$ инвертибилна.

Доказ. Претпоставимо супротно, тј. нека ова матрица није инвертибилна. То значи да су њене врсте линеарно зависне над Ω, тј. постоје $c_i \in \Omega$ такви да је

$$c_1 A_{1\to} + c_2 A_{2\to} + \cdots + c_m A_{m\to} = \mathbf{0}.$$

Ако ово „распишемо", добијамо:

$$\begin{array}{ccccccccccc}
c_1\sigma_1(\alpha_1) & + & c_2\sigma_2(\alpha_1) & + & \cdots & + & c_m\sigma_m(\alpha_1) & = & 0_\Omega & (1)\\
c_1\sigma_1(\alpha_2) & + & c_2\sigma_2(\alpha_2) & + & \cdots & + & c_m\sigma_m(\alpha_2) & = & 0_\Omega & (2)\\
\vdots & & \vdots & & \ddots & & \vdots & & \vdots & \vdots\\
c_1\sigma_1(\alpha_m) & + & c_2\sigma_2(\alpha_m) & + & \cdots & + & c_m\sigma_m(\alpha_m) & = & 0_\Omega & (m).
\end{array}$$

Нека је α произвољан елемент из L. Како је $[\alpha_1, \alpha_2, \ldots, \alpha_m]$ база за L над K, то постоје $a_1, a_2, \ldots, a_m \in K$ такви да је

$$\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m. \tag{36}$$

Ако једначину (1) помножимо са a_1, једначину (2) са a_2, итд. и све добијене једначине саберемо, добићемо, имајући у виду да је, на пример,

$a_1\sigma_1(\alpha_1) = \sigma_1(a_1\alpha_1)$, јер је σ_1 један K-хомоморфизам, као и једнакост **(36)**, да је:

$$c_1\sigma_1(\alpha) + c_2\sigma_2(\alpha) + \cdots + c_m\sigma_m(\alpha) = 0_\Omega. \tag{37}$$

Како је ово тачно за свако $\alpha \in L$, добијамо да је

$$c_1\sigma_1 + c_2\sigma_2 + \cdots + c_m\sigma_m = 0\colon L \to \Omega,$$

при чему нису сви c_i једнаки 0_Ω, што противречи последици **45**. Ова контрадикција нам завршава доказ. □

Следећа лема ће нам користити у наредном одељку.

Лема 47 (Артинова лема) Нека је G коначна група аутоморфизама поља L. Тада је $[L : L^G] \leq |G|$.

Доказ. Нека је $K' = L^G$, $G = \{\sigma_1, \ldots, \sigma_m\}$, $\sigma_1 = \mathrm{id}_L$. Довољно је доказати да је сваки подскуп од L у коме има више од m елемената линеарно зависан над K'. Нека је $\{\alpha_1, \ldots, \alpha_n\} \subseteq L$, где је $n > m$, а $\alpha_i \neq \alpha_j$ за $i \neq j$. Посматрајмо систем једначина

$$\begin{array}{ccccccccccc} \sigma_1(\alpha_1)x_1 & + & \sigma_1(\alpha_2)x_2 & + & \cdots & + & \sigma_1(\alpha_n)x_n & = & 0_L \\ \sigma_2(\alpha_1)x_1 & + & \sigma_2(\alpha_2)x_2 & + & \cdots & + & \sigma_2(\alpha_n)x_n & = & 0_L \\ \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\ \sigma_m(\alpha_1)x_1 & + & \sigma_m(\alpha_2)x_2 & + & \cdots & + & \sigma_m(\alpha_n)x_n & = & 0_L. \end{array} \tag{38}$$

С обзиром на то да је $n > m$, овај систем једначина има нетривијална решења. Нека је $(b_1, \ldots, b_n) \in L^n$ неко нетривијално решење. То значи да нису сви b_i једнаки 0. Нека је, на пример, $b_1 \neq 0$. Како је систем хомоген, то је и $(\alpha b_1, \ldots, \alpha b_n)$ такође решење за ма које α. Између осталог, можемо да постигнемо да ПРВА компонента у нетривијалном решењу буде МА КОЈИ елемент из L. Како су $\sigma_1, \ldots, \sigma_m$ линеарно независни на основу последице **45**, то сигурно $\sigma_1 + \cdots + \sigma_m$ није нула пресликавање. Дакле, постоји неки $c_1 \in L$ такав да је $\sigma_1(c_1) + \cdots + \sigma_m(c_1) \neq 0_L$. Нека је $\alpha = c_1/b_1$ и $(c_1, \ldots, c_n) = (\alpha b_1, \ldots, \alpha b_n)$. Дакле

$$\begin{array}{ccccccccccc} \sigma_1(\alpha_1)c_1 & + & \sigma_1(\alpha_2)c_2 & + & \cdots & + & \sigma_1(\alpha_n)c_n & = & 0_L \\ \sigma_2(\alpha_1)c_1 & + & \sigma_2(\alpha_2)c_2 & + & \cdots & + & \sigma_2(\alpha_n)c_n & = & 0_L \\ \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\ \sigma_m(\alpha_1)c_1 & + & \sigma_m(\alpha_2)c_2 & + & \cdots & + & \sigma_m(\alpha_n)c_n & = & 0_L. \end{array} \tag{39}$$

Ако **(39)** „нападнемо” аутоморфизмом σ_i, добијамо

$$\begin{array}{ccccccccccc} (\sigma_i\circ\sigma_1)(\alpha_1)\sigma_i(c_1) & + & (\sigma_i\circ\sigma_1)(\alpha_2)\sigma_i(c_2) & + & \cdots & + & (\sigma_i\circ\sigma_1)(\alpha_n)\sigma_i(c_n) & = & 0_L \\ (\sigma_i\circ\sigma_2)(\alpha_1)\sigma_i(c_1) & + & (\sigma_i\circ\sigma_2)(\alpha_2)\sigma_i(c_2) & + & \cdots & + & (\sigma_i\circ\sigma_2)(\alpha_n)\sigma_i(c_n) & = & 0_L \\ \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\ (\sigma_i\circ\sigma_m)(\alpha_1)\sigma_i(c_1) & + & (\sigma_i\circ\sigma_m)(\alpha_2)\sigma_i(c_2) & + & \cdots & + & (\sigma_i\circ\sigma_m)(\alpha_n)\sigma_i(c_n) & = & 0_L. \end{array} \tag{40}$$

Но, како је $\{\sigma_i \circ \sigma_1, \ldots, \sigma_i \circ \sigma_m\} = \{\sigma_1, \ldots, \sigma_m\}$, то закључујемо да је и $(\sigma_i(c_1), \ldots, \sigma_i(c_n))$ такође (нетривијално) решење почетног система. Систем **(38)** је хомоген систем, па је и збир свака два решења такође решење. Посебно, то значи да је и

$$\left(\sum_{i=1}^{m} \sigma_i(c_1), \sum_{i=1}^{m} \sigma_i(c_2), \ldots, \sum_{i=1}^{m} \sigma_i(c_n)\right)$$

решење тог система. Но, за све k и j:

$$\sigma_j\left(\sum_{i=1}^{m} \sigma_i(c_k)\right) = \sum_{i=1}^{m} (\sigma_j \circ \sigma_i)(c_k) = \sum_{i=1}^{m} \sigma_i(c_k),$$

те можемо закључити да заправо

$$\left(\sum_{i=1}^{m} \sigma_i(c_1), \sum_{i=1}^{m} \sigma_i(c_2), \ldots, \sum_{i=1}^{m} \sigma_i(c_n)\right) \in (L^G)^n = (K')^n.$$

Ако овај елемент означимо са $(d_1, \ldots, d_n)$ и узмемо у обзир то да је $\sigma_1 = \mathrm{id}_\mathrm{L}$ и да је $d_1 = \sigma_1(c_1) + \cdots + \sigma_m(c_1) \neq 0$, прва једначина система **(38)** нам даје:

$$\alpha_1 d_1 + \alpha_2 d_2 + \cdots + \alpha_n d_n = 0,$$

односно

$$d_1 \alpha_1 + d_2 \alpha_2 + \cdots + d_n \alpha_n = 0,$$

при чему сви d_i припадају K' и нису сви једнаки нули. Стога је скуп $\{\alpha_1, \ldots, \alpha_n\}$ линеарно зависан над K' што нам завршава доказ. □

8 Коренско поље сепарабилног полинома

Став 48 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 у L, тих хомоморфизама 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. □

8.1 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, звaћемо 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 49 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 50 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 51 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 $D(f) = (\alpha_1 - \alpha_2)^2 = \alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = b^2 - 4c$. ♣

Пример 52 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:

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

9 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 53 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?

9.1 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 54 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 55 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 $G_f = \mathbb{S}_3$. ♣

9.2 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 $G_f \cap V \lhd G_f$. 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 56 $\left(\Phi^{-1}\left[G_f \cap V\right]\right)^\flat = K(\alpha, \beta, \gamma)$. 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 57 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,

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

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

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

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

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

$$\begin{aligned}
D(g)&=(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2\\
&=((\alpha_1\alpha_2+\alpha_3\alpha_4-\alpha_1\alpha_3-\alpha_2\alpha_4)(\alpha_1\alpha_2+\alpha_3\alpha_4-\alpha_1\alpha_4-\alpha_2\alpha_3)(\alpha_1\alpha_3+\alpha_2\alpha_4-\alpha_1\alpha_4-\alpha_2\alpha_3))^2\\
&=((\alpha_1(\alpha_2-\alpha_3)-\alpha_4(\alpha_2-\alpha_3))(\alpha_1(\alpha_2-\alpha_4)-\alpha_3(\alpha_2-\alpha_4))(\alpha_1(\alpha_3-\alpha_4)-\alpha_2(\alpha_3-\alpha_4)))^2\\
&=((\alpha_1-\alpha_4)(\alpha_2-\alpha_3)(\alpha_1-\alpha_3)(\alpha_2-\alpha_4)(\alpha_1-\alpha_2)(\alpha_3-\alpha_4))^2=D(f).
\end{aligned}$$

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 58 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 59 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 **53** 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 **56**). 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 60 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 61 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 62 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 $\mathbb{C}$. ♠

9.3 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 63 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 $(12), (13), \dots, (1p)$ 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 $\sigma = (ki_2 \dots i_p)$. Јасно је да је $\sigma^r(k) = l$ за неки r, тако да имамо и цикл $\sigma_0 = (klj_3 \dots j_p)$ (приметимо да је σ^r увек p-цикл за $p \nmid r$ пошто је p прост број). Добијамо:

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

Но, имамо да је

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

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 64 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 **63** закључујемо да је $G_f = \mathbb{S}_p$. □

Пример 65 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 **64**, добијамо да је $G_f = \mathbb{S}_5$. ♣

Пример 66 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, ..., 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:

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

Дакле,

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

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 **64** добијамо да је $G_f = \mathbb{S}_p$. ♣

10 Коначна поља

У овом кратком одељку класификоваћемо коначна поља до на изоморфизам и описати њихова међусобна утапања. Најпре један једноставан став из линеарне алгебре.

Став 67 Свако коначно поље има p^n елемената за неки прост број p и природан број $n \geq 1$.

Доказ. Нека је K коначно поље. Пошто је K коначно, оно свакако има коначну карактеристику p, која је прост број. Тада, према ставу **15**, K садржи као своје потпоље поље $\mathbb{Z}_p$. Тада је K векторски простор над $\mathbb{Z}_p$ и то, наравно, коначне димензије пошто је K коначно. Дакле, ако је $\dim_{\mathbb{Z}_p} K = n$, онда је K као векторски простор над $\mathbb{Z}_p$ изоморфно са $(\mathbb{Z}_p)^n$, те има p^n елемената. □

У даљем ћемо, ако $\mathbb{Z}_p$ разматрамо као поље, користити ознаку $\mathbb{F}_p$.

Следећа теорема нам потпуно карактерише коначна поља.

Теорема 68 За сваки прост број p и природан број $n \geq 1$ постоји поље са p^n елемената и оно је одређено јединствено до на изоморфизам. Ако је $\mathbb{F}_{p^n}$ поље са p^n елемената, онда је раширење $\mathbb{F}_{p^n}/\mathbb{F}_p$ Галоаово и $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$ је циклична група генерисана Фробенијусовим аутоморфизмом $\varphi\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ задатим са: $\varphi(x) = x^p$.

Доказ. Покажимо да је поље са $q = p^n$ елемената заправо коренско поље полинома $a(X) = X^q - X \in \mathbb{F}_p[X]$. То ће нам показати и егзистенцију и јединственост на основу егзистенције и јединствености коренског поља.

Најпре, нека је F поље које има $q = p^n$ елемената. Тада је $(F \setminus \{0\}, \cdot)$ група и $|F \setminus \{0\}| = q - 1$. Стога је $\alpha^{q-1} = 1$, за све $\alpha \in F \setminus \{0\}$, па је и $\alpha^q = \alpha$ за све $\alpha \in F$, те је $a(\alpha) = 0$ за све $\alpha \in F \setminus \{0\}$. Како је $\deg a(X) = q$, а сваки елемент из F је његова нула, то је

$$a(X) = X^q - X = \prod_{\alpha \in F} (X - \alpha).$$

Дакле, ако постоји поље са $q = p^n$ елемената, сваки његов елемент је корен полинома $a(X)$. Да бисмо показали да заиста за свако n постоји поље са p^n елемената, посматрајмо коренско поље K_a овог полинома. А приори, не морају сви елементи из K_a бити корени полинома a. Стога посматрамо $L \subseteq K_a$ задат са:

$$L := \{\alpha \in K_a : a(\alpha) = 0\} = \{\alpha \in K : \alpha^q = \alpha\}.$$

Није тешко проверити да је L потпоље поља K_a. Наиме, јасно је да и 1_{K_a} и 0_{K_a} припадају пољу K_a. Осим тога, ако $\alpha, \beta \in K_a$ онда је

$(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$, па и $\alpha\beta \in K_a$. Како је K_a карактеристике p, онда је $(\alpha \pm \beta)^p = \alpha^p \pm \beta^p$, па, индукцијом по $m \geq 1$ добијамо да је и $(\alpha \pm \beta)^{p^m} = \alpha^{p^m} \pm \beta^{p^m}$. Стога је и $(\alpha \pm \beta)^q = \alpha^q \pm \beta^q = \alpha \pm \beta$, те и $\alpha \pm \beta \in L$. L је поље које се састоји од корена полинома $a(X)$. Како је $a'(X) = -1$, то је овај полином сепарабилан и $|L| = \deg a(X) = q$. Дакле, L је поље са q елемената. Но, већ се у $L[X]$ полином $a(X)$ цепа на линеарне факторе: $a(X) = \prod_{\alpha \in L}(X - \alpha)$. Како је коренско поље полинома минимално такво поље, то мора бити $L = K_a$. Овим смо доказали први део теореме.

Пошто је поље са $q = p^n$ елемената одређено јединствено до на изоморфизам, користићемо ознаку $\mathbb{F}_q$. Видели смо да је то коренско поље полинома $X^q - X$, који је сепарабилан па је раширење $\mathbb{F}_q/\mathbb{F}_p$ Галоаово и $|G(\mathbb{F}_q/\mathbb{F}_p)| = n$. Посматрајмо аутоморфизам φ поља $\mathbb{F}_q$ дат са: $\varphi(x) = x^p$. Приметимо да је за свако $x \in \mathbb{F}_q$ испуњено:

$$x \in \mathbb{F}_p \text{ акко } x^p = x \text{ акко } \varphi(x) = x.$$

Дакле, $\varphi \in G(\mathbb{F}_q/\mathbb{F}_p)$ и $\mathbb{F}_p = \langle\varphi\rangle^\flat$. Имамо да је

$$\varphi^2(x) = \varphi(\varphi(x)) = \varphi(x^p) = (\varphi(x))^p = (x^p)^p = x^{p^2}.$$

Индукцијом се лако покаже да је $\varphi^k(x) = x^{p^k}$ за $k \geq 1$. Како је, за све $x \in \mathbb{F}_q$, $x^q (= x^{p^n}) = x$, то је $\varphi^n = \mathrm{id}_{\mathbb{F}_q}$. Може ли се десити да је $\varphi^m = \mathrm{id}_{\mathbb{F}_q}$ за неко $m < n$? Но, то би значило да је за свако $x \in \mathbb{F}_q$: $x^{p^m} = x$ што би нам дало да у $\mathbb{F}_q$ има највише $p^m < q$ елемената. Ова контрадикција нам показује да је ред Фробенијусовог аутоморфизма баш n и да је $G(\mathbb{F}_q/\mathbb{F}_p) = \langle\varphi\rangle$. □

Последица 69 Нека је F поље које има p^n елемената. Доказати да оно има тачно једно потпоље са p^d елемената за сваки делилац d броја n и да су то једина потпоља од F.

Доказ. Знамо да је раширење $F/\mathbb{F}_p$ Галоаово. На основу Галоаове кореспонденције постоји бијекција између подгрупа групе $G(F/\mathbb{F}_p)$ и потпоља од F (која садрже $\mathbb{F}_p$, али у овом случају су то сва потпоља од F). Како је група $G(F/\mathbb{F}_p)$ циклична, она за сваки делилац m броја n садржи тачно једну подгрупу са m елемената. Конкретно, ако $d \mid n$, онда је $[\langle\varphi^d\rangle^\flat : \mathbb{F}_p] = [G : \langle\varphi^d\rangle] = n/(n/d) = d$ (присетимо се да је ред елемента φ^d једнак n/d). Стога је $|\langle\varphi^d\rangle^\flat| = p^d$. Заправо је

$$\langle\varphi^d\rangle^\flat = \{\alpha \in F : \varphi^d(\alpha) = \alpha\}\{\alpha \in F : \alpha^{p^d} = \alpha\},$$

као што је требало и очекивати. □

На пример, поље са 8 елемената не садржи као своје потпоље поље са 4 елемента, јер $2 \nmid 3$, али поље са 16 елемената садржи као своје потпоље поље са 4 елемента.

11 Циклотомична раширења

Овај одељак почињемо једном дефиницијом.

Дефиниција 70 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 71 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 $E = \{\zeta^k : 0 \leq k < n\}$. 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 $1 \leq i \leq n-1$, а $\omega(\zeta^i) = n$ **акко** је $\mathrm{NZD}(i,n) = 1$. Знамо и да је $U(\mathbb{Z}_n) = \Phi(n)(= \{k : 1 \leq k < n, \mathrm{NZD}(k,n) = 1\})$. 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 72 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 $\alpha > 1$:

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

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

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{41}$$

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 **(41)** 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:

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

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 $r \geq 1$, онда је:

$$\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}}). \tag{42}$$

Ово се лако показује. Најпре, приметимо да је

$$\Phi_p(X^{p^{r-1}}) = \frac{\left(X^{p^{r-1}}\right)^p - 1}{X^{p^{r-1}} - 1} = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1}. \tag{43}$$

Но,

$$X^{p^{r-1}} - 1 = \prod_{0 \leq k \leq r-1} \Phi_{p^k}(X), \tag{44}$$

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

$$X^{p^r} - 1 = \prod_{0 \leq k \leq r} \Phi_{p^k}(X), \tag{45}$$

Но, из **(44)** и **(45)** директно следи **(42)**. ♠

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

$$\Phi_{2n}(X) = \Phi_n(-X). \tag{46}$$

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 $1 \leq k \leq p-1$, $1 \leq i \leq \varphi(n)$, где су ζ_i, за $1 \leq i \leq \varphi(n)$ 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

$$\Phi_n(X^p) = \prod_{\omega(\zeta)=n} \prod_{k=0}^{p-1}(X - \eta^k\zeta). \tag{47}$$

Но,

$$\Phi_{pn}(X) = \prod_{\omega(\zeta)=n} \prod_{k=1}^{p-1}(X - \eta^k\zeta). \tag{48}$$

Обратите пажњу на малу, али битну разлику, између производа у **(47)** и **(48)** — 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.

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

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 73 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. □

12 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 74 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 75 Правилни n-тоугао је могуће конструисати ако и само ако је $n = 2^k p_1 \cdots p_s$, за неко $k \geq 0$, 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 $u \geq 0$, 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. □

13 Теорема о нормалној бази

Дефиниција 76 Нека је L/K коначно Галоаово раширење. Нека је $G(L/K) = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$, при чему, као и раније, узимамо да је $\sigma_1 = \mathrm{id}_L$. Ако је за неки елемент $\alpha \in L$: $[\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_m(\alpha)]$ база векторског простора L над пољем K, онда за елемент α кажемо да је НОРМАЛАН, а за наведену базу кажемо да је НОРМАЛНА БАЗА.

Наравно, увек се при формулисању нове дефиниције поставља питање да ли објекат који она дефинише уопште постоји. Но, заиста је то тако, пошто важи следећа теорема.

Теорема 77 За свако коначно Галоаово раширење L/K постоји нормална база.

Пре доказа ове теореме докажимо једну једноставну, али важну лему.

Лема 78 Нека је L бесконачно поље и $S \subseteq L$ бесконачан подскуп од L. Ако је $f \in L[X_1, \ldots, X_m] \setminus \{0\}$, онда је $0 \neq \tilde{f}_{|S^m} \colon S^m \to L$.

Доказ. Радимо индукцијом. Ако је $m = 1$, онда знамо да полином f има највише $\deg f$ нула у пољу L. Како је скуп S бесконачан, постоји $a \in S$, такво да је $\tilde{f}(a) \neq 0$.

Претпоставимо сада да је $m > 1$ и да је тврђење доказано за све полиноме са мање од m неодређених. Посматрајмо дати полином f из $L[X_1, \ldots, X_m]$ као полином степена $r \geq 0$ у неодређеној X_m са коефицијентима у $L[X_1, \ldots, X_{m-1}]$:

$$f(X_1, \ldots, X_m) = g_r(X_1, \ldots, X_{m-1})X_m^r + g_{r-1}(X_1, \ldots, X_{m-1})X_m^{r-1} + \cdots + g_1(X_1, \ldots, X_{m-1})X_m + g_0(X_1, \ldots, X_{m-1}). \quad (49)$$

Дакле, $g_r(X_1, \ldots, X_{m-1}) \neq 0$ (приметимо да нам ништа не смета и ако је $r = 0$, доказ је још лакши). По индуктивној хипотези, постоји $(m-1)$-торка $(a_1, \ldots, a_{m-1}) \in S^{m-1}$ таква да је $\tilde{g}_r(a_1, \ldots, a_{m-1}) \neq 0$. Стога је

$$0 \neq \tilde{g}_r(a_1, \ldots, a_{m-1})X_m^r + \cdots + \tilde{g}_1(a_1, \ldots, a_{m-1})X_m + \tilde{g}_0(a_1, \ldots, a_{m-1}) \in L[X_m]$$

Сада смо поново у случају полинома са једном неодређеном и можемо да констатујемо да постоји $a_m \in S$ за који је

$$0 \neq \tilde{g}_r(a_1, \ldots, a_{n-1})a_m^r + \cdots + \tilde{g}_1(a_1, \ldots, a_{m-1})a_m + \tilde{g}_0(a_1, \ldots, a_{m-1}) \in L,$$

а то значи да је $\tilde{f}(a_1, \ldots, a_m) \neq 0$. □

Напомена 79 Мада то обично не радимо, овде смо користили посебну ознаку за полиномску функцију да би била више истакнута разлика полинома и полиномске функције. Добро нам је познато да полиномска функција може бити нула функција мада полином није једнак нули. На пример, ако је $f(X) = X^p - X \in \mathbb{F}_p[X]$, имамо да је $0 = \tilde{f} \colon \mathbb{F}_p \to \mathbb{F}_p$. ♠

Доказ теореме 77. Прво дајемо **доказ за случај када је K бесконачно поље**. Анализирајмо мало ситуацију. Нека је $\alpha \in L$. Како знамо да је $[\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_m(\alpha)]$ база? За то је довољно показати линеарну независност над K пошто је број елемената једнак $\dim_K L$. Дакле, претпоставимо да је

$$a_1\sigma_1(\alpha) + a_2\sigma_2(\alpha) + \cdots + a_m\sigma_m(\alpha) = 0,$$

где $a_1, \ldots, a_m \in K$. Треба показати да су сви они једнаки 0. Као и раније, погодно је ову једнакост „напасти" аутоморфизмима σ_i. Добијамо хомогени систем (знамо да су све ово K-аутоморфизми) једначина по $a_1, \ldots, a_m$.

$$\begin{gathered}
a_1(\sigma_1 \circ \sigma_1)(\alpha) + a_2(\sigma_1 \circ \sigma_2)(\alpha) + \cdots + a_m(\sigma_1 \circ \sigma_m)(\alpha) = 0 \\
a_1(\sigma_2 \circ \sigma_1)(\alpha) + a_2(\sigma_2 \circ \sigma_2)(\alpha) + \cdots + a_m(\sigma_2 \circ \sigma_m)(\alpha) = 0 \\
\vdots \\
a_1(\sigma_m \circ \sigma_1)(\alpha) + a_2(\sigma_m \circ \sigma_2)(\alpha) + \cdots + a_m(\sigma_m \circ \sigma_m)(\alpha) = 0.
\end{gathered}$$

Да би овај систем једначина имао само тривијално решење потребно је и довољно да матрица система буде инвертибилна, односно да њена детерминанта буде различита од 0.

$$\begin{vmatrix}
(\sigma_1 \circ \sigma_1)(\alpha) & (\sigma_1 \circ \sigma_2)(\alpha) & \ldots & (\sigma_1 \circ \sigma_m)(\alpha) \\
(\sigma_2 \circ \sigma_1)(\alpha) & (\sigma_2 \circ \sigma_2)(\alpha) & \ldots & (\sigma_2 \circ \sigma_m)(\alpha) \\
\vdots & \vdots & \ddots & \vdots \\
(\sigma_m \circ \sigma_1)(\alpha) & (\sigma_m \circ \sigma_2)(\alpha) & \ldots & (\sigma_m \circ \sigma_m)(\alpha)
\end{vmatrix} \neq 0. \tag{50}$$

Ова детерминанта, или матрица система би могла да нас асоцира на таблицу множења у групи $G(= G(L/K)$.

$\circ$	σ_1	σ_2	$\ldots$	σ_m
σ_1	$\sigma_1 \circ \sigma_1$	$\sigma_1 \circ \sigma_2$	$\ldots$	$\sigma_1 \circ \sigma_m$
σ_2	$\sigma_2 \circ \sigma_1$	$\sigma_2 \circ \sigma_2$	$\ldots$	$\sigma_2 \circ \sigma_m$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
σ_m	$\sigma_m \circ \sigma_1$	$\sigma_m \circ \sigma_2$	$\ldots$	$\sigma_m \circ \sigma_m$

Сваком елементу групе σ можемо придружити једну неодређену X_σ. Ако уместо $(\sigma_i \circ \sigma_j)(\alpha)$ у детерминанти **50** поставимо неодређену $X_{\sigma_i \circ \sigma_j}$ добијамо полином по неодређеним $X_{\sigma_1}, X_{\sigma_2}, \ldots, X_{\sigma_m}$. Ако уместо X_{σ_i} после развоја детерминанте ставимо X_i, добијамо полином h:

$$h(X_1, X_2, \ldots, X_m) = \begin{vmatrix}
X_{\sigma_1 \circ \sigma_1} & X_{\sigma_1 \circ \sigma_2} & \ldots & X_{\sigma_1 \circ \sigma_m} \\
X_{\sigma_2 \circ \sigma_1} & X_{\sigma_2 \circ \sigma_2} & \ldots & X_{\sigma_2 \circ \sigma_m} \\
\vdots & \vdots & \ddots & \vdots \\
X_{\sigma_m \circ \sigma_1} & X_{\sigma_m \circ \sigma_2} & \ldots & X_{\sigma_m \circ \sigma_m}
\end{vmatrix} \in L[X_1, X_2, \ldots, X_m]. \tag{51}$$

Приметимо да је свака врста пермутација прве врсте, као што је то у таблици множења за групу. Ако израчунамо вредност $\tilde{h}(1,0,\ldots,0)$ добићемо 1 или -1 пошто је то вредност детерминанте матрице добијене од јединичне пермутовањем врста. Дакле, h свакако није нула полином. Но, ако уместо X_σ поставимо $\sigma(\alpha)$ (сетимо се да је X_i идентификовано са X_{σ_i})) у **51** добијамо:

$$\tilde{h}(\sigma_1(\alpha),\sigma_2(\alpha),\ldots,\sigma_m(\alpha)) = \begin{vmatrix} (\sigma_1\circ\sigma_1)(\alpha) & (\sigma_1\circ\sigma_2)(\alpha) & \ldots & (\sigma_1\circ\sigma_m)(\alpha) \\ (\sigma_2\circ\sigma_1)(\alpha) & (\sigma_2\circ\sigma_2)(\alpha) & \ldots & (\sigma_2\circ\sigma_m)(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ (\sigma_m\circ\sigma_1)(\alpha) & (\sigma_m\circ\sigma_2)(\alpha) & \ldots & (\sigma_m\circ\sigma_m)(\alpha) \end{vmatrix}.$$

Дакле, доказ смо свели на доказивање следеће чињенице: постоји $\alpha \in L$ такво да је $\tilde{h}(\sigma_1(\alpha),\sigma_2(\alpha),\ldots,\sigma_m(\alpha)) \neq 0$.

Претпоставимо да ово није тачно, тј. нека је

$$\tilde{h}(\sigma_1(\alpha),\sigma_2(\alpha),\ldots,\sigma_m(\alpha)) = 0 \tag{52}$$

за све α. Нека је $[\alpha_1,\alpha_2,\ldots,\alpha_m]$ нека база за векторски простор L над пољем K. Из **(52)** добијамо да је

$$\tilde{h}(\sigma_1(a_1\alpha_1+\cdots+a_m\alpha_m),\ldots,\sigma_m(a_1\alpha_1+\cdots+a_m\alpha_m)) = 0 \tag{53}$$

за све $(a_1,\ldots,a_m) \in K^m$. Искористимо да σ_i фиксирају поље K:

$$\tilde{h}(a_1\sigma_1(\alpha_1)+\cdots+a_m\sigma_1(\alpha_m),\ldots,a_1\sigma_m(\alpha_1)+\cdots+a_m\sigma_m(\alpha_m)) = 0 \tag{54}$$

Дефинишимо полином $g(X_1,X_2,\ldots,X_m) \in L[X_1,X_2,\ldots,X_m]$ са:

$$\begin{aligned} &g(X_1,\ldots,X_m) \\ &\quad = h(X_1\sigma_1(\alpha_1)+\cdots+X_m\sigma_1(\alpha_m),\ldots,X_1\sigma_m(\alpha_1)+\cdots+X_m\sigma_m(\alpha_m)) \\ &\qquad\qquad \in L[X_1,\ldots,X_m]. \end{aligned} \tag{55}$$

Из (**54**) добијамо да је $\tilde{g}(a_1,a_2,\ldots,a_m) = 0$ за све $(a_1,a_2,\ldots,a_m) \in K$. Из леме **78** добијамо да је $g(X_1,\ldots,X_m) = 0$.

Но, присетимо се сада последице **46**, која нам каже да је матрица $[\sigma_i(\alpha_j)]$ инвертибилна. Посматрајмо полиноме $Y_1,\ldots,Y_m$ дефинисане са:

$$\begin{aligned} \sigma_1(\alpha_1)X_1+\sigma_1(\alpha_2)X_2+\cdots+\sigma_1(\alpha_m)X_m &= Y_1 \\ \sigma_2(\alpha_1)X_1+\sigma_2(\alpha_2)X_2+\cdots+\sigma_2(\alpha_m)X_m &= Y_2 \\ \vdots \qquad\quad \vdots \qquad\quad \ddots \qquad\quad \vdots &= \vdots \\ \sigma_m(\alpha_1)X_1+\sigma_m(\alpha_2)X_2+\cdots+\sigma_m(\alpha_m)X_m &= Y_m. \end{aligned}$$

Имамо да је $h(Y_1,Y_2,\ldots,Y_m) = 0$. Докажимо да је $L[X_1,X_2,\ldots,X_m] = L[Y_1,Y_2,\ldots,Y_m]$, То ће нам показати да је и $h(X_1,X_2,\ldots,X_m) = 0$. Та контрадикција завршава доказ.

Наравно, јасно је да је $L[Y_1, Y_2, \ldots, Y_m] \subseteq L[X_1, X_2, \ldots, X_m]$. Но, како је матрица $[\sigma_i(\alpha_j)]$ инвертибилна, она има инверзну матрицу $[\beta_{ij}]$. То значи да је

$$\begin{array}{rcl} \beta_{11}Y_1 + \beta_{12}Y_2 + \cdots + \beta_{1m}Y_m & = & X_1 \\ \beta_{21}Y_1 + \beta_{22}Y_2 + \cdots + \beta_{2m}Y_m & = & X_2 \\ \vdots \quad \vdots \quad \ddots \quad \vdots & = & \vdots \\ \beta_{m1}Y_1 + \beta_{m2}Y_2 + \cdots + \beta_{mm}Y_m & = & X_m, \end{array}$$

а ово нам показује да је и $L[X_1, X_2, \ldots, X_m] \subseteq L[Y_1, Y_2, \ldots, Y_m]$.

Сада дајемо доказ у случају када је **група** $G(L/K)$ **циклична**. Овај случај покрива и случај коначних поља. Наиме, на основу теореме **68** раширење $F/\mathbb{F}_p$ је Галоаово за свако коначно поље и група $G(F/\mathbb{F}_p)$ је циклична. Одатле није тешко, користећи Галоаову кореспонденцију, показати да је и група $G(L/K)$, где су поља K и L коначна, циклична (оба су раширења поља $\mathbb{F}_p$ и потом се примени теорема **68**).

Дакле, нека је $G(L/K) = \langle\sigma\rangle$ циклична група реда n. Тада је $\sigma^n = \mathrm{id}_L$, па минимални полином аутоморфизма σ (σ је и K-линеарни оператор на пољу L) дели полином $X^n - 1$. Међутим, аутоморфизми $\mathrm{id}_L, \sigma, \ldots, \sigma^{n-1}$ су различити, па су на основу последице **45** они линеарно независни, тј. из једнакости $a_0\mathrm{id}_K + a_1\sigma + \cdots + a_{n-1}\sigma^{n-1} = 0$, за $a_0, a_1, \ldots, a_{n-1} \in K$ следи да је $a_0 = a_1 = \cdots = a_{n-1} = 0$. Но, то значи да је заправо $X^n - 1$ минимални полином оператора σ. У овом тренутку се у литератури аутори позивају на теорему о класификацији модула над главноидеалским доменима, но ми, срећом, то не морамо да радимо. Наиме, постоји теорема из линеарне алгебре која нам завршава доказ и доказ те теореме се може наћи у уџбенику професора Калајџића.

Теорема. Ако је L линеарни оператор простора V димензије n и ако је $\deg\mu_L = n$, где је са μ_L означен минимални полином оператора L, онда постоји вектор $v \in V$ такав да је $[v, L(v), \ldots, L^{n-1}(v)]$ једна база простора V.

Дакле, то је баш оно што нам треба! Добијамо да постоји $\alpha \in L$ тако да је $[\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)]$ база за L над K. Овим је завршен доказ теореме о нормалној бази. □

Напомена 80 У случају да имамо раширење $\mathbb{F}_{q^m}/\mathbb{F}_q$, где је $q = p^n$, за прост број p и природне $n, m \geq 1$, онда знамо да је $G(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle\varphi^n\rangle$, где је $\varphi\colon \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ Фробенијусов аутоморфизам: $\varphi(x) = x^p$. Дакле, нормална база има облик: $[\alpha, \varphi^n(\alpha), \ldots \varphi^{n(m-1)}(\alpha)] = [\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}]$. ♠

Пример 81 Нека је $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$, где α задовољава једначину $\alpha^3 + \alpha + 1 = 0$. Ми знамо да је једна база за $\mathbb{F}_8$ свакако $[1, \alpha, \alpha^2]$. Да ли је и $[\alpha, \alpha^2, \alpha^4]$ такође база, тј. да ли је елемент α нормалан (наравно, овде је $q = 2$)?

То можемо директно проверити. Наиме, како је $\alpha^3 = \alpha + 1$, то је $\alpha^4 = \alpha^2 + \alpha$. Но, тај елемент је збир претходна два те ово свакако није база, тј. α није нормалан.

Но, посматрајмо елемент $1 + \alpha$. Тада је

$$\begin{aligned}[1+\alpha, (1+\alpha)^2, (1+\alpha)^4] &= [1+\alpha, 1+\alpha^2, 1+\alpha^4] \\ &= [1+\alpha, 1+\alpha^2, 1+\alpha+\alpha^2] \sim [1+\alpha, 1+\alpha^2, \alpha^2] \\ &\sim [1+\alpha, 1, \alpha^2] \sim [\alpha, 1, \alpha^2] \sim [1, \alpha, \alpha^2].\end{aligned}$$

те добијамо да ово јесте база (овде смо изводили једноставне операције које систем вектора преводе у еквивалентан систем; на пример најпре смо први вектор додали трећем). ♣

Пример 82 Нека је $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$, где α задовољава једначину $\alpha^2 + 1 = 0$. Да ли је овде α нормалан?

Дакле, посматрамо систем $[\alpha, \alpha^3] = [\alpha, 2\alpha]$ и ово свакако није база.

Ако посматрамо $[1 + \alpha, (1 + \alpha)^3] = [1 + \alpha, 1 + \alpha^3] = [1 + \alpha, 1 + 2\alpha]$, онда видимо да ово јесте база: одузимањем првог вектора од другог добијамо $[1 + \alpha, \alpha]$ и потом одузимањем другог од првог $[1, \alpha]$. ♣

Пример 83 Нека је $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, где α задовољава једначину $\alpha^2+\alpha+1 = 0$. Овде α јесте нормалан. Наиме,

$$[\alpha, \alpha^2] = [\alpha, 1 + \alpha] \sim [\alpha, 1] \sim [1, \alpha].$$ ♣

Пример 84 Нека је $\mathbb{F}_{16} = \mathbb{F}_4(\beta)$, где β задовољава једначину $\beta^2 + \beta + \alpha = 0$. Да ли је β нормалан? Наравно, овде је $\mathbb{F}_4$ као у претходном примеру.

Уверимо се најпре да је полином $X^2 + X + \alpha \in \mathbb{F}_4[X]$ нерастављив. Наравно, довољно је да проверимо да нема нула пошто је полином степена 2. Но, $0+0+\alpha \neq 0$, $1+1+\alpha = \alpha \neq 0$, $\alpha^2+\alpha+\alpha = \alpha^2 = 1+\alpha \neq 0$ и $(1+\alpha)^2 + (1+\alpha) + \alpha = 1 + \alpha^2 + 1 = 1 + \alpha \neq 0$.

$$[\beta, \beta^4] = [\beta, \beta + 1] \sim [\beta, 1] \sim [1, \beta].$$

Користили смо да је $\beta^4 = (\beta^2)^2 = (\beta + \alpha)^2 = (\beta + \alpha) + (\alpha + 1) = \beta + 1$. ♣

Пример 85 Нека је $\mathbb{F}_{16} = \mathbb{F}_2(\gamma)$, где γ задовољава једначину $\gamma^4+\gamma+1 = 0$. Да ли је γ нормалан?

Наравно, најпре треба проверити да је $X^4 + X + 1 \in \mathbb{F}_2[X]$ нерастављив. Јасно је да нема нулу, тако да остаје само растав на два нерастављива полинома степена 2. Но, једини нерастављиви полином степена 2 из $\mathbb{F}_2[X]$ је $X^2 + X + 1$, а $(X^2 + X + 1)^2 = X^4 + X^2 + 1$.

Дакле, посматрамо систем вектора $[\gamma, \gamma^2, \gamma^4, \gamma^8]$. Знамо да је $\gamma^4 = \gamma + 1$. Стога је $\gamma^8 = \gamma^2 + 1$ и видимо да то није база.

Да ли је елемент $1 + \gamma$ нормалан?

$$[1+\gamma, (1+\gamma)^2, (1+\gamma)^4, (1+\gamma)^8] = [1+\gamma, 1+\gamma^2, 1+\gamma^4, 1+\gamma^8] = [1+\gamma, 1+\gamma^2, \gamma, \gamma^2]$$

те ни $1 + \gamma$ није нормалан. Нађите за вежбу који елемент ЈЕСТЕ нормалан. ◇

Напомена 86 Могуће је разматрати и „јаче" питање: да ли за раширење $\mathbb{F}_{q^n}/\mathbb{F}_q$ постоји примитивна нормална база, тј. да ли постоји нормалан елемент α, који је уједно и генератор (цикличне) групе $\mathbb{F}_{q^n}^\times$? Доказ овог резултата је комплетиран 1987. године. За вежбу би било добро проверити да ли су нормалне базе из претходних примера уједно и примитивне нормалне базе и, уколико нису, наћи примитивне нормалне базе у овим примерима. ♠

14 Хилбертова теорема 90

Добро нам је познато дејство групе на скупу. У случају да је тај скуп носач и неке алгебарске структуре, природно је посматрати дејство које „поштује" ту структуру. Уводимо појам G-модула следећом дефиницијом.

Дефиниција 87 Нека је G група. G-МОДУЛ је Абелова група $(M, +)$ на којој је задато дејство групе G које задовољава услов:

$$(\forall \sigma \in G)(\forall m, m' \in M)\sigma \bullet (m + m') = \sigma \bullet m + \sigma \bullet m'.$$

Наравно да је и $(\sigma\tau) \bullet m = \sigma \bullet (\tau \bullet m)$ за све $\sigma, \tau \in G$ и $m \in M$ и $e \bullet m = m$ за све $m \in M$ као и за свако друго дејство групе на скупу. Дакле, овде је задавање структуре G-модула на Абеловој групи M еквивалентно задавању хомоморфизма $G \to \mathrm{Aut}(M)$, док је код обичног дејства у питању хомоморфизам $G \to \mathbb{S}_M$.

Напомена 88 У наведеној дефиницији коришћен је адитиван запис. Уколико је Абелова група $(M, \cdot)$, онда је услов:

$$(\forall \sigma \in G)(\forall m, m' \in M)\sigma \bullet (mm') = (\sigma \bullet m) \cdot (\sigma \bullet m').$$ ♠

Пример 89 Нека је L/K Галоаово раширење са Галоаовом групом G. Тада су и $(L, +)$ и $(L^\times, \cdot)$ G-модули: $\sigma \bullet x = \sigma(x)$. ♣

У овом контексту, за $(L, +)$ користићемо ознаку L^+.

Дефиниција 90 Нека је M један G-модул. Укрштени хомоморфизам је пресликавање $f\colon G \to M$ такво да је за све $\sigma, \tau \in G$:

$$f(\sigma\tau) = f(\sigma) + \sigma \bullet f(\tau).$$

У мултипликативном запису:

$$f(\sigma\tau) = f(\sigma) \cdot (\sigma \bullet f(\tau)).$$

Уколико G дејствује тривијално на M, тј. ако је $\sigma \bullet m = m$ за све $\sigma \in G$ и $m \in M$, онда је укрштени хомоморфизам заправо обичан хомоморфизам. Приметимо да је, ако је e неутрал групе G, испуњено:

$$f(e) = f(ee) = f(e) + e \bullet f(e) = f(e) + f(e),$$

те добијамо да је $f(e) = 0_M$, као и за обичан хомоморфизам.

Пример 91 Нека је $f\colon G \to M$ укрштени хомоморфизам. Ако је $\sigma \in G$, онда имамо:

$$\begin{aligned}
f(\sigma^2) &= f(\sigma) + \sigma \bullet f(\sigma),\\
f(\sigma^3) &= f(\sigma\sigma^2) = f(\sigma) + \sigma \bullet f(\sigma^2) = f(\sigma) + \sigma \bullet (f(\sigma) + \sigma \bullet f(\sigma))\\
&= f(\sigma) + \sigma \bullet f(\sigma) + \sigma^2 \bullet f(\sigma),\\
&\vdots\\
f(\sigma^n) &= f(\sigma) + \sigma \bullet f(\sigma) + \cdots + \sigma^{n-1} \bullet f(\sigma).
\end{aligned}$$

Посебно, ако је G циклична група реда n у којој је σ генератор, укрштени хомоморфизам f је потпуно задат задавањем $f(\sigma) = x$ при чему мора бити испуњен услов да је

$$x + \sigma \bullet x + \cdots + \sigma^{n-1} \bullet x = 0_M.$$

Дакле, сваки такав елемент $x \in M$ одређује јединствен укрштени хомоморфизам. У мултипликативном запису:

$$x \cdot (\sigma \bullet x) \cdots (\sigma^{n-1} \bullet x) = 1_M. \qquad \clubsuit$$

Пример 92 Нека је $x \in M$ произвољан. Тада је са $f(\sigma) = \sigma \bullet x - x$, за $\sigma \in G$ задат један укрштени хомоморфизам:

$$\begin{aligned}
f(\sigma\tau) &= (\sigma\tau) \bullet x - x = \sigma \bullet (\tau \bullet x) - x = \sigma \bullet (\tau \bullet x - x + x) - x\\
&= \sigma \bullet (\tau \bullet x - x) + \sigma \bullet x - x = \sigma \bullet f(\tau) + f(\sigma)\\
&= f(\sigma) + \sigma \bullet f(\tau)
\end{aligned}$$

Овакав хомоморфизам се назива главним хомоморфизмом. $\clubsuit$

Скуп свих укрштених хомоморфизама $f\colon G \to M$ означићемо са $Z^1(G,M)$, а скуп свих главних укрштених хомоморфизама са $B^1(G,M)$. Збир два укрштена хомоморфизма је укрштени хомоморфизам:

$$\begin{aligned}(f+g)(\sigma\tau) &= f(\sigma\tau)+g(\sigma\tau) = f(\sigma)+\sigma\bullet f(\tau)+g(\sigma)+\sigma\bullet g(\tau)\\ &= f(\sigma)+g(\sigma)+\sigma\bullet(f(\tau)+g(\tau)) = (f+g)(\sigma)+\sigma\bullet(f+g)(\tau).\end{aligned}$$

Такође је збир два главна укрштена хомоморфизма главни:

$$(f+g)(\sigma) = f(\sigma)+g(\sigma) = \sigma\bullet x - x + \sigma\bullet y - y = \sigma\bullet(x+y)-(x+y).$$

Дакле и $Z^1(G,M)$ и $B^1(G,M)$ су Абелове групе, при чему је додатно $B^1(G,M) \leq Z^1(G,M)$.

Дефиниција 93 Прва кохомологија групе G са коефицијентима у G-модулу M дефинише се са:

$$H^1(G,M) := Z^1(G,M)/B^1(G,M).$$

Заправо је могуће дефинисати и $H^n(G,M)$ за све $n \geq 0$. Напоменимо да је $H^0(G,M) \cong M^G$, где смо са M^G наравно означили скуп фиксних тачака у M при дејству групе G.

Овде се завршава материјал за други колоквијум.

Постоји веза између ових група. Најпре наведимо следећу дефиницију.

Дефиниција 94 Нека су M и N неки G-модули. Хомоморфизам G-модула $\alpha\colon M \to N$ је хомоморфизам Абелових група $M \to N$ који „поштује" структуру G-модула, тј. такав да је, за све $\sigma \in G$, $m \in M$: $\alpha(\sigma\bullet m) = \sigma\bullet\alpha(m)$.

Ако је

$$\cdots \longrightarrow M' \xrightarrow{\alpha} M'' \xrightarrow{\beta} M''' \longrightarrow \cdots,$$

низ G-модула и хомоморфизама за који је $\operatorname{Ker}\beta = \operatorname{Im}\alpha$, онда кажемо да је тај низ ТАЧАН у M. Низ G-модула и хомоморфизама је ТАЧАН ако је тачан у сваком модулу тог низа.

Посебно, низ G-модула

$$\{0\} \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to \{0\} \tag{56}$$

је тачан **акко**: α је „1–1", β је „на" и $\operatorname{Ker}\beta = \operatorname{Im}\alpha$. Наиме,

$$\operatorname{Im}(\{0\} \to M') = \{0\}, \qquad \operatorname{Ker}(M'' \to \{0\}) = M''.$$

Уместо $\{0\}$ уобичајено је да се пише краће само 0.

Ако са M^G означимо скуп свих фиксних тачака у M при дејству групе G, онда можемо приметити следеће.

1. Фиксне тачке се сликају у фиксне тачке при хомоморфизму G-модула. Наиме, ако је $x \in (M')^G$ и $\sigma \in G$, онда је $\sigma \bullet \alpha(x) = \alpha(\sigma \bullet x) = \alpha(x)$. Стога је могуће дефинисати сужења α_0 и β_0 од α и β и посматрати низ Абелових група:

$$0 \longrightarrow (M')^G \xrightarrow{\alpha_0} M^G \xrightarrow{\beta_0} (M'')^G \longrightarrow 0. \tag{57}$$

2. Овај низ је тачан свуда сем у $(M'')^G$. Јасно је да је α_0 мономорфизам, јер је он сужење од α који јесте мономорфизам. Такође је $\beta_0 \circ \alpha_0 = 0$, па је $\operatorname{Im}\alpha_0 \subseteq \operatorname{Ker}\beta_0$. Нека је $x \in \operatorname{Ker}\beta_0$. То значи да је $\beta(x) = \beta_0(x) = 0$, па је, због тачности почетног низа, $x = \alpha(x')$. Но, ако је $\sigma \in G$, онда је $\alpha(\sigma \bullet x') = \sigma \bullet \alpha(x') = \sigma \bullet x = x = \alpha(x')$, те из чињенице да је α „1–1" следи да је $\sigma \bullet x' = x'$, тј. $x' \in (M')^G$, па је $x = \alpha_0(x')$.

Покажимо примером да низ **57** не мора бити тачан. Нека је $M' = M = \mathbb{Z}$, $M'' = \mathbb{Z}_2$, $\alpha(x) = 2x$, $\beta(x) = \rho(x, 2)$, где је са $\rho(x, 2)$ означен остатак при дељењу x са 2. За групу G узмимо $G = \mathbb{C}_2 = \{1, -1\}$. Горенаведене Абелове групе постају G-модули тако што дефинишемо дејство са: $(-1) \bullet x = -x$. Јасно је да добијамо тачан низ G-модула:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\alpha} \mathbb{Z} \xrightarrow{\beta} \mathbb{Z}_2 \longrightarrow 0. \tag{58}$$

Но, $\mathbb{Z}^G = \{0\}$, $\mathbb{Z}_2^G = \mathbb{Z}_2$ и добијамо низ

$$0 \longrightarrow \{0\} \xrightarrow{\alpha_0} \{0\} \xrightarrow{\beta_0} \mathbb{Z}_2 \longrightarrow 0, \tag{59}$$

који свакако није тачан.

Следећи став нам ово поправља.

Став 95 Сваки кратак тачан низ G-модула

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0 \tag{60}$$

индукује дуги тачан низ Абелових група:

$$0 \longrightarrow (M')^G \xrightarrow{\alpha_0} M^G \xrightarrow{\beta_0} (M'')^G \xrightarrow{\delta^0} H^1(G, M') \xrightarrow{\alpha_1} H^1(G, M) \xrightarrow{\beta_1} H^1(G, M''). \tag{61}$$

Доказ. Почетни део смо већ „обрадили".

Дефинишимо сада

$$\delta^0 \colon (M'')^G \to H^1(G, M') = Z^1(G, M')/B^1(G, M').$$

Нека је $m'' \in (M'')^G$. Како је β „на", то постоји $m \in M$ тако да је $\beta(m) = m''$. Ако је $\sigma \in G$, имамо да је

$$\beta(\sigma \bullet m - m) = \beta(\sigma \bullet m) - \beta(m) = \sigma \bullet \beta(m) - \beta(m) = \sigma \bullet m'' - m'' = m'' - m'' = 0.$$

Наравно, овде смо користили да $m'' \in (M'')^G$, па је $\sigma \bullet m'' = m''$ за све $\sigma \in G$. Дакле, $\sigma \bullet m - m \in \operatorname{Ker} \beta$. Како је низ (**60**) тачан, то је $\sigma \bullet m - m = \alpha(m')$ за јединствено одређен $m' \in M'$ (пошто је α „1–1"). Дакле, на овај начин смо елементу $\sigma \in G$ придружили елемент $m' \in M'$ те имамо пресликавање из G у M'. Како је избор елемента m' зависио од избора елемента m који се слика у m'', то пресликавање ћемо означити са $f_m \colon G \to M'$. Дакле,

$$f_m(\sigma) = m' \text{ акко је } \alpha(m') = \sigma \bullet m - m.$$

Проверимо да ли је ово f_m један укрштени хомоморфизам. Дакле, треба проверити да ли је

$$f_m(\sigma\tau) = f_m(\sigma) + \sigma \bullet f_m(\tau),$$

за све $\sigma, \tau \in G$. Нека је $f_m(\sigma\tau) = m'_1$, а $f_m(\tau) = m'_2$. Тада је $(\sigma\tau) \bullet m - m = \alpha(m'_1)$ и $\tau \bullet m - m = \alpha(m'_2)$. Ми треба да проверимо да ли је

$$m'_1 = m' + \sigma \bullet m'_2.$$

Имамо да је

$$\begin{aligned} \alpha(m' + \sigma \bullet m'_2) &= \alpha(m') + \sigma \bullet \alpha(m'_2) = (\sigma \bullet m - m) + \sigma \bullet (\tau \bullet m - m) \\ &= \sigma \bullet m - m + (\sigma\tau) \bullet m - \sigma \bullet m = (\sigma\tau) \bullet m - m = \alpha(m'_1). \quad (62) \end{aligned}$$

Како је α „1–1", из (**62**) следи да је $m' + \sigma \bullet m'_2 = m'_1$ те закључујемо да је f_m заиста укрштени хомоморфизам. Дакле, δ^0 дефинишемо са:

$$\delta^0(m'') := [f_m].$$

Покажимо да ова класа не зависи од избора m. То значи да треба да покажемо да, ако је $\beta(\widetilde{m}) = m''$ онда је $f_m - f_{\widetilde{m}}$ један ГЛАВНИ укрштени хомоморфизам. Но, ако је $\beta(\widetilde{m}) = m''$, онда је $\beta(\widetilde{m} - m) = 0$, па постоји неки $x' \in M'$ тако да је $\widetilde{m} - m = \alpha(x')$. Ако сада уместо m узмемо $\widetilde{m} = m + \alpha(x')$, онда је

$$\sigma \bullet \widetilde{m} - \widetilde{m} = \sigma \bullet m + \sigma \bullet \alpha(x') - m - \alpha(x') = \alpha(m') + \alpha(\sigma \bullet x' - x') = \alpha(m' + \sigma \bullet x' - x').$$

Дакле, $f_{\widetilde{m}}(\sigma) = f_m(\sigma) + \sigma \bullet x' - x'$. Како је придруживање $\sigma \mapsto \sigma \bullet x' - x'$ заиста један главни укрштени хомоморфизам, добијамо то што смо тражили, тј. класа $[f_m]$ не зависи од m, те је $\delta^0(m'') := [f_m]$ добро дефинисано.

Треба показати и да је δ^0 један хомоморфизам Абелових група, тј. да је $\delta^0(m'' + m''_0) = \delta^0(m'') + \delta^0(m''_0)$. У ту сврху, нека је $m_0 \in M$

такав да је $\beta(m_0) = m_0''$. Тада је $\beta(m + m_0) = m'' + m_0''$, те ми елемент $m + m_0$ можемо да користимо за налажење $\delta^0(m'' + m_0'')$. Треба да покажемо да је $[f_{m+m_0}] = [f_m] + [f_{m_0}]$. Но, ако је $f_{m_0}(\sigma) = m_0'$, онда је $\alpha(m_0') = \sigma \bullet m_0 - m_0$ и имамо да је $\alpha(m' + m_0') = \sigma \bullet (m + m_0) - (m + m_0)$, а то значи да је $f_{m+m_0}(\sigma) = m' + m_0' = f_m(\sigma) + f_{m_0}(\sigma)$, те је заправо $f_{m+m_0} = f_m + f_{m_0}$.

Тачност у $(M'')^G$. Најпре треба проверити да ли је $\delta^0 \circ \beta_0 = 0$. То ће нам дати да је $\operatorname{Im} \beta_0 \subseteq \operatorname{Ker} \delta^0$. Узмимо $m \in M^G$. Треба проверити да ли је $\delta^0(\beta(m)) = 0_{H^1(G,M')}$. Но, како је дефинисано $\delta^0(\beta(m))$? Најпре, посматрамо $\beta(m)$ и тражимо елемент из M који се при β, слика у њега. Али, то је баш елемент m! Потом рачунамо $\sigma \bullet m - m$. Но, како је $m \in M^G$, то је једнако 0. Стога је $m' = 0$ и добијамо да је $f_m = 0 \colon G \to M$. Дакле, заиста је $\delta^0 \circ \beta_0 = 0$.

Претпоставимо сада да је $m'' \in (M'')^G$ такав да је $\delta^0(m'') = 0$ у $H^1(G, M')$. То заправо значи да је f_m, где је m такав да је $\beta(m) = m''$ главни укрштени хомоморфизам, тј. да постоји $x' \in M'$ такав да је $f_m(\sigma) = \sigma \bullet x' - x'$. Но, то значи да је $\sigma \bullet m - m = \alpha(\sigma \bullet x' - x')$. Одавде добијамо да је $\sigma \bullet (m - \alpha(x')) = m - \alpha(x')$ и то за све $\sigma \in G$. То значи да је $m - \alpha(x') \in M^G$. Како је $\beta(m - \alpha(x')) = \beta(m) = m''$, добијамо да је $\beta_0(m - \alpha(x')) = m''$, те имамо тачност у $(M'')^G$.

Тачност у $H^1(G, M')$. Најпре се треба уверити да је $\alpha_1 \circ \delta^0 = 0$. Но, како је заправо дефинисамо α_1? Ево како. Ако је $[f] \in H^1(G, M)$, онда је $f \colon G \to M$ један укрштени хомоморфизам. Тада је $\alpha_1[f] := [\alpha \circ f]$. Да бисмо проверили да је ово добро дефинисан хомоморфизам треба проверити: $\alpha \circ f \in Z^1(G, M'')$ ако $f \in Z^1(G, M')$ и $\alpha \circ f \in B^1(G, M'')$ за $f \in B^1(G, M)$. Дакле:

$$\begin{aligned}(\alpha \circ f)(\sigma\tau) = \alpha(f(\sigma\tau)) &= \alpha(f(\sigma) + \sigma \bullet f(\tau)) = \alpha(f(\sigma)) + \alpha(\sigma \bullet f(\tau)) \\ &= (\alpha \circ f)(\sigma) + \sigma \bullet \alpha(f(\tau)) = (\alpha \circ f) + \sigma \bullet (\alpha \circ f)(\tau).\end{aligned}$$

Ако је $f \in B^1(G, M)$ онда је $f(\sigma) = \sigma \bullet m - m$ за неко $m \in M$, па је:

$$(\alpha \circ f)(\sigma) = \alpha(f(\sigma)) = \alpha(\sigma \bullet m - m) = \alpha(\sigma \bullet m) - \alpha(m) = \sigma \bullet \alpha(m) - \alpha(m).$$

Наравно,

$$\alpha_1([f]+[g]) = \alpha_1[f+g] = [\alpha \circ (f+g)] = [\alpha \circ f + \alpha \circ g] = [\alpha \circ f] + [\alpha \circ g] = \alpha_1[f] + \alpha_1[g].$$

На аналогни начин се дефинише и β_1. Вратимо се доказу тачности у $H^1(G, M')$. Нека је $m'' \in (M'')^G$. Тада је $\delta^0(m'') = [f_m]$, где је m такав да је $\beta(m) = m''$, док је $(\alpha_1 \circ \delta^0)(m'') = [\alpha \circ f_m]$. Покажимо да је $\alpha \circ f_m$ главни укрштени хомоморфизам. Но, ако је $\sigma \in G$ онда је

$$(\alpha \circ f_m)(\sigma) = \alpha(f_m(\sigma)) = \alpha(m') = \sigma \bullet m - m,$$

а то је управо оно што нам је и требало (погледати поново како смо дефинисали f_m).

Претпоставимо сада да је $[f] \in \operatorname{Ker}\alpha_1$. То значи да је $\alpha \circ f$ главни, тј. постоји $m \in M$ тако да је за свако $\sigma \in G$: $(\alpha \circ f)(\sigma) = \sigma \bullet m - m$. Тада је

$$\beta(\sigma \bullet m - m) = \beta((\alpha \circ f)(\sigma)) = (\beta \circ \alpha \circ f)(\sigma) = 0.$$

Стога је $\sigma \bullet \beta(m) = \beta(\sigma \bullet m) = \beta(m)$, па је $m'' = \beta(m) \in M^G$. По дефиницији $\delta^0(m'')$ можемо да видимо да је $\delta^0(m'') = [f_m]$, где је m такво да је $\beta(m) = m''$, а $f_m(\sigma) = m'$, при чему је $\alpha(m') = \sigma \bullet m - m$. Но, видимо да је код нас $\alpha(f(\sigma)) = \sigma \bullet m - m$, а како је α „1–1", то нам показује да је $f = f_m$ и добили смо да је $[f] = \delta^0(m'')$. Тиме је завршен доказ тачности у $H^1(G, M')$.

Тачност у $H^1(G, M)$. Најпре, ако је $[f] \in H^1(G, M')$ онда је $(\beta_1 \circ \alpha_1)[f] = [\beta \circ \alpha \circ f] = [0]$, па је $\operatorname{Im}\alpha_1 \subseteq \operatorname{Ker}\beta_1$.

Претпоставимо да је $\beta_1([g]) = 0_{H^1(G,M'')}$, за неки $g \in Z^1(G, M)$. То значи да је $\beta \circ g$ главни, тј. да постоји $m'' \in M''$ такав да је за свако $\sigma \in G$: $\beta(g(\sigma)) = \sigma \bullet m'' - m''$. Ми треба да покажемо да постоји $f \in Z^1(G, M')$ тако да је $\alpha_1([f]) = [g]$, односно да постоји $f \in Z^1(G, M')$ тако да је $g - \alpha \circ f$ главни. Како је β „на", то постоји $m \in M$ тако да је $\beta(m) = m''$. Дакле, имамо да је $\beta(g(\sigma)) = \sigma \bullet \beta(m) - \beta(m) = \beta(\sigma \bullet m - m)$, те свакако $g(\sigma) - (\sigma \bullet m - m) \in \operatorname{Ker}\beta = \operatorname{Im}\alpha$. Дакле, за свако $\sigma \in G$ постоји тачно једно $m' \in M'$ (α је „1–1") тако да је $g(\sigma) - (\sigma \bullet m - m) = \alpha(m')$. Дефинишимо $f\colon G \to M'$ са: $f(\sigma) = m'$. Добијамо да је $g(\sigma) - (\sigma \bullet m - m) = \alpha(f(\sigma))$ за свако $\sigma \in G$. Како је пресликавање $\sigma \mapsto g(\sigma) - (\sigma \bullet m - m)$ сигурно укрштени хомоморфизам, као разлика два таква и α „1–1, добијамо да је и f укрштени хомоморфизам (уверите се зашто је то тако). Стога је

$$(g - \alpha \circ f)(\sigma) = \sigma \bullet m - m,$$

па је $[g - \alpha \circ f] = 0_{H^1(G,M)}$ те је $\alpha_1([f]) = [g]$.

Овим је завршен доказ тачности индукованог низа. □

Вратимо се мало на пример који је претходио разматрању овог дугог тачног низа и применимо новодобијено знање на њега. Имамо тачан низ:

$$0 \longrightarrow \mathbb{Z}^{\mathbb{C}_2} \xrightarrow{\alpha_0} \mathbb{Z}^{\mathbb{C}_2} \xrightarrow{\beta_0} (\mathbb{Z}_2)^{\mathbb{C}_2} \xrightarrow{\delta^0} H^1(\mathbb{C}_2, \mathbb{Z}) \xrightarrow{\alpha_1} H^1(\mathbb{C}_2, \mathbb{Z}) \xrightarrow{\beta_1} H^1(\mathbb{C}_2, \mathbb{Z}_2). \qquad (63)$$

Први део низа нам је познат, да видимо за остале групе. Најпре одредимо укрштене хомоморфизме $f\colon \mathbb{C}_2 \to \mathbb{Z}$. Имајући у виду дејство групе $\mathbb{C}_2$ и дефиницију укрштеног хомоморфизма, треба видети колико може бити $f(-1) \in \mathbb{Z}$ тако да важи$0 = f((-1)^2) = f(-1) + (-f(-1))$. Но, то је тачно за сваки избор $f(-1)$, па је $Z^1(\mathbb{C}_2, \mathbb{Z}) = \mathbb{Z}$, а такође је и $Z^1(\mathbb{C}_2, \mathbb{Z}_2) = \mathbb{Z}_2$. Ако је $f\colon \mathbb{C}_2 \to \mathbb{Z}$ главни хомоморфизам, онда

је $f(-1) = -x - x = -2x$ за неки $x \in \mathbb{Z}$. Дакле, $B^1(\mathbb{C}_2, \mathbb{Z}) = 2\mathbb{Z}$, а $B^1(\mathbb{C}_2, \mathbb{Z}_2) = 0$. Добијамо да је $H^1(\mathbb{C}_2, \mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$, а $H^1(\mathbb{C}_2, \mathbb{Z}) = \mathbb{Z}_2$. Одредимо и хомоморфизме у тачном низу **63**. Најпре, $\alpha_1[f] = [\alpha \circ f] = [2f] = 0$. Такође је $\beta_1[f] = [\beta \circ f]$ и имамо да је $\beta_1(2\mathbb{Z}) = 0$, а $\beta_1(1 + 2\mathbb{Z}) = 1$. Остављамо читаоцима да се увере да је $\delta^0(k) = k + 2\mathbb{Z}$, за $k \in \{0, 1\}$.

Дакле, имамо низ:

$$0 \longrightarrow \{0\} \xrightarrow{0} \{0\} \xrightarrow{0} \mathbb{Z}_2 \xrightarrow{\cong} \mathbb{Z}/2\mathbb{Z} \xrightarrow{0} \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}_2. \tag{64}$$

Напомена 96 Индуковани низ се заправо наставља у десну страну; следеће групе су $H^2(G, M')$, $H^2(G, M)$, $H^2(G, M'')$, $H^3(G, M')$, итд. Но, пошто се тим групама не бавимо, а нисмо их ни дефинисали, тај део нисмо ни исписивали. ♠

Теорема 97 Ако је L/K коначно Галоаово раширење, онда је $H^1(G, L^\times) = 0$, где је $G = G(L/K)$.

Доказ. Треба доказати да је сваки укрштени хомоморфизам $f\colon G \to L^\times$ главни, тј. да постоји елемент $\gamma \in L^\times$ тако да је $f(\sigma) = \frac{\sigma\gamma}{\gamma}$ (користимо наравно мултипликативну нотацију, јер је G-модул са којим радимо $L^\times$). Ако је $\tau \in G$, онда је $f(\tau) \neq 0$. Како су аутоморфизми из G линеарно независни (видети последицу **45**), имамо да је

$$\sum_{\tau \in G} f(\tau)\tau \neq 0\colon L \to L.$$

Дакле, постоји $\alpha \in L$ тако да је

$$\sum_{\tau \in G} f(\tau)\tau(\alpha) \neq 0.$$

Означимо овај ненула елемент са β. Ако је $\sigma \in G$:

$$\begin{aligned}
\sigma(\beta) &= \sum_{\tau \in G} \sigma(f(\tau))\sigma(\tau(\alpha)) \\
&= \sum_{\tau \in G} \frac{f(\sigma\tau)}{f(\sigma)}(\sigma\tau)(\alpha) \\
&= \frac{1}{f(\sigma)} \sum_{\tau \in G} f(\sigma\tau)(\sigma\tau)(\alpha) \\
&= \frac{1}{f(\sigma)} \sum_{\theta \in \sigma G} f(\theta)\theta(\alpha) \\
&= \frac{1}{f(\sigma)} \sum_{\theta \in G} f(\theta)\theta(\alpha) \\
&= \frac{1}{f(\sigma)}\beta.
\end{aligned}$$

Овде смо наравно користили чињеницу да је f укрштени хомоморфизам што у мултипликативној нотацији даје:

$$f(\sigma\tau) = f(\sigma) \cdot (\sigma \bullet f(\tau)) = f(\sigma) \cdot \sigma(f(\tau)).$$

Дакле,

$$f(\sigma) = \frac{\beta}{\sigma(\beta)} = \frac{\sigma(\beta^{-1})}{\beta^{-1}},$$

те је тражено γ заправо β^{-1}. □

За Галоаово раширење L/K могуће је дефинисати два пресликавања — норму ($\mathrm{Nm}_{L/K}$) и траг ($\mathrm{Tr}_{L/K}$) на следећи начин.

$$\mathrm{Nm}_{L/K}(\alpha) := \prod_{\tau \in G} \tau(\alpha), \qquad \mathrm{Tr}_{L/K}(\alpha) := \sum_{\tau \in G} \tau(\alpha).$$

Стандардно добијамо да је за све $\sigma \in G$:

$$\sigma(\mathrm{Nm}_{L/K}(\alpha)) = \mathrm{Nm}_{L/K}(\alpha) \quad \text{и} \quad \sigma(\mathrm{Tr}_{L/K}(\alpha)) = \mathrm{Tr}_{L/K}(\alpha),$$

те заправо имамо да

$$\mathrm{Nm}_{L/K} \colon L^\times \to K^\times \quad \text{и} \quad \mathrm{Tr}_{L/K} \colon L \to K.$$

Пример 98 За раширење $\mathbb{Q}(i)/\mathbb{Q}$, имамо:

$$\mathrm{Nm}_{\mathbb{Q}(i)/\mathbb{Q}}(a+bi) = (a+bi)(a-bi) = a^2 + b^2,$$

док је у случају раширења $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$:

$$\mathrm{Nm}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(a+b\sqrt{2}) = (a+b\sqrt{2})(a-b\sqrt{2}) = a^2 - 2b^2. \qquad \clubsuit$$

Године 1893. *Немачко математичко друштво* је задужило младе математичаре Давида Хилберта и Хермана Минковског да припреме извештај о резултатима из теорије бројева, до којих су у претходним деценијама дошли превасходно немачки математичари и за тај посао су им дали две године. Минковски је добио задужење да се позабави елементарнијим питањима, а Хилберт алгебарском теоријом бројева. Хилберт је врло озбиљно приступио на посао, а Минковски и није био за то заинтересован. Тако да је на крају само Хилберт објавио свој *Zahlbericht — Извештај о бројевима* (у преводу Google translate: Извештај о плаћању ☺) 1897. године. У њему је доказао, под бројем 90, следећу теорему, која представља генерализацију Кумеровог резултата из тридесетих година XIX века о циклотомичним раширењима. Она је постала позната као Хилбертова теорема 90.

Последица 99 Нека је L коначно циклично раширење од K степена n и нека је $G(L/K) = \langle\sigma\rangle$. Ако је $\alpha \in L^\times$ такав да је $\mathrm{Nm}_{L/K}(\alpha) = 1_K$, онда је $\alpha = \beta/\sigma(\beta)$ за неко $\beta \in L$.

Доказ. Како је $1 = \mathrm{Nm}_{L/K}(\alpha) = \alpha \cdot \sigma(\alpha) \cdots \sigma^{n-1}(\alpha)$, на основу примера **91** имамо да је са $f(\sigma) = \alpha$ задат један укрштени хомоморфизам. На основу теореме **97** добијамо да је он главни, те постоји β такво да је $\alpha = \beta/\sigma(\beta)$ (приметимо да у доказу те теореме добијамо $f(\sigma)$ баш у овом облику). □

Пример 100 Како за дато α, наћи тражено β? Ево најједноставнијег случаја где се појављује ова теорема. Могли бисмо га назвати „Хилбертова теорема 90 у средњој школи". Нека је z комплексан број јединичног модула такав да је $z \neq -1$. Тада је

$$z = \frac{1+z}{1+\overline{z}}. \tag{65}$$

Ово се може непосредно генерализати на следећи начин. Нека је L/K Галоаово раширење такво да је $G(L/K) = \langle\sigma\rangle$ циклична група реда 2, $\alpha \in L\{-1\}$ такав да је $\alpha \cdot \sigma(\alpha) = 1 (= 1_K)$. Тада је

$$\alpha = \frac{1+\alpha}{1+\sigma(\alpha)}, \tag{66}$$

те за β можемо узети $1+\alpha$. Како бисмо проширили овај метод на случај цикличне групе реда 3? Нека је $\alpha \in L$ такав да је $\alpha \cdot \sigma(\alpha) \cdot \sigma^2(\alpha) = 1$. Наслућује се шта треба урадити. Посматрамо $\beta = 1 + \alpha + \alpha \cdot \sigma(\alpha)$. Уколико је овај елемент различит од нуле, непосредна провера даје

$$\alpha = \frac{1+\alpha+\alpha\cdot\sigma(\alpha)}{1+\sigma(\alpha)+\sigma(\alpha)\cdot\sigma^2(\alpha)}. \tag{67}$$

Није тешко видети да се ово може проширити и на случај произвољне цикличне групе кад је одговарајући елемент, чијом сликом желимо да делимо, различит од нуле. Уколико је, пак, он једнак нули, онда то треба мало „промешати", тј. посматрати елемент (за случај цикличне групе реда 3): $\beta = \theta + \sigma(\theta)\cdot\alpha + \sigma^2(\theta)\cdot\alpha\cdot\sigma(\alpha)$. Уверите се да увек постоји $\theta \in L$ за који је $\beta \neq 0$ и да је, под претпоставком да је $\mathrm{Nm}_{L/K}(\alpha) = 1$ испуњено: $\alpha = \frac{\beta}{\sigma(\beta)}$. ♣

Позабавимо се сада адитивном варијантом Теореме **97**.

Теорема 101 Ако је L/K циклично раширење, онда је $H^1(G, L^+) = \{0\}$, где је $G = G(L/K)$.

Доказ. Нека је $G = \langle\sigma\rangle$ циклична група реда n. Нека је $f : G \to L^+$ укрштени хомоморфизам. По теореми **77**, постоји нормалан елемент $\alpha \in L$ и нормална база $[\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)]$. Тада је

$$f(\sigma) = c_0\alpha + c_1\sigma(\alpha) + \cdots + c_{n-1}\sigma^{n-1}(\alpha),$$

за неке $c_i \in K$. Покажимо да постоји $\beta \in L$ такав да је $\beta - \sigma(\beta) = f(\sigma)$. Нека је $\beta = d_0\alpha + d_1\sigma(\alpha) + \cdots + d_{n-1}\sigma^{n-1}(\alpha)$. Тада је

$$\sigma(\beta) = d_0\sigma(\alpha)+d_1\sigma^2(\alpha)+\cdots+d_{n-1}\sigma^n(\alpha) = d_{n-1}\alpha+d_0\sigma(\alpha)+\cdots+d_{n-2}\sigma^{n-1}(\alpha).$$

Услов $\beta-\sigma(\beta) = f(\sigma)$ нам каже да, за налажење β треба решити систем једначина

$$\begin{array}{rrcrcl} d_0 & & & & -d_{n-1} & = & c_0 \\ -d_0 & +d_1 & & & & = & c_1 \\ & & \ddots & & & \vdots & \\ & & & -d_{n-2} & +d_{n-1} & = & c_{n-1}. \end{array}$$

Приметимо да, ако саберемо све једначине са леве стране добијамо 0, стога је потребно да је и $c_0 + c_1 + \cdots + c_{n-1} = 0_K$. Но, ми знамо да је f укрштени хомоморфизам и да је $\sigma^n = id_L$. Стога је (видети пример **91**)

$$f(\sigma) + \sigma(f(\sigma)) + \cdots + \sigma^{n-1}(f(\sigma)) = 0_L. \tag{68}$$

Но, $\sigma^k(f(\sigma)) = c_0\sigma^k(\alpha) + c_1\sigma^{k+1}(\alpha) + \cdots + \sigma^{k+n-1}(\alpha)$, те се једначина **68** своди на (проверите):

$$(c_0 + c_1 + \cdots + c_{n-1})(\alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha)) = 0_L,$$

те закључујемо да је заиста $c_0 + c_1 + \cdots + c_{n-1} = 0_K$. Горњи систем једначина има решење:

$$\begin{aligned} d_1 &= c_1 + d_0 \\ d_2 &= c_2 + c_1 + d_0 \\ &\vdots \\ d_{n-1} &= c_{n-1} + \cdots + c_1 + d_0, \end{aligned}$$

где d_0 може бити произвољан елемент из K. Дакле, добили смо да је, за тако изабрано β, $f(\sigma) = \beta - \sigma(\beta)$. Но, тада је и

$$f(\sigma^2) = f(\sigma) + \sigma(f(\sigma)) = \beta - \sigma(\beta) + \sigma(\beta - \sigma(\beta)) = \beta - \sigma^2(\beta)$$

и индукцијом се лако показује да је за све k: $f(\sigma^k) = \beta - \sigma^k(\beta)$, те је за све $\tau \in G$: $f(\tau) = \tau(-\beta) - (-\beta)$, те је f главни укрштени хомоморфизам, тј. $H^1(G, L^+) = \{0\}$. □

Последица ове теореме је адитивна верзија Хилбертове теореме 90.

Последица 102 Нека је L коначно циклично раширење од K и нека је $G(L/K) = \langle\sigma\rangle$. Ако је $\gamma \in L$ такав да је $\mathrm{Tr}_{L/K}(\gamma) = 0_K$, онда је $\gamma = \beta - \sigma(\beta)$ за неко $\beta \in L$.

Доказ. Са $f(\sigma) = \gamma$ је задат један укрштени хомоморфизам и резултат следи из горњег доказа. □

За крај наведимо пар коментара. Најпре, о појму укрштеног хомоморфизма. Чини се да је он мало вештачки уведен, али то није тако. Заправо се укрштени хомоморфизам појављује у проблемима раширења (екстензије) група, посебно у случају семидиректног производа.

Ако имамо тачан низ група

$$1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1 \tag{69}$$

онда кажемо да је група G РАШИРЕЊЕ групе H помоћу групе N. Приметимо да овде радимо са општим групама, које не морају бити комутативне. Занимљиво је питање да ли раширење (**69**) има сечење. Лево сечење је хомоморфизам $\sigma\colon G \to N$ такав да је $\sigma \circ \alpha = \mathrm{Id}_N$, док је десно сечење хомоморфизам $\tau\colon H \to G$ такав да је $\beta \circ \tau = \mathrm{Id}_H$. Важно је напоменути две ствари.

1. Не мора постојати ни лево ни десно сечење. Најједноставнији пример је раширење

$$0 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 0.$$

2. У случају да су све групе Абелове, постојање левог и десног сечења је еквивалентно.

Посматрајмо општи случај раширења (**69**). Постојање левог сечења σ нам показује да је $G \cong N \times H$. Наиме, можемо дефинисати хомоморфизам $\phi\colon G \to N \times H$ са $\phi(g) = (\sigma(g), \beta(g))$. Покажимо да је ово један изоморфизам. Нека је $(n, h) \in N \times H$. Како је β „на", постоји $g \in G$ тако да је $\beta(g) = h$. Ако је $\sigma(g) = n_0$, добијамо да је

$$\phi(\alpha(nn_0^{-1})g) = (\sigma(\alpha(nn_0^{-1})g), \beta(\alpha(nn_0^{-1})g)) = (nn_0^{-1}\sigma(g), e_H\beta(g)) = (n, h).$$

Дакле, ϕ је „на". Уколико је $\phi(g) = (e_N, e_H)$, добијамо да је $\beta(g) = e_H$, па је $g = \alpha(n)$ за неко $n \in N$. Но, тада је $e_N = \sigma(g) = \sigma(\alpha(n)) = n$. Стога је $g = \alpha(e_N) = e_G$.

Постојање десног сечења τ нема такав ефекат. Нека је $H_1 = \tau[H]$ и $N_1 = \alpha[N]$. Покажимо да важи следеће:

$$N_1 \lhd G, \quad N_1 \cap H_1 = \{e_G\}, \quad N_1H_1 = G.$$

Наравно да је прва ствар јасна пошто је $N_1 = \operatorname{Ker}\beta$. Уколико $g \in N_1 \cap H_1$, имамо да је $\beta(g) = e_H$, пошто $g \in \operatorname{Ker}\beta$. Но, с друге стране је $g = \tau(h)$ за неки $h \in H$. Стога је $e_H = \beta(g) = \beta(\tau(h)) = h$. Следи да је $g = \tau(e_H) = e_G$. Коначно, ако је $g \in G$, посматрајмо елемент $g(\tau(\beta(g)))^{-1}$. Он се са β слика у e_H, те припада N_1. Стога је $g =$

$(g(\tau(\beta(g)))^{-1})\tau(\beta(g))$. Први фактор је из N_1, а други из H_1, па је и трећа релација испуњена. Ово управо значи да је H семидиректан производ своје нормалне подгрупе N_1 и подгрупе H_1: $G = N_1 \rtimes H_1$. Дакле, постоји бијекција између G и $N \times H$, само што то није хомоморфизам ако је операција у $N \times H$ она у директном производу. Ради се о другој операцији. Но, ако се идентификује овако G са $N \times H$, онда сечењу τ одговара хомоморфизам $H \to N \times H$: $h \mapsto (f(h), h)$. Уколико је N Абелова група, имамо пресликавање $f\colon H \to N$ које је укрштени хомоморфизам. Детаље нећемо проверавати.

Нека је G група и M један G-модул. Ако је

$$C^n(G, M) = \{f : G^n \to M\}, \text{ за } n \geq 0$$

(у случају да је $n = 0$, имамо идентификацију $C^0(G, M)$ и M), онда су ово Абелове групе (операција $+$ се задаје помоћу сабирања у M). Можемо посматрати низ група и хомоморфизама

$$0 \to C^0(G, M) \xrightarrow{d^0} C^1(G, M) \xrightarrow{d^1} C^2(G, M) \xrightarrow{d^2} C^3(G, M) \to \cdots$$

при чему су d^n дефинисани са:

$$\begin{aligned}
d^0(m)(\sigma) &= \sigma \bullet m - m,\\
d^1(f)(\sigma, \tau) &= \sigma \bullet f(\tau) - f(\sigma\tau) + f(\sigma),\\
d^2(f)(\sigma, \tau, \theta) &= \sigma \bullet f(\tau, \theta) - f(\sigma\tau, \theta) + f(\sigma, \tau\theta) - f(\sigma, \tau)\\
&\vdots\\
d^n(f)(\sigma_0, \sigma_1, \ldots, \sigma_n) &= \sigma_0 \bullet f(\sigma_1, \ldots, \sigma_n) - f(\sigma_0\sigma_1, \ldots, \sigma_n)\\
&\quad + f(\sigma_0, \sigma_1\sigma_2, \ldots, \sigma_n) - + \cdots + (-1)^{n+1} f(\sigma_0, \ldots, \sigma_{n-1}).
\end{aligned}$$

Горенаведени низ није тачан, али је испуњено: $d^n \circ d^{n-1} = 0$ за све $n \geq 0$ (за $C^{-1}(G, M)$ узимамо 0). Приметимо:

1. $\mathrm{Im}(d^0)$ чине главни укрштени хомоморфизми.
2. $\mathrm{Ker}(d^1)$ чине укрштени хомоморфизми.
3. $\mathrm{Ker}(d^0) = M^G$.

Ако је $Z^n(G, M) := \mathrm{Ker}\, d^n$, а $B^n(G, M) := \mathrm{Im}\, d^{n-1}$, онда дефинишемо кохомолошке групе са:

$$H^n(G, M) := Z^n(G, M)/_{B^n(G, M)}.$$

Видимо да кохомологија мери одступање горенаведеног низа од тачности, као и да се прве две кохомологије поклапају са оним које смо претходно дефинисали.

За сам крај, наведимо да ако је L/K коначно Галоаво раширење, $G = G(L/K)$, онда је заправо $H^n(G, L^+) = 0$ за све $n \geq 1$. Ово такође следи из теореме о нормалној бази, али то је нека друга прича.

15 Циклична и Кумерова раширења

Дефиниција 103 За раширење L/K кажемо да је Абелово, ако је група $G(L/K)$ Абелова, а циклично, уколико је $G(L/K)$ циклична.

15.1 Циклична раширења

Нека је K поље које садржи примитивни n-ти корен из јединице и нека је $\operatorname{char} K = 0$, или је $\operatorname{char} K = p$, где $p \nmid n$. Са $\mu_n(K)$ означавамо скуп свих n-тих корена из јединице у K:

$$\mu_n(K) := \{\alpha \in K : \alpha^n = 1_K\}.$$

Тада је $\mu_n(K) \leq K^\times$ и то је циклична група реда n генерисана ма којим примитивним n-тим кореном из јединице. У овом пододељку класификујемо циклична раширења од K степена n.

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.

Став 104 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 $1 \leq s < n$. 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 $1 \leq s < n$.

Доказ. Нека је $a = \alpha^n \in K$. Посматрајмо полином $f = X^n - a \in K[X]$. Његове нуле су $\zeta^i\alpha$, за $0 \leq i < n$, где је $\zeta \in K$ неки примитивни n-ти корен из јединице. Стога је $L = K_f = K(\alpha)$. Како је $f' = nX^{n-1} \neq 0$, полином f је сепарабилан, раширење L/K је Галоаово и f је минимални полином елемента α над K. Нека је $G = G(L/K)$. Желимо да докажемо да је G циклична група. Ако $\sigma \in G$, онда је $\sigma(\alpha)^n = \sigma(\alpha^n) = \sigma(a) = a$, па је $\sigma(\alpha) = \zeta^i\alpha$ за неко i. Дакле, $\sigma(\alpha)/\alpha = \zeta^i$ па је $(\sigma(\alpha)/\alpha)^n = 1$. Стога можемо да дефинишемо пресликавање $h\colon G \to \mu_n(K)$ са: $h(\sigma) = \sigma(\alpha)/\alpha$. Покажимо да је ово хомоморфизам.

$$h(\sigma\tau) = \frac{(\sigma\tau)(\alpha)}{\alpha} = \frac{\sigma(\tau(\alpha))}{\alpha} = \frac{\sigma(\tau(\alpha))}{\tau(\alpha)}\frac{\tau(\alpha)}{\alpha}.$$

Но, како је $\tau(\alpha) = \zeta^k\alpha$ за неко k:

$$h(\sigma\tau) = \frac{\sigma(\zeta^k\alpha)}{\zeta^k\alpha}\frac{\tau(\alpha)}{\alpha} = \frac{\zeta^k\sigma(\alpha)}{\zeta^k\alpha}\frac{\tau(\alpha)}{\alpha} = \frac{\sigma(\alpha)}{\alpha}\frac{\tau(\alpha)}{\alpha} = h(\sigma)h(\tau).$$

Докажимо да је h заправо изоморфизам. Уколико је $\sigma \in \operatorname{Ker} h$, тј. $h(\sigma) = 1_K$, онда је $\sigma(\alpha)/\alpha = 1_K$, те је $\sigma(\alpha) = \alpha$, па је $\sigma = \operatorname{Id}_L$. Како је $\operatorname{Im} h \leq \mu_n(K)$, а знамо да свака циклична група садржи тачно једну

подгрупу датог реда, то мора бити заправо $\operatorname{Im} h = \mu_d(K)$ за неко d, такво да $d \mid n$. Добијамо да је за све $\sigma \in G$: $h(\sigma)^d = 1_K$, те је за све $\sigma \in G$: $(\sigma(\alpha)/\alpha)^d = 1_K$, тј. за све $\sigma \in G$: $\sigma(\alpha^d) = \alpha^d$. Закључујемо да $\alpha^d \in L^G = K$. Како по претпоставци $\alpha^s \notin K$ за $1 \leq s < n$, закључујемо да је $d = n$, те је h и „на". Тако смо добили да је $G \cong \mu_n(K)$, а $\mu_n(K)$ је циклична група реда n.

Претпоставимо сада да је L циклично раширење од K степена n. Дакле, $G(L/K) = \langle\sigma\rangle$, при чему је $\omega(\sigma) = n$. Покажимо да постоји $\alpha \in L \setminus \{0\}$ тако да је $\sigma(\alpha) = \zeta^{-1}\alpha$.

Према теореми о нормалној бази, постоји $\gamma \in L$ тако да је

$$e = [\gamma, \sigma(\gamma), \ldots, \sigma^{n-1}(\gamma)]$$

једна база за векторски простор L над пољем K. Приметимо да је матрица оператора σ у овој бази:

$$[\sigma]_e = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}.$$

Посматрајмо вектор α такав да је $\alpha_e = [1, \zeta, \zeta^2, \ldots, \zeta^{n-1}]^T$, где са v_e означавамо колону координата овог вектора у бази e. Тада је

$$\sigma(\alpha)_e = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ \zeta \\ \zeta^2 \\ \vdots \\ \zeta^{n-1} \end{bmatrix} = \begin{bmatrix} \zeta^{n-1} \\ 1 \\ \zeta \\ \vdots \\ \zeta^{n-2} \end{bmatrix} = \zeta^{-1} \begin{bmatrix} 1 \\ \zeta \\ \zeta^2 \\ \vdots \\ \zeta^{n-1} \end{bmatrix} = \zeta^{-1}\alpha_e.$$

Дакле, $\sigma(\alpha) = \zeta^{-1}\alpha$.

Имамо да је $\sigma(\alpha^n) = (\sigma(\alpha))^n = (\zeta^{-1}\alpha)^n = \zeta^{-n}\alpha^n = \alpha^n$, те закључујемо да $\alpha^n \in K$.

Уколико $\alpha^s \in K$ за неко $1 \leq s < n$, онда је $\sigma(\alpha^s) = \alpha^s$. Но, како је $\sigma(\alpha) = \zeta^{-1}\alpha$, добијамо да је $\zeta^{-s}\alpha^s = \alpha^s$, па би следило да је $\zeta^s = 1$, што наравно није тачно. Дакле, $\alpha^s \notin K$ за $1 \leq s < n$.

Покажимо да је $L = K(\alpha)$. Како је $\sigma^k(\alpha) = \zeta^{-k}\alpha$ и ово су све различити елементи за $0 \leq k < n$, то орбита елемента α при дејству групе G има $n = |G|$ елемената. Дакле, стабилизатор овог елемента је тривијална подгрупа. Но, то је заправо подгрупа $K(\alpha)^\sharp$. Дакле, $K(\alpha)^\sharp = \{\mathrm{id}_L\}$, па је $K(\alpha) = (K(\alpha)^\sharp)^\flat = \{\mathrm{id}_L\}^\flat = L$. □