Jón Kristinn Arason

Galois

Vor 2016

Inngangur

Allt fram til miðrar 19. aldar var það höfuðverkefni í algebru að leysa það sem við nú köllum algebrulegar jöfnur. Þetta eru jöfnur af taginu

$$a_0 + a_1 x + \cdots + a_n x^n = 0$$

þar sem x er óþekkt. Menn gerðu sér það snemma ljóst að til að leysa slíkar jöfnur þyrfti meira til en grunnreiknigerðirnar fjórar — samlagningu, frádrátt, margföldun og deilingu. Babylóníumenn uppgötvuðu að til þess að leysa jöfnur af annarri gráðu, þ.e.a.s. jöfnur af taginu

$$a_0 + a_1 x + a_2 x^2 = 0$$

þar sem $a_2 \neq 0$, þurfti aðeins að bæta við einni reiknigerð — ferningsrótardrætti. Nú á dögum þekkja allir almennu lausnina

$$x = \frac{-a_1 \pm \sqrt{{a_1}^2 - 4a_0a_2}}{2a_2}$$

Forngrikkir enduruppgötvuðu þetta með rúmfræðilegri framsetningu. Þeir reyndu að leysa almennu jöfnuna á sama hátt en tókst ekki. Arabískir eftirmenn þeirra innleiddu nýjar reiknigerðir — almenna rótardrætti. Evrópubúar miðalda lærðu stærðfræði af aröbum og reyndu að leysa almennu jöfnuna með rótardráttum (og, að sjálfsögðu, grunnreiknigerðunum fjórum). Á fyrri hluta 16. aldar tókst þeim, eftir þriggja alda leit, að finna almennu lausnina á þriðju gráðu jöfnunni. Skömmu síðar fannst almenna lausnin á fjórðu gráðu jöfnunni. Eftir langa leit að almennu lausninni á fimmtu gráðu jöfnunni kom í ljós á fyrri hluta 19. aldar að slík lausn var ekki til ef menn einskorðuðu sig við rótardrætti (og grunnreiknigerðirnar fjórar). Það var norðmaðurinn Abel sem fyrstur sýndi fram á þetta og frakkinn Galois sem skýrði leysanleika n-tu gráðu jöfnunnar.

Hér ætlum við að fjalla um niðurstöður Abels og Galois. Við munum að sjálfsögðu nota nútímalegt orðafar og hugsunarhátt. Sér í lagi munum við alltaf gera ráð fyrir að stuðlarnir $a_0, a_1, \ldots, a_n$ í jöfnunni hér að ofan séu í einhverjum kroppi K. (Það þýðir að við gerum ráð fyrir að grunnreiknigerðirnar fjórar séu til taks.)

Ef við táknum margliðuna $a_0 + a_1 X + \cdots + a_n X^n$ með $f(X)$ þá er það að leysa jöfnuna hér að ofan jafngilt því að finna stak r þannig að $f(r) = 0$, þ.e. að finna rót r á f. Þessi staðreynd tengir athuganir á lausnum algebrulegra

jafna yfir K athugunum á margliðubaugnum $K[X]$ yfir K. Þessi tenging kemur sérlega í ljós í vel kunnri setningu sem hér fer á eftir.

Setning 1. Stak r í K er rót á margliðunni $f(X)$ yfir K þá og því aðeins að $X - r$ gangi upp í $f(X)$.

Sönnunin á þessari setningu er líka vel kunn, svo að óþarfi er að endurtaka hana hér. Við minnum þó á að hún byggist á því að setningin um deilingu með afgangi gildir í margliðubaugnum. Á þeirri setningu hvílir líka sú staðreynd að í $K[X]$ gildir setningin um frumþáttun.

Af Setningu 1 fæst svo eftirfarandi setning (með þrepun yfir gráðuna).

Setning 2. Margliða $f(X)$ af gráðu $n \geq 1$ yfir K hefur í mesta lagi n rætur í K.

Við þekkjum mörg dæmi þess að margliða $f(X)$ yfir K hafi enga rót í K en hafi rót í stærri kroppi L. Til dæmis hefur margliðan $X^2 + 1$ enga rót í $\mathbf{R}$ en hefur rót í $\mathbf{C}$. Margliðan $X^2 - 2$ hefur enga rót í $\mathbf{Q}$ en hefur rót í $\mathbf{R}$. Margliðan $X^3 - 2$ hefur enga rót í $\mathbf{Q}$ en hefur rót í $\mathbf{R}$. Af eftirfarandi setningu sést að þetta eru ekki tilviljanir.

Setning 3. Gefin sé margliða $f(X)$ af gráðu ≥ 1 yfir K. Þá er til kroppur L, sem inniheldur K sem hlutkropp, þannig að $f(X)$ hefur rót í L.

Sönnun. Vegna setningarinnar um frumþáttun í margliðubaugnum $K[X]$ nægir að sanna setninguna fyrir staðlaðar frummargliður $f(X)$ yfir K. Við látum þá $L = K[X]/K[X]f(X)$ og samsömum K við mynd hans í L. Ljóst er að mynd X í L er rót á $f(X)$.

Athugasemd. Gefin sé stöðluð frummargliða $f(X)$ af gráðu n yfir K. L sé eins og í sönnuninni og x sé mynd X í L. Af setningunni um deilingu með afgangi í $K[X]$ leiðir þá að sérhvert stak í L má skrifa á einn og aðeins einn hátt á forminu $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ með $a_0, a_1, \ldots, a_{n-1}$ í K.

Ef til dæmis $K = \mathbf{R}$ og $f(X) = X^2 + 1$ þá fæst $L = \{a + bx \mid a, b \in \mathbf{R}\}$. Auk þess gildir $x^2 + 1 = 0$, þ.e. $x^2 = -1$. Hér er L því í raun það sama og $\mathbf{C}$.

Ef $K = \mathbf{Q}$ og $f(X) = X^2 - 2$ þá fæst $L = \{a + bx \mid a, b \in \mathbf{Q}\}$. Auk þess gildir $x^2 - 2 = 0$, þ.e.a.s. $x^2 = 2$.

Ef $K = \mathbf{Q}$ og $f(X) = X^3 - 2$ þá fæst $L = \{a + bx + cx^2 \mid a, b, c \in \mathbf{Q}\}$. Auk þess gildir $x^3 - 2 = 0$, þ.e.a.s. $x^3 = 2$.

Lokasetningin í þessum inngangi samsvarar Setningu 3 fyrir verkefnið að finna „allar“ rætur margliðunnar.

Setning 4. Gefin sé margliða $f(X)$ af gráðu ≥ 1 yfir K. Þá er til kroppur L, sem inniheldur K sem hlutkropp, þannig að $f(X)$ klofnar í línulega þætti yfir L.

Sönnun. Þetta fæst af Setningu 3 með þrepun.

Það að margliðan $f(X)$ í setningunni klofnar í línulega þætti yfir L þýðir að skrifa má $f(X) = c_0(X - c_1) \cdots (X - c_n)$ með $c_0, c_1, \ldots, c_n \in L$. (Ljóst er þó að $c_0 \in K$.) Við segjum oftast einfaldlega að $f(X)$ klofni yfir L.

Spurningunni um lausnir algebrulegra jafna er alls ekki fullsvarað með Setningum 3 og 4. Eftir er að athuga hvaða L duga, hvaða samband er á milli tveggja L sem duga, hvort til er eitthvert „bezta“ L sem dugar o.s.frv. Í því sem á eftir fer munum við almennt athuga kroppa L sem innihalda K sem hlutkropp.

1 Útvíkkanir kroppa

Í þessum kafla táknar K alltaf kropp.

Kroppur L, sem inniheldur K sem hlutkropp, er sagður vera útvíkkun á kroppinum K. Í stað útvíkkana á K er einnig talað um kroppa yfir K. Þá er gjarna skrifað L/K í stað $K \subseteq L$.

Kroppurinn L sé útvíkkun á K. Gefið sé hlutmengi S í L. Auðvelt er að sjá að sniðmengi allra hlutútvíkkana á K í L sem innihalda S er hlutútvíkkun á K í L. Því er til minnsta hlutútvíkkun á K í L sem inniheldur S. Hún er kölluð hlutútvíkkunin á K í L sem spönnuð er af S og er táknuð $K(S)$.

Kroppurinn L er sér í lagi víxlin K-algebra. Við getum því eins athugað allar hlut-K-algebrur í L sem innihalda S. Sniðmengi þeirra er þá minnsta hlut-K-algebran í L sem inniheldur S. Hún er kölluð hlut-K-algebran í L sem spönnuð er af S og er táknuð $K[S]$. Þá er $K(S)$ greinilega mengi allra brota x/y, þar sem $x, y \in K[S]$, $y \neq 0$.

Ef $S = \{s_1, \ldots, s_n\}$ er endanlegt þá er venjulega skrifað $K[s_1, \ldots, s_n]$ í stað $K[S]$ og $K(s_1, \ldots, s_n)$ í stað $K(S)$. Ljóst er að $K[s_1, \ldots, s_n]$ er mengi allra $f(s_1, \ldots, s_n)$ þar sem f er margliða í n breytum yfir K. Því fæst að $K(s_1, \ldots, s_n)$ er mengi allra brota $f(s_1, \ldots, s_n)/g(s_1, \ldots, s_n)$, þar sem f og g eru margliður í n breytum yfir K þannig að $g(s_1, \ldots, s_n) \neq 0$.

Almennt er $K[S]$ er sammengi allra $K[s_1, \ldots, s_n]$ þar sem $\{s_1, \ldots, s_n\}$ er endanlegt hlutmengi í S. Af þessu leiðir að $K(S)$ er sammengi allra $K(s_1, \ldots, s_n)$ þar sem $\{s_1, \ldots, s_n\}$ er endanlegt hlutmengi í S.

Útvíkkun L á K er sögð vera endanlega spönnuð ef til er endanlegt hlutmengi S í L þannig að $L = K(S)$.

Setning 1. Ef L er endanlega spönnuð útvíkkun á K og M er endanlega spönnuð útvíkkun á L þá er M endanlega spönnuð útvíkkun á K.

Sönnun. Ef $L = K(S)$ og $M = L(T)$ þá er $M = K(S \cup T)$.

Raunar er líka ljóst að ef $K \subseteq L \subseteq M$ eru útvíkkanir þannig að M er endanlega spönnuð yfir K þá er M líka endanlega spönnuð yfir L.

Útvíkkun L á K er sögð vera einföld ef til er stak s í L þannig að $L = K(s)$. Ef svo er þá er s sagt vera frumstætt stak fyrir útvíkkunina L á K.

L sé útvíkkun á K og s sé stak í L. Vörpunin frá $K[X]$ yfir í L, sem varpar margliðunni f yfir í $f(s)$, er þá mótun K-algebra. Við vitum að $K[s]$ er mynd þessarar mótunar.

Ef þessi mótun er eintæk þá er sagt að stakið s í L sé torrætt yfir K. Þá gefur mótunin af sér einsmótun frá $K[X]$ yfir á $K[s]$. Af því leiðir að $K(s)$ er einsmóta $K(X)$, kroppi ræðra falla yfir K.

Gerum nú ráð fyrir að mótunin sé ekki eintæk. Það þýðir að til er margliða f yfir K, $f \neq 0$, þannig að $f(s) = 0$. Þá er sagt að stakið s í L sé algebrulegt yfir K. Kjarni mótunarinnar er íðal I í $K[X]$ og $I \neq \{0\}$. Það er því til ótvírætt ákvörðuð stöðluð margliða p yfir K þannig að $I = K[X]p$. Það þýðir að $f(s) = 0$ þá og því aðeins að p gangi upp í f. Þessi margliða p er kölluð lágmargliða s yfir K og gráða p er líka kölluð gráða s yfir K. Mótunin gefur nú af sér einsmótun frá $K[X]/K[X]p$ yfir á $K[s]$. Þar sem $K[s]$ er hlutbaugur í L og því heilbaugur, þá hlýtur p að vera frummargliða yfir K. En þá er $K[X]/K[X]p$ kroppur, svo að $K[s]$ er kroppur. Það þýðir að $K(s) = K[s]$.

Ef $s \in K$ þá er s augljóslega algebrulegt yfir K. Lágmargliðan er $X - s$. Einnig er ljóst að ef s hefur gráðu 1 yfir K þá er $s \in K$.

Útvíkkun L á K er sögð vera algebruleg ef sérhvert stak í L er algebrulegt yfir K.

L sé útvíkkun á K. Þá er L sér í lagi vigurrúm yfir K. Vídd L sem vigurrúms yfir K er kölluð gráða L yfir K og er táknuð $[L : K]$.

$L = K(s)$ sé einföld útvíkkun á K. Ef s er torrætt yfir K þá er $K[s] \subseteq L$ einsmóta $K[X]$. Af því leiðir að gráða L yfir K er óendanleg. Gerum þá ráð fyrir að s sé algebrulegt yfir K og látum p vera lágmargliðu s yfir K. Ef n er gráða p þá leiðir af athugasemd við Setningu 3 í inngangínum að stökin $1, s, \ldots, s^{n-1}$ mynda grunn fyrir L sem vigurrúm yfir K. Því fæst að gráða L yfir K er jöfn gráðu p, þ.e.a.s. jöfn gráðu s yfir K.

Setning 2. Ef L er útvíkkun á K og M er útvíkkun á L þá er

$$[M : K] = [M : L][L : K]$$

Sönnun. Ef $(u_i)_{i \in I}$ er grunnur fyrir L yfir K og $(v_j)_{j \in J}$ er grunnur fyrir M yfir L þá er auðvelt að sjá að $(u_i v_j)_{i \in I, j \in J}$ er grunnur fyrir M yfir K.

Útvíkkun L á K er sögð vera endanleg ef gráðan $[L : K]$ er endanleg.

Setning 3. Ef L er endanleg útvíkkun á K og M er endanleg útvíkkun á L þá er M endanleg útvíkkun á K.

Sönnun. Þetta er augljós afleiðing af Setningu 2.

Raunar er líka ljóst að ef $K \subseteq L \subseteq M$ eru útvíkkanir þannig að M er endanleg yfir K þá er M endanleg yfir L og L endanleg yfir K.

Setning 4. Sérhver endanleg útvíkkun á K er algebruleg.

Sönnun. L sé útvíkkun á K. Ef L er ekki algebruleg útvíkkun á K þá er til stak s í L sem er torrætt yfir K. Við höfum þegar séð að þá er gráðan $[K(s) : K]$ óendanleg. En þá er gráðan $[L : K]$ líka óendanleg.

Augljóst er að sérhver endanleg útvíkkun er endanlega spönnuð.

Setning 5. Ef $L = K(s_1, \ldots, s_n)$ og sérhvert s_i, $i = 1, \ldots, n$, er algebrulegt yfir K þá er L endanleg útvíkkun á K. Auk þess gildir þá að $L = K[s_1, \ldots, s_n]$.

Sönnun. Notum þrepun yfir n. Við höfum þegar séð að þetta er rétt ef $n = 1$. Ef $n > 1$ þá er $K(s_1, \ldots, s_n) = K(s_1, \ldots, s_{n-1})(s_n) = K(s_1, \ldots, s_{n-1})[s_n]$.

Setning 5 segir sér í lagi að sérhver endanlega spönnuð algebruleg útvíkkun sé endanleg.

Setning 6. Ef $L = K(S)$ er útvíkkun á K þannig að sérhvert stak í S er algebrulegt yfir K þá er L algebruleg útvíkkun á K. Auk þess gildir þá að $L = K[S]$.

Sönnun. Ef S er endanlegt þá er þetta afleiðing af Setningum 5 og 4. Almenna tilfellið fæst af því að $K(S)$ er sammengi allra $K(s_1, \ldots, s_n)$, þar sem $\{s_1, \ldots, s_n\}$ er endanlegt hlutmengi í S.

Setning 7. Ef L er algebruleg útvíkkun á K og M er algebruleg útvíkkun á L þá er M algebruleg útvíkkun á K.

Sönnun. Gefið sé stak s í M. Þar sem M er algebruleg útvíkkun á L, þá er til margliða $f \neq 0$ yfir L þannig að $f(s) = 0$. Látum L_0 vera hlutútvíkkunina á K í L sem spönnuð er af stuðlum margliðunnar f. Þá er f margliða yfir L_0 og s því algebrulegt yfir L_0. Sér í lagi er $L_0(s)$ endanleg útvíkkun á L_0. Nú er L_0 endanlega spönnuð algebruleg útvíkkun á K og því endanleg útvíkkun á K samkvæmt Setningu 5. Af Setningu 3 leiðir því að $L_0(s)$ er endanleg útvíkkun á K og því algebruleg samkvæmt Setningu 4. Sér í lagi er s algebrulegt yfir K.

Raunar er líka ljóst að ef $K \subseteq L \subseteq M$ eru útvíkkanir þannig að M er algebruleg yfir K þá er M algebruleg yfir L og L algebruleg yfir K.

Setning 8. L sé útvíkkun á K. Látum L_0 vera mengi allra staka í L sem eru algebruleg yfir K. Þá er L_0 algebruleg útvíkkun á K.

Sönnun. Látum $L_1 = K(L_0)$. Samkvæmt Setningu 6 er L_1 þá algebruleg útvíkkun á K. En þá er $L_1 \subseteq L_0$, þar með $L_1 = L_0$.

L sé útvíkkun á K. Útvíkkunin L_0 í Setningu 8 er þá kölluð algebruleg lokun K í L. Af Setningu 7 leiðir að ekki er til eiginleg algebruleg hlutútvíkkun á L_0 í L. Af Setningu 6 leiðir þá að sérhvert stak í L sem er algebrulegt yfir L_0 er þegar í L_0. Við tjáum þetta með því að segja að L_0 sé algebrulega lokað í L.

Algebruleg lokun $\mathbf{Q}$ í $\mathbf{C}$ er kölluð kroppur algebrulegra talna. Kroppur algebrulegra talna er oft táknaður $\mathbf{A}$.

Við segjum að kroppur sé algebrulega lokaður ef hann hefur enga eiginlega algebrulega útvíkkun. Þetta þýðir að kroppur er algebrulega lokaður þá og því aðeins að hann sé algebrulega lokaður í hvaða útvíkkun sem er.

Setning 9. Eftirfarandi skilyrði fyrir kropp K eru jafngild.
(i) K er algebrulega lokaður.
(ii) Sérhver margliða af gráðu ≥ 1 yfir K hefur rót í K.
(iii) Sérhver frummargliða yfir K er línuleg (hefur gráðu 1).

Sönnun. (i) $\Rightarrow$ (ii): Ef f er margliða af gráðu ≥ 1 yfir K þá er til algebruleg útvíkkun L á K þannig að f hefur rót í L (samanber Setningu 3 í inngangi). Ef K er algebrulega lokaður þá er $L = K$.
(ii) $\Rightarrow$ (iii): Augljóst (samkvæmt Setningu 1 í inngangi).
(iii) $\Rightarrow$ (i): Lágmargliða algebrulegs staks yfir K er frummargliða yfir K. Ef lágmargliðan er línuleg þá er stakið í K.

Ef K er algebrulega lokaður þá klofnar sérhver margliða f yfir K í línulega þætti yfir K, þ.e.a.s. skrifa má $f(X) = c_0(X - c_1) \cdots (X - c_n)$ með stökum $c_0, c_1, \ldots, c_n$ í K. Hin áttin gildir að sjálfsögðu líka.

Í tvinnfallagreiningu er sannað að $\mathbf{C}$ sé algebrulega lokaður kroppur. (Við munum koma með aðra sönnun á því.)

Endanlegur kroppur getur ekki verið algebrulega lokaður. (Sönnun Evklíðs á því að til séu óendanlega margar frumtölur má nota til þess að sýna að til séu óendanlega margar staðlaðar frummargliður yfir hvaða kropp K sem er. En ef K er algebrulega lokaður þá eru einu stöðluðu frummargliðurnar yfir K margliðurnar $X - c$ þar sem $c \in K$.)

Útvíkkun L á K er sögð vera algebruleg lokun á K ef L er algebruleg útvíkkun á K og L er algebrulega lokaður. Skilyrðið má orða þannig að L

sé algebruleg útvíkkun á K þannig að ekki sé til „stærri“ algebruleg útvíkkun á K, þ.e.a.s. algebruleg útvíkkun á K sem inniheldur L sem eiginlegan hlutkropp.

Setning 10. L sé algebrulega lokuð útvíkkun á K. Þá er algebruleg lokun K í L algebrulega lokuð.

Sönnun. Látum L_0 vera algebrulega lokun K í L. Gefin sé margliða f af gráðu ≥ 1 yfir L_0. Þar sem L er algebrulega lokaður, þá hefur f rót s í L. Þar sem $f(s) = 0$, þá er s algebrulegt yfir L_0. Samkvæmt Setningu 7 er s þá algebrulegt yfir K. En þá er s í L_0.

Samkvæmt Setningu 10 er $\mathbf{A}$ algebrulega lokaður kroppur.

L sé algebruleg útvíkkun á K. Ef K er ekki endanlegur þá hefur L sömu fjöldatölu og K. (Látum $\mathbf{c}$ vera fjöldatölu K. Mengi allra staðlaðra margliða af gráðu n yfir K hefur þá fjöldatölu $\mathbf{c}^n$. Hver slík margliða hefur í mesta lagi n rætur í L. Mengi R_n allra staka í L sem eru rót á einhverri staðlaðri margliðu af gráðu n yfir K hefur því fjöldatölu $\leq n\mathbf{c}^n$. Þar sem $\mathbf{c}$ er óendanleg, þá er $n\mathbf{c}^n = \mathbf{c}$. Nú er L sammengi allra R_n, $n = 1, 2, 3, \ldots$, og teljanlegt sammengi mengja með fjöldatölu $\leq \mathbf{c}$, þar sem $\mathbf{c}$ er óendanleg, hefur fjöldatölu $\leq \mathbf{c}$.) Af þessu leiðir t.d. að kroppurinn $\mathbf{A}$ er teljanlegur.

Ef K er endanlegur þá fæst (með svipuðum rökum) að L er teljanlegur.

Setning 11. Sérhver kroppur K hefur algebrulega lokun.

Sönnun. Veljum okkur mengi U sem inniheldur K þannig að fjöldatala U sé stærri en fjöldatala K. Ef K er endanlegur þá veljum við U þannig að U sé auk þess óteljanlegt.

Með lemma Zorns fæst að til er algebruleg útvíkkun L á K sem er innihaldin í U (sem mengi) þannig að ekki sé til eiginleg útvíkkun M á L sem er algebruleg yfir K og er innihaldin í U (sem mengi).

Gerum nú ráð fyrir að L sé ekki algebrulega lokaður. Þá er til eiginleg algebruleg útvíkkun M á L, sem er þá einnig algebruleg útvíkkun á K. Þar sem M hefur sömu fjöldatölu og K (ef K er ekki endanlegur) og U hefur stærri fjöldatölu en K, þá hefur mengjamismunurinn $M \setminus L$ minni fjöldatölu en $U \setminus L$. Það er því til eintæk vörpun $M \setminus L \to U \setminus L$. Það þýðir að við megum gera ráð fyrir að $M \setminus L \subseteq U \setminus L$ og þarmeð $M \subseteq U$. En það er í mótsögn við skilgreinandi eiginleika L. Því hlýtur L að vera algebrulega lokaður.

Ef K er endanlegur þá er M teljanlegur og við fáum eins og áður að $M \setminus L$ hefur minni fjöldatölu en $U \setminus L$.

Við munum brátt sjá að allar algebrulegar lokanir á K eru í eðlilegum skilningi eins.

L_1 og L_2 séu útvíkkanir á K. Kroppamótun $\varphi : L_1 \to L_2$ er sögð vera mótun útvíkkana á K, eða K-mótun, ef $\varphi(a) = a$ fyrir öll $a \in K$.

Allar kroppamótanir eru eintækar. Sér í lagi eru K-mótanir eintækar.

Setning 12. L sé algebruleg útvíkkun á K og $\varphi : L \to L$ sé K-mótun. Þá er φ einsmótun.

Sönnun. Gefið sé $r \in L$. Látum p vera lágmargliðu r yfir K og látum S vera mengi allra róta á p í L. Ljóst er að φ varpar S yfir í S. Þar sem φ er eintæk og S er endanlegt, þá leiðir af þessu að $\varphi(S) = S$. Sér í lagi fæst $r \in \varphi(S)$ og því $r \in \varphi(L)$.

Næstu setningar fjalla um tilvist K-mótana.

Setning 13. $K(r)$ sé einföld algebruleg útvíkkun á K og p sé lágmargliða r yfir K. Gefin sé útvíkkun L á K og stak s í L þannig að $p(s) = 0$. Þá er til ein og aðeins ein K-mótun $\varphi : K(r) \to L$ þannig að $\varphi(r) = s$.

Sönnun. Látum x vera deild X í $K[X]/K[X]p$. Þá er $K[X]/K[X]p = K[x]$. Með $E_r(f) = f(r)$ er skilgreind mótun K-algebra $E_r : K[X] \to K(r)$ sem varpar X í r. Samkvæmt umfjölluninni á undan Setningu 1 gefur E_p af sér K-einsmótun $\varepsilon_r : K[x] \to K(r)$ sem varpar x í r. Á sama hátt fæst K-mótun $\varepsilon_s : K[x] \to L$ sem varpar x í s. Við látum nú $\varphi = \varepsilon_s \circ {\varepsilon_r}^{-1}$. Ljóst er að ekki er til nema ein slík K-mótun φ, því að ε_s er eina mótun K-algebra $K[x] \to L$ sem varpar x í s.

Athugasemd. Þar sem p er frummargliða yfir K og $p(s) = 0$, þá hlýtur p að vera lágmargliða s yfir K.

Ef $\chi : K_1 \to K_2$ er kroppamótun, L_1 er útvíkkun á K_1 og L_2 er útvíkkun á K_2 þá er sagt að kroppamótun $\varphi : L_1 \to L_2$ sé χ-mótun ef $\varphi(a) = \chi(a)$ fyrir öll $a \in K_1$. Svo að K-mótun er þá það sama og id_K-mótun.

Nú sé $K_1(r)$ einföld algebruleg útvíkkun á K_1 og p lágmargliða r yfir K_1. Gefin sé kroppamótun $\chi : K_1 \to K_2$, útvíkkun L_2 á K_2 og stak s í L_2 þannig að $\chi(p)(s) = 0$. (Hér er $\chi(p)$ margliðan yfir K_2 sem fæst með því að nota χ á stuðla margliðunnar p yfir K_1.) Eins og í Setningu 13 fæst þá að til er ein og aðeins ein χ-mótun $\varphi : K_1(r) \to L_2$ þannig að $\varphi(r) = s$.

Segja má að þetta sé ljóst út frá Setningu 13 því að χ gefur af sér einsmótun frá K_1 yfir á $\chi(K_1)$. En athuga ber að $\chi(p)$ þarf ekki að vera frummargliða yfir K_2, svo að $\chi(p)$ þarf ekki að vera lágmargliða s yfir K_2.

Setning 14. L sé algebruleg útvíkkun á K og M sé algebrulega lokuð útvíkkun á K. Þá er til K-mótun $\varphi : L \to M$.

Sönnun. Með lemma Zorns fæst að til er hlutútvíkkun A á K í L og K-mótun $\varphi : A \to M$ þannig að ekki er hægt að framlengja φ á einhverja stærri hlutútvíkkun á K í L.

Gerum nú ráð fyrir að $A \neq L$. Veljum $r \in L$ þannig að $r \notin A$ og látum p vera lágmargliðu r yfir A. Þar sem M er algebrulega lokað, þá hefur $\varphi(p)$ rót s í M. Samkvæmt Setningu 13 (og umræðunni þar á eftir) er til φ-mótun $\chi : A(r) \to M$. En þá er χ líka K-mótun sem útvíkkar φ. Þetta er í mótsögn við eiginleika A og φ. Því hlýtur $A = L$.

Af sönnun Setningar 14 er ljóst að ef L_0 er hlutútvíkkun á K í L og $\varphi_0 : L_0 \to M$ er K-mótun þá má velja K-mótunina φ í setningunni þannig að φ sé framlenging á φ_0.

Það er líka hægt að útvíkka Setningu 14 í anda umræðunnar á eftir Setningu 13. Þá fæst eftirfarandi.

Gefin sé kroppamótun $\chi : K_1 \to K_2$, algebruleg útvíkkun L_1 á K_1 og algebrulega lokuð útvíkkun L_2 á K_2. Þá er til χ-mótun $\varphi : L_1 \to L_2$.

Segja má að þetta sé ljóst út frá Setningu 14 því að χ gefur af sér einsmótun frá K_1 yfir á $\chi(K_1)$.

Setning 15. Sérhverjar tvær algebrulegar lokanir á K eru einsmóta yfir K (þ.e.a.s. K-einsmóta).

Sönnun. L og M séu algebrulegar lokanir á K. Samkvæmt Setningu 14 er til K-mótun $\varphi : L \to M$. Þar sem $\varphi(L)$ er einsmóta L, þá er $\varphi(L)$ algebrulega lokaður. Þar sem $\varphi(L) \subseteq M$ og M er algebruleg útvíkkun á K, þá hlýtur $\varphi(L) = M$.

Gefin sé margliða f af gráðu ≥ 1 yfir K. Við skulum segja að útvíkkun L á K sé rótarkroppur fyrir f yfir K ef f hefur rót í L en ekki í nokkurri eiginlegri hlutútvíkkun á K í L.

Við vitum að til er útvíkkun L á K þannig að f hefur rót í L. Ef $r \in L$ er rót á f þá er ljóst að f hefur rót í $K(r)$, nefnilega rótina r. Þar sem r er algebrulegt yfir K, þá er $K(r)$ endanleg útvíkkun á K. En þá er ljóst að $K(r)$ inniheldur rótarkropp fyrir f yfir K. Það eru því til rótarkroppar fyrir f yfir K og sérhver slíkur er endanlegur yfir K.

Setning 16. f sé frummargliða yfir K og L sé rótarkroppur fyrir f yfir K. Gefin sé útvíkkun M á K þannig að f hafi rót í M. Þá er til K-mótun $\varphi : L \to M$.

Sönnun. Ef $r \in L$ er rót á f þá hefur f rót í $K(r)$. Þar sem L er rótarkroppur fyrir f yfir K, þá leiðir af þessu að $L = K(r)$. Við notum nú Setningu 13.

Setning 17. f sé frummargliða yfir K. Þá eru sérhverjir tveir rótarkroppar fyrir f yfir K einsmóta yfir K.

Sönnun. L og M séu rótarkroppar fyrir f yfir K. Samkvæmt Setningu 16 er til K-mótun $\varphi : L \to M$. Þar sem f hefur rót í L, þá hefur f rót í $\varphi(L)$. En þá hlýtur $\varphi(L) = M$.

Gefin sé margliða f yfir K, $f \neq 0$. Útvíkkun L á K er sögð vera klofningskroppur fyrir f yfir K ef f klofnar yfir L en ekki yfir nokkra eiginlega hlutútvíkkun á K í L.

Við vitum að til er útvíkkun L á K þannig að f klofnar yfir L. Ef við skrifum $f = a(X - c_1) \cdots (X - c_n)$ með $a \in K$ og $c_1, \ldots, c_n \in L$ þá er ljóst að f klofnar yfir $K(c_1, \ldots, c_n)$. Þar sem $c_1, \ldots, c_n$ eru algebruleg yfir K, þá er $K(c_1, \ldots, c_n)$ endanleg útvíkkun á K. En þá er ljóst að $K(c_1, \ldots, c_n)$ inniheldur klofningskropp fyrir f yfir K. Það eru því til klofningskroppar fyrir f yfir K og sérhver slíkur er endanlegur yfir K.

Setning 18. f sé margliða yfir K, $f \neq 0$, og L sé klofningskroppur fyrir f yfir K. Gefin sé útvíkkun M á K þannig að f klofni yfir M. Þá er til K-mótun $\varphi : L \to M$.

Sönnun. Skrifum $f = a(X - c_1) \cdots (X - c_n)$ með $c_1, \ldots, c_n \in L$. Þá klofnar f yfir $K(c_1, \ldots, c_n)$, svo að $L = K(c_1, \ldots, c_n)$. Sér í lagi er L algebruleg útvíkkun á K. Látum N vera algebrulega lokaða útvíkkun á M. Samkvæmt Setningu 14 er þá til K-mótun $\varphi : L \to N$. Með því að nota hana á f fæst að $f = \varphi(f) = a(X - \varphi(c_1)) \cdots (X - \varphi(c_n))$. Þar sem f klofnar yfir M, þá hljóta ræturnar $\varphi(c_i)$, $i = 1, ..., n$, allar að vera í M. En þá er $\varphi(L) = K(\varphi(c_1), \ldots, \varphi(c_n)) \subseteq M$.

Setning 19. f sé margliða yfir K, $f \neq 0$. Þá eru sérhverjir tveir klofningskroppar fyrir f yfir K einsmóta yfir K.

Sönnun. L og M séu klofningskroppar fyrir f yfir K. Samkvæmt Setningu 18 er til K-mótun $\varphi : L \to M$. Þar sem f klofnar yfir L, þá klofnar f yfir $\varphi(L)$. En þá hlýtur $\varphi(L) = M$.

Útvíkka má hugtakið klofningskroppur margliðu. Gefin sé fjölskylda $(f_i)_{i \in I}$ af margliðum $f_i \neq 0$ yfir K. Útvíkkun L á K er þá sögð vera klofningskroppur fyrir fjölskylduna $(f_i)_{i \in I}$ yfir K ef sérhvert f_i, $i \in I$, klofnar yfir L en engin eiginleg hlutútvíkkun á K í L uppfyllir þetta skilyrði.

M sé einhver útvíkkun á K sem uppfyllir skilyrðið. M gæti til dæmis verið algebruleg lokun á K. Auðvelt er að sjá að sniðmengi allra hlutútvíkkana á

K í M sem uppfylla skilyrðið er útvíkkun á K sem uppfyllir skilyrðið. Þetta sniðmengi er því klofningskroppur fyrir $(f_i)_{i\in I}$ yfir K. Raunar er ljóst að þetta sniðmengi er $K(S)$ þar sem S er mengi allra staka í M sem eru rót á einhverri margliðanna f_i, $i \in I$. Það eru því til klofningskroppar fyrir $(f_i)_{i\in I}$ yfir K og sérhver slíkur er algebrulegur yfir K.

Setning 18+. $(f_i)_{i\in I}$ sé fjölskylda af margliðum $f_i \neq 0$ yfir K og L sé klofningskroppur fyrir $(f_i)_{i\in I}$ yfir K. Gefin sé útvíkkun M á K þannig að sérhvert f_i, $i \in I$, klofni yfir M. Þá er til K-mótun $\varphi : L \to M$.

Sönnun. Látum S vera mengi allra staka í L sem eru rót á einhverri margliðanna f_i, $i \in I$. Þá klofnar sérhvert f_i, $i \in I$, yfir $K(S)$, svo að $L = K(S)$. Sér í lagi er L algebruleg útvíkkun á K. Látum N vera algebrulega lokaða útvíkkun á M. Samkvæmt Setningu 14 er þá til K-mótun $\varphi : L \to N$. Látum T vera mengi allra staka í N sem eru rót á einhverri margliðanna f_i, $i \in I$. Þar sem sérhvert f_i, $i \in I$, klofnar yfir M, þá er $T \subseteq M$. Ef nú $s \in S$ er rót á f_i, þar sem $i \in I$, þá er $\varphi(s)$ rót á f_i, svo að $\varphi(s) \in T$, sér í lagi $\varphi(s) \in M$. En þá er $\varphi(L) = K(\varphi(S)) \subseteq M$.

Setning 19+. $(f_i)_{i\in I}$ sé fjölskylda af margliðum $f_i \neq 0$ yfir K. Þá eru sérhverjir tveir klofningskroppar fyrir $(f_i)_{i\in I}$ yfir K einsmóta yfir K.

Sönnun. Þetta fæst af Setningu 18+ á sama hátt og Setning 19 fékkst af Setningu 18.

Ef fjölskyldan $(f_i)_{i\in I}$ af margliðum $f_i \neq 0$ yfir K er endanleg og f er margfeldi stakanna í fjölskyldunni þá er klofningskroppur fyrir $(f_i)_{i\in I}$ yfir K það sama og klofningskroppur fyrir f yfir K. Klofningskroppur fjölskyldu allra margliða $\neq 0$ yfir K er hinsvegar það sama og algebruleg lokun á K. (Þetta er auðveld afleiðing af því að sérhvert stak í algebrulegri lokun á K er rót á einhverri margliðu $\neq 0$ yfir K.) Það má því líta á Setningu 15 sem sértilfelli af Setningu 19+.

1_+ Teikning með sirkli og reglustiku

Það er sígilt verkefni í flatarmyndafræði að teikna mynd út frá gefinni mynd með því að nota aðeins sirkil og reglustiku.

Gefna myndin samanstendur af einstökum punktum og heilum línum og hringjum. Það sem gera má er að draga beina línu í gegnum tvo gefna punkta og teikna hring, sem hefur miðju í gefnum punkti og radíus sem er fjarlægð á milli tveggja gefinna punkta, og finna skurðpunkta slíkra lína og hringa.

Í raun eru það aðeins punktarnir sem skipta máli, því að lína ákvarðast af tveim punktum og hringur ákvarðast af miðpunktinum og radíusnum. Það er alltaf gert ráð fyrir að gefnu punktarnir séu að minnsta kosti tveir.

Innleiðum nú hnitakerfi þannig að einhverjir tveir gefnu punktanna séu 0 og 1 á láásnum. Látum K vera útvíkkunina á $\mathbf{Q}$ í $\mathbf{R}$ sem er spönnuð af hnitum allra gefnu punktanna. Línur og hringir, sem leyfilegt er að teikna, hafa þá jöfnur með stuðlum í K. Skurðpunktur tveggja slíkra lína hefur þá líka hnit í K og til að finna hnit skurðpunkta línu og hrings eða tveggja hringa þarf í mesta lagi að draga ferningsrót af jákvæðu staki í K, svo að hnitin liggja í K eða í útvíkkun K_1 af K í $\mathbf{R}$ þannig að $[K_1 : K] = 2$.

Með því að halda svona áfram sjáum við að ef hægt er að teikna einhvern punkt út frá gefnu punktunum þá liggja hnit hans í útvíkkun L af K í $\mathbf{R}$, sem er þannig að til er runa af útvíkkunum $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = L$ þannig að $[K_i : K_{i-1}] = 2$, $i = 1, 2, \ldots, n$.

Þetta gildir raunar í hina áttina líka. Ef til er svona runa þannig að hnit punkts liggja í L þá er hægt að teikna punktinn út frá gefnu punktunum. Þetta byggist á því að út frá strikum af lengdum a og b má teikna strik af lengdum $a + b$, $|a - b|$, ab, a/b og $\sqrt{a}$.

K sé útvíkkun á $\mathbf{Q}$ í $\mathbf{R}$. Stak s í $\mathbf{R}$ er þá sagt vera teiknanlegt út frá K ef til er runa af útvíkkunum $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ með $[K_i : K_{i-1}] = 2$, $i = 1, 2, \ldots, n$, þannig að $s \in K_n$. Mengi allra slíkra staka s er þá kroppur — útvíkkun á K í $\mathbf{R}$. Þessi kroppur er kallaður kroppur teiknanlegra talna út frá K.

Athugum að ef s er teiknanlegt út frá K og K_n er eins og að ofan þá er $[K_n : K] = 2^n$ veldi af 2. Þar sem $[K(s) : K]$ gengur upp í $[K_n : K]$, þá fæst að $[K(s) : K]$ er líka veldi af 2. Þetta sýnir að ef s er teiknanlegt út frá K þá er s algebrulegt yfir K og $[K(s) : K]$ er veldi af 2. (Hin áttin gildir ekki.)

Teiknanlegar tölur út frá $\mathbf{Q}$ eru einfaldlega sagðar vera teiknanlegar og kroppur teiknanlegra talna út frá $\mathbf{Q}$ er kallaður kroppur teiknanlegra talna. Hann er stundum táknaður með $\mathbf{K}$.

Hér á eftir notum við þessar niðurstöður til að sýna að nokkur af þeim teikniverkefnum, sem forngrikkir glímdu við, séu óleysanleg.

Tvöföldun tenings

Gefið sé strik. Við hugsum okkur tening sem hefur lengd striksins fyrir hliðarlengd. Teikna skal út frá gefna strikinu annað strik þannig að tilsvarandi teningur hafi tvöfalt rúmmál upphaflega teningsins.

Hlutfall strikalengdanna er $\sqrt[3]{2}$. Ef verkefnið væri leysanlegt þá væri því talan $\sqrt[3]{2}$ teiknanleg. En það er hún ekki, því að $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$.

Þrískipting horns

Gefið sé horn. Teikna skal út frá gefna horninu annað horn sem er þriðjungur gefna hornsins að stærð.

Ef einingarstrik er gefið þá er það að teikna horn af stærð θ jafngilt því að teikna strik af lengd $\cos\theta$. Að verkefnið sé leysanlegt fyrir horn af stærð θ þýðir því að talan $\cos\frac{\theta}{3}$ sé teiknanleg út frá $\mathbf{Q}(\cos\theta)$. Nú gildir almennt að $4\cos^3\frac{\theta}{3} - 3\cos\frac{\theta}{3} = \cos\theta$, svo að þetta þýðir að rót á margliðunni $4X^3 - 3X - \cos\theta$ sé teiknanleg út frá $\mathbf{Q}(\cos\theta)$. Ef þessi margliða er óþáttanleg yfir $\mathbf{Q}(\cos\theta)$ þá er verkefnið ekki leysanlegt, því að þá hefur rót á margliðunni gráðu 3 yfir $\mathbf{Q}(\cos\theta)$. Verkefnið er því aðeins leysanlegt að þessi margliða hafi rót í $\mathbf{Q}(\cos\theta)$. Það er almennt ekki rétt. Til dæmis er það ekki rétt ef $\theta = 60°$, því að auðvelt er að sjá að margliðan $4X^3 - 3X - \frac{1}{2}$ hefur enga rót í $\mathbf{Q}$.

Ferningun hrings

Gefinn sé hringur. Teikna skal út frá hringnum strik þannig að ferningur, sem hefur lengd striksins sem hliðarlengd, hafi sama flatarmál og gefni hringurinn.

Hlutfall lengdar striksins og radíuss hringsins er $\sqrt{\pi}$. Að verkefnið sé leysanlegt þýðir því að talan $\sqrt{\pi}$ sé teiknanleg, sem er jafngilt því að talan π sé teiknanleg. En sýna má að talan π sé ekki einu sinni algebruleg yfir $\mathbf{Q}$, svo að verkefnið er óleysanlegt.

2 Normlegar útvíkkanir og aðskiljanlegar útvíkkanir

Í þessum kafla táknar K alltaf kropp.

Algebruleg útvíkkun L á K er sögð vera normleg útvíkkun á K ef fyrir sérhvert stak s í L gildir að lágmargliða s yfir K klofnar yfir L.

Þetta skilyrði þýðir að sérhver frummargliða yfir K, sem hefur rót í L, klofnar yfir L. Ef við einskorðum okkur við stök í einhverri ákveðinni algebrulega lokaðri útvíkkun á K sem inniheldur L þá má orða skilyrðið þannig að ef frummargliða yfir K hefur rót í L þá eru allar rætur hennar í L.

Við minnum á að ef L er algebruleg útvíkkun á K þá er til algebrulega lokuð útvíkkun M á K sem inniheldur L. Við gætum t.d. valið M sem algebrulega lokun á L. Algebrulega lokaða útvíkkunin M á K gæti líka verið gefin. Við vitum að þá er til K-mótun $\varphi : L \to M$. Þá gætum við athugað $\varphi(L)$ í stað L.

Setning 1. L sé algebruleg útvíkkun á K og M sé algebrulega lokuð útvíkkun á K sem inniheldur L. Þá er L normleg útvíkkun á K þá og því aðeins að fyrir sérhverja K-mótun $\varphi : L \to M$ gildi að $\varphi(L) = L$.

Sönnun. L sé normleg útvíkkun á K og $\varphi : L \to M$ sé K-mótun. Gefið sé $r \in L$. Látum p vera lágmargliðu r yfir K. Þar sem r er rót á p, þá er $\varphi(r)$ líka rót á p. En L inniheldur allar rætur p í M, svo að af þessu leiðir að $\varphi(r) \in L$. Þetta sýnir að $\varphi(L) \subseteq L$. Af Setningu 12 í Kafla 1 leiðir nú að $\varphi(L) = L$.

Nú sé gefið að fyrir sérhverja K-mótun $\varphi : L \to M$ gildi $\varphi(L) = L$. Gefið sé $r \in L$ með lágmargliðu p yfir K. Gefin sé rót s á p í M. Samkvæmt Setningu 13 í Kafla 1 er til K-mótun $\varphi_0 : K(r) \to M$ með $\varphi_0(r) = s$. Samkvæmt umræðunni á eftir Setningu 14 í Kafla 1 má framlengja φ_0 í K-mótun $\varphi : L \to M$. Samkvæmt forsendu er þá $\varphi(L) = L$, sér í lagi $s = \varphi(r) \in L$. Þetta sýnir að L inniheldur allar rætur á p í M.

Setning 2. Útvíkkun L á K er normleg þá og því aðeins að til sé fjölskylda $(f_i)_{i \in I}$ af margliðum $f_i \neq 0$ yfir K þannig að L sé klofningskroppur fyrir $(f_i)_{i \in I}$ yfir K.

Sönnun. L sé normleg útvíkkun á K. Fyrir sérhvert $s \in L$ látum við p_s vera lágmargliðu s yfir K. Þá er L greinilega klofningskroppur fyrir fjölskylduna $(p_s)_{s \in L}$ yfir K.

L sé klofningskroppur fyrir fjölskylduna $(f_i)_{i \in I}$ yfir K. Látum $\overline{K}$ vera algebrulega lokun á K sem inniheldur L. Þá er $L = K(S)$ þar sem S er mengi allra staka í $\overline{K}$ sem eru rót á einhverri margliðanna f_i, $i \in I$. Gefin sé

K-mótun $\varphi : L \to \overline{K}$. Þar sem φ varpar rót á f_i í rót á f_i, þá er $\varphi(S) \subseteq S$. Af því leiðir að $\varphi(L) \subseteq L$. Af Setningu 12 í Kafla 1 leiðir þá að $\varphi(L) = L$. Samkvæmt Setningu 1 sýnir þetta að L er normleg útvíkkun á K.

Setning 3. L sé endanleg normleg útvíkkun á K. Þá er til margliða $f \neq 0$ yfir K þannig að L sé klofningskroppur fyrir f yfir K.

Sönnun. Skrifum $L = K(s_1, \ldots, s_n)$. Látum p_i vera lágmargliðu s_i yfir K, $i = 1, \ldots, n$. Þá er L klofningskroppur fyrir margfeldið $f = p_1 \cdots p_n$ yfir K.

Hin áttin gildir að sjálfsögðu líka. Nánar tiltekið gildir að ef L er klofningskroppur fyrir margliðu f af gráðu n yfir K þá er $[L : K] \leq n!$. Það sést með því að mynda L í skrefum út frá K, bæta við einni rót á f í einu.

L sé algebruleg útvíkkun á K. Normleg útvíkkun N á K sem inniheldur L er sögð vera normleg lokun á L yfir K ef engin eiginleg hlutútvíkkun á K í N, sem inniheldur L, er normleg.

Látum S vera eitthvert hlutmengi í L þannig að $L = K(S)$. (Til dæmis gæti $S = L$.) Fyrir sérhvert $s \in S$ látum við p_s vera lágmargliðu s yfir K.

M sé einhver normleg útvíkkun á K sem inniheldur L. Þá hefur sérhvert p_s, $s \in S$, rót í M, nefnilega rótina s. Þar sem M er normleg yfir K, þá leiðir af þessu að sérhvert p_s, $s \in S$, klofnar yfir M.

Nú sé M einhver útvíkkun á K sem inniheldur L þannig að sérhvert p_s, $s \in S$, klofnar yfir M. Þá inniheldur M klofningskropp N fyrir $(p_s)_{s \in S}$ yfir K. Þar sem N inniheldur allar rætur sérhvers p_s, $s \in S$, þá er sér í lagi $S \subseteq N$, þar með $L \subseteq N$. Auk þess er N normleg útvíkkun á K samkvæmt Setningu 2.

Af þessu öllu sést að útvíkkun N á K sem inniheldur L er normleg lokun á L yfir K þá og því aðeins að N sé klofningskroppur fyrir $(p_s)_{s \in S}$ yfir K. En þar sem $L \subseteq N$ og $L = K(S)$, þá er það jafngilt því að N sé klofningskroppur fyrir $(p_s)_{s \in S}$ yfir L.

Sér í lagi fæst að til eru normlegar lokanir á L yfir K. Auk þess getum við notað setningar um klofningskroppa til að sanna setningar um normlegar lokanir. Þannig fæst eftirfarandi setning.

Setning 4. L sé algebruleg útvíkkun á K. Þá eru sérhverjar tvær normlegar lokanir á L yfir K einsmóta yfir L.

Setning 5. L sé endanleg útvíkkun á K. Þá er normleg lokun á L yfir K líka endanleg.

Sönnun. Við notum umræðuna á undan Setningu 4. Þar sem L er endanleg yfir K, þá getum við valið S endanlegt. Við getum því látið N vera klofningskropp fyrir eina margliðu yfir K.

Við munum síðar sjá að ef L er endanleg útvíkkun á K og N er normleg lokun á L yfir K þá er $[N : K] \leq [L : K]!$.

Við ljúkum umfjölluninni um normlegar útvíkkanir hér með setningu um tilvist K-mótana.

Setning 6. L sé algebruleg útvíkkun á K og N sé normleg útvíkkun á K sem inniheldur L. Gefin sé K-mótun $\varphi : L \to N$. Þá má framlengja φ í K-einsmótun $\chi : N \to N$.

Sönnun. Látum $\overline{K}$ vera algebrulega lokun á K sem inniheldur N. Samkvæmt umræðunni á eftir Setningu 14 í Kafla 1 má framlengja φ í K-mótun $\chi : N \to \overline{K}$. En þar sem N er normleg yfir K, þá hlýtur $\chi(N) = N$ samkvæmt Setningu 1.

L sé algebruleg útvíkkun á K og M sé algebrulega lokuð útvíkkun á K. Samkvæmt Setningu 14 í Kafla 1 er þá til K-mótun $L \to M$. Þessi K-mótun þarf ekki að vera ótvírætt ákvörðuð. Við vildum því gjarna vita hve margar slíkar K-mótanir eru til. Af ýmsum dæmum mætti ætla að fjöldi þeirra væri jafn $[L : K]$. Það er ekki alltaf rétt.

Athugum fyrst tilfellið að $L = K(s)$ sé einföld algebruleg útvíkkun á K. Látum p vera lágmargliðu s yfir K. Þá er $[L : K]$ jafnt gráðu p. Samkvæmt Setningu 13 í Kafla 1 er fyrir sérhverja rót t á p í M til ein og aðeins ein K-mótun $\varphi : L \to M$ með $\varphi(s) = t$. Fjöldi K-mótana $\varphi : L \to M$ er því jafn fjölda mismunandi róta á p í M. Þessi fjöldi er því ekki meiri en gráða p, þ.e.a.s. ekki meiri en $[L : K]$.

$f \neq 0$ sé margliða yfir K. Veljum algebrulega lokaða útvíkkun M á K. Þá klofnar f yfir M, segjum $f = c_0(X - c_1) \cdots (X - c_n)$ með $c_0, c_1, \ldots, c_n \in M$. Fjöldi mismunandi róta á f í M er þá jafn fjölda staka í menginu $\{c_1, \ldots, c_n\}$. Þessi fjöldi er óháður valinu á M því að það nægir að athuga algebrulegu lokunina á K sem innihaldin er í M. En allar algebrulegar lokanir á K eru einsmóta yfir K. Við segjum því einfaldlega að þetta sé fjöldi mismunandi róta á f.

Fjöldi mismunandi róta á f er að sjálfsögðu aldrei meiri en gráða f. Sagt er að f sé aðskiljanleg ef fjöldinn er jafn gráðu f. Ef M er eins og hér að ofan þá þýðir þetta að stöðluðu línulegu þættirnir $X - c_i$, $i = 1, \ldots, n$, í f eru allir mismunandi. Við orðum þetta líka þannig að rætur f séu allar mismunandi.

Afleiða margliðu $f = \sum_{i=0}^{n} a_i X^i$ yfir K er skilgreind sem margliðan $f' = \sum_{i=1}^{n} i a_i X^{i-1}$ yfir K.

Afleiðuvörpunin $K[X] \to K[X]$, $f \mapsto f'$, er greinilega K-línuleg. Ennfremur gildir $(fg)' = f'g + fg'$ fyrir allar margliður f og g yfir K. (Með því að nota að afleiðuvörpunin er K-línuleg nægir að sanna þetta fyrir tilfellin $f = X^i$ og $g = X^j$ þar sem $i, j \geq 0$. En í þessum tilfellum er reglan augljós.)

Setning 7. Margliða $f \neq 0$ yfir K er aðskiljanleg þá og því aðeins að f og f' hafi engan sameiginlegan þátt.

Sönnun. M sé útvíkkun á K þannig að f klofnar í línulega þætti yfir M, segjum

$$f = c_0(X - c_1) \cdots (X - c_n)$$

með $c_0, c_1, \ldots, c_n \in M$. Með því að nota regluna fyrir afleiðu margfeldis fæst þá að

$$f' = \sum_{i=1}^{n} c_0(X - c_1) \cdots (X - c_{i-1})(X - c_{i+1}) \cdots (X - c_n)$$

Þátturinn $X - c_j$ í f gengur upp í alla liði þessarar summu nema kannski j-ta liðinn. Hann gengur upp í j-ta liðinn þá og því aðeins að til sé $i \neq j$ þannig að $c_i = c_j$. Af þessu sést að f og f' hafa engan sameiginlegan þátt yfir M þá og því aðeins að f sé aðskiljanleg. Við notum nú að stærsti samdeilir margliða f og g yfir K er sá sami hvort sem reiknað er yfir K eða M.

Ef f er frummargliða yfir K þá geta f og f' engan sameiginlegan þátt haft nema f gangi upp í þeim báðum. Þar sem gráða f' er minni en gráða f, þá gengur f ekki upp í f' nema $f' = 0$. En hvenær er $f' = 0$ fyrir margliðu f yfir K?

Skrifum $f = \sum_{i=0}^{n} a_i X^i$. Þá er $f' = \sum_{i=1}^{n} i a_i X^{i-1}$, svo að $f' = 0$ þá og því aðeins að $i a_i = 0$ fyrir $i = 1, \ldots, n$. Ef kennitala K er 0 þá þýðir þetta að $a_i = 0$ fyrir $i = 1, \ldots, n$, svo að f er fasti. Ef kennitala K er $p > 0$ þá þýðir þetta aðeins að $a_i = 0$ ef p gengur ekki upp í i, svo að $f = \sum_{j=0}^{[n/p]} a_{pj} X^{pj}$, þ.e.a.s. $f \in K[X^p]$.

Við fáum því tvö tilfelli.

Ef kennitala K er 0 þá er sérhver frummargliða yfir K aðskiljanleg.

Ef kennitala K er $p > 0$ þá er frummargliða f yfir K aðskiljanleg þá og því aðeins að $f \notin K[X^p]$.

K er sagður vera fullkominn ef sérhver frummargliða yfir K er aðskiljanleg.

Ef kennitala K er 0 þá er K fullkominn samkvæmt ofansögðu.

Setning 8. K hafi kennitölu $p > 0$. K er fullkominn þá og því aðeins að sérhvert stak í K sé p-ta veldi staks í K.

Sönnun. Sérhvert stak í K sé p-ta veldi staks í K. Gefin sé margliða $f = \sum_{i=0}^{n} a_i X^{pi}$ í $K[X^p]$. Skrifum $a_i = {b_i}^p$ með $b_i \in K$ fyrir $i = 1, \ldots, n$. Þá fæst $f = \sum_{i=0}^{n} {b_i}^p X^{pi} = (\sum_{i=0}^{n} b_i X^i)^p$, svo að f er ekki frummargliða yfir K. Þetta sýnir að K er fullkominn.

Þá sé til stak a í K sem er ekki p-ta veldi staks í K. Þá hefur margliðan $X^p - a$ ekki rót í K. Samkvæmt heimaverkefni er $X^p - a$ þá frummargliða yfir K. Hún er greinilega ekki aðskiljanleg, svo að K er ekki fullkominn.

Athugasemd. Mengi allra staka í K sem eru p-ta veldi staks í K er auðvitað myndmengi vörpunarinnar $K \to K$, $x \mapsto x^p$. Þar sem kennitala K er p, þá er þessi vörpun kroppamótun. Þetta mengi er því hlutkroppur í K. Þessi hlutkroppur er táknaður K^p. Setningin segir að K sé fullkominn þá og því aðeins að $K^p = K$.

Setning 9. Ef K er endanlegur þá er K fullkominn.

Sönnun. Látum p vera kennitölu K. Kroppamótunin $K \to K$, $x \mapsto x^p$, er eintæk. Þar sem K er endanlegur, þá er hún þar með átæk.

Algebrulegt stak yfir K er sagt vera aðskiljanlegt yfir K ef lágmargliða þess yfir K er aðskiljanleg. Algebruleg útvíkkun L á K er sögð vera aðskiljanleg ef sérhvert stak í L er aðskiljanlegt yfir K.

$L = K(s)$ sé einföld algebruleg útvíkkun á K og p sé lágmargliða s yfir K. M sé algebrulega lokuð útvíkkun á K. Við höfum þegar séð að fjöldi K-mótana $\varphi : L \to M$ er jafn fjölda mismunandi róta á p í M og að þessi fjöldi er aldrei meiri en $[L : K]$. Ennfremur að hann er jafn $[L : K]$ þá og því aðeins að rætur p séu allar mismunandi, þ.e.a.s. þá og því aðeins að p sé aðskiljanleg, m.ö.o. þá og því aðeins að s sé aðskiljanlegt yfir K.

Eftirfarandi setning er útvíkkun á þessu. Við getum litið á hana sem lemma, því að hún er tæknileg og mikilvægustu niðurstöður hennar koma fram í öðrum setningum.

Setning 10. $L = K(s_1, \ldots, s_k)$ sé endanlega spönnuð algebruleg útvíkkun á K. Látum $L_0 = K$ og $L_i = K(s_1, \ldots, s_i)$ fyrir $i = 1, \ldots, k$. Látum p_i vera lágmargliðu s_i yfir L_{i-1} og látum m_i vera fjölda mismunandi róta á p_i, $i = 1, \ldots, k$. Gefin sé algebrulega lokuð útvíkkun M á K. Fjöldi K-mótana $L \to M$ er þá jafn $m_1 \cdots m_k$.

Sér í lagi er fjöldi K-mótana $L \to M$ aldrei meiri en $[L : K]$. Hann er jafn $[L : K]$ þá og því aðeins að sérhvert s_i sé aðskiljanlegt yfir L_{i-1}, $i = 1, \ldots, k$.

Sönnun. Við sönnum fyrri hlutann með þrepun yfir k. Við höfum þegar séð að þetta er rétt ef $k = 1$. Fyrir þrepunarskrefið þurfum við aðeins eftirfarandi almennari útgáfu af tilfellinu $k = 1$.

K' sé algebruleg útvíkkun á K og $\chi : K' \to M$ sé K-mótun. Auk þess sé $L' = K'(s)$ einföld algebruleg útvíkkun á K' og p lágmargliða s yfir K'. Þá er fjöldi framlenginga á χ í K-mótun $\psi : L' \to M$ jafn fjölda mismunandi róta á p.

En þetta er einföld afleiðing af umræðunni á eftir Setningu 13 í Kafla 1 og því að fjöldi mismunandi róta á $\chi(p)$ er jafn fjölda mismunandi róta á p.

Látum $n_i = [L_i : L_{i-1}]$, $i = 1, \ldots, k$. Samkvæmt umræðunni á undan setningunni þá er $m_i \leq n_i$ og $m_i = n_i$ þá og því aðeins að s_i sé aðskiljanlegt yfir L_{i-1}. Seinni hlutinn er afleiðing af þessu, því að $n_1 \cdots n_k = [L : K]$.

Athugasemd. Ef s_i er aðskiljanlegt yfir K þá er s_i líka aðskiljanlegt yfir L_{i-1}, því að lágmargliða s_i yfir L_{i-1} gengur upp í lágmargliðu s_i yfir K.

Setning 11. Ef $L = K(S)$ er útvíkkun á K þannig að sérhvert stak í S er aðskiljanlegt yfir K þá er L aðskiljanleg útvíkkun á K.

Sönnun. Gefið sé $t \in L$. Þá er til endanlegt hlutmengi $\{s_1, \ldots, s_k\}$ í S þannig að $t \in K(s_1, \ldots, s_k)$. Við megum því gera ráð fyrir að $L = K(s_1, \ldots, s_k)$. Þar sem sérhvert s_i er aðskiljanlegt yfir K, þá er fjöldi K-mótana $L \to M$ jafn $[L : K]$ samkvæmt Setningu 10 og athugasemd við hana. En við getum líka skrifað $L = K(t, s_1, \ldots, s_k)$. Þar sem fjöldi K-mótana $L \to M$ er jafn $[L : K]$ þá er t aðskiljanlegt yfir K samkvæmt Setningu 10.

Við getum nú umorðað seinni hluta Setningar 10.

Setning 12. L sé endanleg útvíkkun á K. Gefin sé algebrulega lokuð útvíkkun M á K. Þá er fjöldi K-mótana $L \to M$ aldrei meiri en $[L : K]$. Hann er jafn $[L : K]$ þá og því aðeins að L sé aðskiljanleg útvíkkun á K.

Sönnun. Skrifum $L = K(s_1, \ldots, s_k)$. Fyrri fullyrðingin er þá beint úr Setningu 10. Það að fjöldi K-mótana $L \to M$ sé jafn $[L : K]$ ef L er aðskiljanleg útvíkkun á K fæst af Setningu 10 og athugasemd við hana. Gerum þá ráð fyrir að fjöldi K-mótana $L \to M$ sé jafn $[L : K]$. Af Setningu 10 leiðir þá að s_1 er aðskiljanlegt yfir K. En það að fjöldi K-mótana $L \to M$ sé jafn $[L : K]$ er greinilega óháð röðinni á $s_1, \ldots, s_k$, svo að það fæst á sama hátt að sérhvert s_i er aðskiljanlegt yfir K. Samkvæmt Setningu 11 er L því aðskiljanleg útvíkkun á K.

Setning 13. Ef L er aðskiljanleg útvíkkun á K og M er aðskiljanleg útvíkkun á L þá er M aðskiljanleg útvíkkun á K.

Sönnun. Gefið sé stak $t \in M$. Látum $f = \sum_{i=0}^{n} c_i X^i$ vera lágmargliðu t yfir L. Þá hefur f engar margfaldar rætur. Látum $L_0 = K(c_0, \ldots, c_n)$. Þá er f líka lágmargliða t yfir L_0, svo að t er aðskiljanlegt yfir L_0. Látum

nú N vera einhverja algebrulega lokaða útvíkkun á K. Af Setningu 10 og athugasemd við hana fæst þá að fjöldi K-mótana $K(c_0, \ldots, c_n, t) \to N$ er jafn $[K(c_0, \ldots, c_n, t) : K]$. Samkvæmt Setningu 12 er $K(c_0, \ldots, c_n, t)$ því aðskiljanleg útvíkkun á K. Sér í lagi er t aðskiljanlegt yfir K.

Raunar er líka ljóst að ef $K \subseteq L \subseteq M$ eru útvíkkanir þannig að M er aðskiljanleg yfir K þá er M aðskiljanleg yfir L og L aðskiljanleg yfir K.

Setning 14. L sé útvíkkun á K. Látum L_0 vera mengi allra staka í L sem eru aðskiljanleg yfir K. Þá er L_0 aðskiljanleg útvíkkun á K.

Sönnun. Látum $L_1 = K(L_0)$. Samkvæmt Setningu 11 er L_1 þá aðskiljanleg útvíkkun á K. En þá er $L_1 \subseteq L_0$, þarmeð $L_1 = L_0$.

L sé útvíkkun á K. Útvíkkunin L_0 í Setningu 14 er þá kölluð aðskiljanleg lokun K í L. Af Setningu 13 leiðir að ekki er til eiginleg aðskiljanleg hlutútvíkkun á L_0 í L. Af Setningu 11 leiðir þá að sérhvert stak í L sem er aðskiljanlegt yfir L_0 er þegar í L_0. Við tjáum þetta með því að segja að L_0 sé aðskiljanlega lokað í L.

Við segjum að kroppur sé aðskiljanlega lokaður ef hann hefur enga eiginlega aðskiljanlega útvíkkun. Þetta þýðir að kroppur er aðskiljanlega lokaður þá og því aðeins að hann sé aðskiljanlega lokaður í hvaða útvíkkun sem er.

Algebrulega lokaður kroppur er greinilega aðskiljanlega lokaður.

Útvíkkun L á K er sögð vera aðskiljanleg lokun á K ef L er aðskiljanleg útvíkkun á K og L er aðskiljanlega lokaður. Skilyrðið má orða þannig að L sé aðskiljanleg útvíkkun á K þannig að ekki sé til „stærri“ aðskiljanleg útvíkkun á K, þ.e.a.s. aðskiljanleg útvíkkun á K sem inniheldur L sem eiginlegan hlutkropp.

Setning 15. Sérhver kroppur K hefur aðskiljanlega lokun og sérhverjar tvær aðskiljanlegar lokanir á K eru einsmóta yfir K.

Sönnun. Aðskiljanleg lokun á K er greinilega klofningskroppur fyrir fjölskyldu allra aðskiljanlegra frummargliða yfir K.

Af sönnun Setningar 15 sést að aðskiljanleg lokun á K er normleg útvíkkun á K. Við getum litið á næstu setningu sem útvíkkun á þessari staðreynd.

Setning 16. L sé aðskiljanleg útvíkkun á K. Þá er normleg lokun á L yfir K líka aðskiljanleg útvíkkun á K.

Sönnun. Normleg lokun á L yfir K er spönnuð af öllum rótum lágmargliða allra staka í L. Þessar lágmargliður eru allar aðskiljanlegar og ræturnar því líka.

$L = K(r, s)$ sé algebruleg útvíkkun á K sem spönnuð er af tveim stökum r og s. Látum p vera lágmargliðu r yfir K og q vera lágmargliðu s yfir K. Veljum okkur algebrulega lokun $\overline{K}$ á K sem inniheldur L. Þá klofna p og q yfir $\overline{K}$, segjum $p = (X - r_1) \cdots (X - r_m)$ með $r_1 = r$ og $q = (X - s_1) \cdots (X - s_n)$ með $s_1 = s$.

Við gerum ráð fyrir að s sé aðskiljanlegt yfir K. Þá eru ræturnar $s_1, \ldots, s_n$ á q allar mismunandi. Fyrir sérhvert $i = 1, \ldots, m$ og sérhvert $j = 2, \ldots, n$ er þá til ein og aðeins ein lausn á jöfnunni $r_i + xs_j = r_1 + xs_1$. Við skulum gera ráð fyrir að K sé ekki endanlegur. Þá fæst af þessu að til er stak c í K þannig að $r_i + cs_j \neq r_1 + cs_1$ fyrir öll $i = 1, \ldots, m$ og öll $j = 2, \ldots, n$. Við látum $t = r_1 + cs_1 = r + cs$. Við látum líka $f(X) = p(t - cX)$. Þá er f margliða yfir $K(t)$ þannig að $f(s) = p(t - cs) = p(r) = 0$, svo að q og f hafa báðar rótina s. Sér í lagi gengur $X - s$ upp í f. Ef til væri $j > 1$ þannig að $X - s_j$ gengi upp í f þá væri $p(t - cs_j) = f(s_j) = 0$, svo að $t - cs_j = r_i$ fyrir eitthvert $i = 1, \ldots, m$. Það þýddi að $r_i + cs_j = t = r_1 + cs_1$ í mótsögn við val okkar á c. Þetta sýnir að $X - s$ er stærsti samdeilir q og f.

Þessir reikningar eru gerðir yfir $\overline{K}$. En stærsti samdeilir q og f er sá sami hvort sem reiknað er yfir $K(t)$ eða $\overline{K}$, svo að $X - s$ er einnig stærsti samdeilir q og f í $K(t)[X]$. Sér í lagi er $X - s$ í $K(t)[X]$, þ.e.a.s. $s \in K(t)$. En þá er líka $r = t - cs \in K(t)$. Þar sem $t \in K(r, s)$, þá leiðir af þessu að $K(r, s) = K(t)$.

Næsta setning er útvíkkun á þessu.

Setning 17. $L = K(s_1, \ldots, s_n)$ sé endanlega spönnuð algebruleg útvíkkun á K þannig að s_i sé aðskiljanlegt yfir K fyrir $i = 2, \ldots, n$. Þá er til $t \in L$ þannig að $L = K(t)$.

Sönnun. Ef K er endanlegur þá er þetta heimaverkefni. Við getum því gert ráð fyrir að K sé ekki endanlegur. Við sönnum þá setninguna með þrepun yfir n. Tilfellið $n = 1$ er augljóst og í tilfellinu $n = 2$ var þetta sannað hér að ofan. Ef $n > 2$ þá getum við samkvæmt þrepunarforsendu skrifað $K(s_1, \ldots, s_{n-1}) = K(r)$. En þá er $L = K(r, s_n)$. Samkvæmt því sem gert var hér að ofan er þá til $t \in L$ þannig að $L = K(t)$.

Næsta setning er sértilfelli af Setningu 17. Hún er kölluð setningin um frumstætt stak.

Setning 18. Sérhver endanleg aðskiljanleg útvíkkun á K er einföld.

Ef kennitala K er 0 þá er skilyrðið um aðskiljanleika óþarft.

L sé endanleg aðskiljanleg útvíkkun á K og N sé normleg lokun á L yfir K. Samkvæmt Setningunni um frumstætt stak má skrifa $L = K(s)$ með $s \in L$. Látum f vera lágmargliðu s yfir K. Þá er gráðan $[L : K]$ jöfn gráðu

f. Ennfremur er N klofningskroppur fyrir f yfir K. Samkvæmt ábendingu á eftir Setningu 3 er því $[N : K] \leq [L : K]!$.

3 Galois útvíkkanir

Í þessum kafla táknar K alltaf kropp.

Algebruleg útvíkkun L á K er sögð vera Galois útvíkkun á K ef hún er bæði normleg og aðskiljanleg yfir K.

Setning 1. Útvíkkun L á K er Galois þá og því aðeins að til sé fjölskylda $(f_i)_{i\in I}$ af aðskiljanlegum margliðum f_i yfir K þannig að L sé klofningskroppur fyrir $(f_i)_{i\in I}$ yfir K.

Sönnun. L sé Galois útvíkkun á K. Fyrir sérhvert $s \in L$ látum við p_s vera lágmargliðu s yfir K. Þá er sérhver margliðanna p_s, $s \in L$, aðskiljanleg yfir K og L er klofningskroppur fyrir fjölskylduna $(p_s)_{s\in L}$ yfir K.

L sé klofningskroppur fyrir fjölskylduna $(f_i)_{i\in I}$ yfir K þar sem sérhver margliðanna f_i, $i \in I$, er aðskiljanleg. Samkvæmt Setningu 2 í Kafla 2 er L þá normleg útvíkkun á K. Við vitum líka að $L = K(S)$ þar sem S er mengi allra staka í L sem eru rót á einhverri margliðanna f_i, $i \in I$. Ef $s \in S$ er rót á f_i og p er lágmargliða s yfir K þá gengur p upp í f_i. Þar sem f_i er aðskiljanleg, þá er p það því líka. Samkvæmt Setningu 11 í Kafla 2 sýnir þetta að L er aðskiljanleg útvíkkun á K.

Setning 2. L sé endanleg Galois útvíkkun á K. Þá er til aðskiljanleg frummargliða f yfir K þannig að L sé klofningskroppur fyrir f yfir K.

Sönnun. Samkvæmt Setningu 18 í Kafla 2 er til stak s í L þannig að $L = K(s)$. Látum f vera lágmargliðu s yfir K. Þá er L klofningskroppur fyrir f yfir K.

L sé kroppur. Grúpa allra einsmótana kroppa $L \to L$ er þá táknuð $\mathrm{Aut}(L)$. Ef G er hlutgrúpa í $\mathrm{Aut}(L)$ þá er mengið

$$\{x \in L \mid \sigma(x) = x \text{ fyrir sérhvert } \sigma \in G\}$$

greinilega hlutkroppur í L. Þessi hlutkroppur í L er kallaður fastakroppur hlutgrúpunnar G í $\mathrm{Aut}(L)$.

Nú sé L útvíkkun á K. Grúpa allra K-einsmótana $L \to L$ er þá táknuð $\mathrm{Aut}_K(L)$. Þetta er hlutgrúpa í $\mathrm{Aut}(L)$ — hlutgrúpa allra þeirra $\sigma \in \mathrm{Aut}(L)$ þannig að $\sigma(a) = a$ fyrir sérhvert $a \in K$. Ef G er hlutgrúpa í $\mathrm{Aut}_K(L)$ þá inniheldur fastakroppur G augljóslega K, svo að hann er útvíkkun á K.

Ef L er algebruleg útvíkkun á K þá er sérhver K-mótun $L \to L$ einsmótun samkvæmt Setningu 12 í Kafla 1.

Setning 3. L sé algebruleg útvíkkun á K. L er Galois útvíkkun á K þá og því aðeins að fastakroppur $\mathrm{Aut}_K(L)$ sé jafn K.

Sönnun. L sé Galois útvíkkun á K. Látum $\overline{K}$ vera algebrulega lokun á K sem inniheldur L. Gefið sé $x \in L$, $x \notin K$. Þá hefur lágmargliða x yfir K gráðu sem er stærri en 1. Þar sem x er aðskiljanlegt yfir K, þá er til rót y í $\overline{K}$ á þessari lágmargliðu þannig að $y \neq x$. Samkvæmt Setningu 13 í Kafla 1 er til K-mótun $\varphi_0 : K(x) \to \overline{K}$ með $\varphi_0(x) = y$ og samkvæmt umræðunni á eftir Setningu 14 í Kafla 1 má framlengja φ_0 í K-mótun $\varphi : L \to \overline{K}$. Þar sem L er normleg útvíkkun á K, þá er $\varphi(L) = L$ samkvæmt Setningu 1 í Kafla 2, svo að φ gefur af sér K-einsmótun $\sigma : L \to L$. Þar sem $\sigma(x) = y \neq x$, þá sýnir þetta að x er ekki í fastakroppi $\mathrm{Aut}_K(L)$.

Nú sé fastakroppur $\mathrm{Aut}_K(L)$ jafn K. Gefið sé $x \in L$. Látum p_x vera lágmargliðu x yfir K. Ef $\sigma \in \mathrm{Aut}_K(L)$ þá er p_x líka lágmargliða $\sigma(x)$ yfir K. Þar sem p_x hefur ekki nema endanlega margar rætur í L, þá leiðir af þessu að ekki eru til nema endanlega mörg mismunandi stök $x_1, \ldots, x_n$ í L af taginu $\sigma(x)$ þar sem $\sigma \in \mathrm{Aut}_K(L)$. Látum $f_x = (X - x_1) \cdots (X - x_n)$. Ljóst er að margliðan f_x er aðskiljanleg. Ef $\sigma \in \mathrm{Aut}_K(L)$ þá varpar σ menginu $\{x_1, \ldots, x_n\}$ yfir í sjálft sig. Þar sem σ er eintæk, þá þýðir þetta að σ gefur af sér umröðun á þessu mengi. Af því leiðir að $\sigma(f_x) = f_x$. Þar sem þetta gildir fyrir sérhvert $\sigma \in \mathrm{Aut}_K(L)$, þá leiðir af forsendunni að $f_x \in K[X]$. Nú er L greinilega klofningskroppur fyrir fjölskylduna $(f_x)_{x \in L}$ yfir K. Af Setningu 1 leiðir því að L er Galois útvíkkun á K.

Athugasemd. Margliðan f_x í seinni hluta sönnunarinnar er reyndar lágmargliða x yfir K. Sérhvert x_i, $i = 1, \ldots, n$, er nefnilega rót á lágmargliðunni p_x. Það sýnir að f_x gengur upp í p_x. En x er líka rót á f_x, svo að p_x gengur upp í f_x.

Ef L er Galois útvíkkun á K þá er grúpan $\mathrm{Aut}_K(L)$ líka kölluð Galois grúpa útvíkkunarinnar L á K. Hún er þá táknuð $\mathrm{Gal}(L/K)$.

Setning 4. N sé Galois útvíkkun á K og L sé hlutútvíkkun á K í N. Þá er N líka Galois útvíkkun á L og

$$\mathrm{Gal}(N/L) = \{\sigma \in \mathrm{Gal}(N/K) \mid \sigma(x) = x \text{ fyrir sérhvert } x \in L\}$$

Sér í lagi er $\mathrm{Gal}(N/L)$ hlutgrúpa í $\mathrm{Gal}(N/K)$.

Sönnun. Þar sem N er normleg og aðskiljanleg útvíkkun á K, þá er N líka normleg og aðskiljanleg útvíkkun á L. Ef $\sigma \in \mathrm{Aut}(N)$ þá er $\sigma \in \mathrm{Aut}_L(N)$ þá og því aðeins að $\sigma(x) = x$ fyrir sérhvert $x \in L$.

Athugasemd. Samkvæmt Setningu 3 gildir þá

$$L = \{x \in N \mid \sigma(x) = x \text{ fyrir sérhvert } \sigma \in \mathrm{Gal}(N/L)\}$$

Setning 5. N sé Galois útvíkkun á K og L sé hlutútvíkkun á K í N. Ef $\tau \in \mathrm{Gal}(N/K)$ þá er

$$\mathrm{Gal}(N/\tau(L)) = \tau \circ \mathrm{Gal}(N/L) \circ \tau^{-1}$$

Sönnun. Ef $x \in L$ og $\sigma \in \mathrm{Gal}(N/K)$ þá er $\sigma(\tau(x)) = \tau(x)$ þá og því aðeins að $\tau^{-1}(\sigma(\tau(x))) = x$. Af Setningu 4 leiðir því að $\sigma \in \mathrm{Gal}(N/\tau(L))$ þá og því aðeins að $\tau^{-1} \circ \sigma \circ \tau \in \mathrm{Gal}(N/L)$.

Setning 6. N sé Galois útvíkkun á K og L sé hlutútvíkkun á K í N. Þá er L normleg útvíkkun á K þá og því aðeins að $\mathrm{Gal}(N/L)$ sé normleg hlutgrúpa í $\mathrm{Gal}(N/K)$. Ef svo er þá er L Galois útvíkkun á K og einskorðun við L gefur af sér einsmótun grúpna

$$\mathrm{Gal}(N/K)/\mathrm{Gal}(N/L) \cong \mathrm{Gal}(L/K)$$

Sönnun. Látum $\overline{K}$ vera algebrulega lokun á K sem inniheldur N. Samkvæmt Setningu 1 í Kafla 2 er L þá normleg útvíkkun á K þá og því aðeins að fyrir sérhverja K-mótun $\varphi : L \to \overline{K}$ gildi $\varphi(L) = L$. Samkvæmt umræðunni á eftir Setningu 14 í Kafla 1 má framlengja sérhverja slíka K-mótun φ í K-mótun $\chi : N \to \overline{K}$. Þar sem N er normleg útvíkkun á K, þá er $\chi(N) = N$, svo að χ gefur af sér K-einsmótun $\tau : N \to N$. Auk þess er $\varphi(L) = \chi(L) \subseteq \chi(N) = N$. Þetta sýnir að L er normleg útvíkkun á K þá og því aðeins að $\tau(L) = L$ fyrir sérhvert $\tau \in \mathrm{Gal}(N/K)$. Af Setningu 4 og athugasemd við hana leiðir að $\tau(L) = L$ þá og því aðeins að $\mathrm{Gal}(N/\tau(L)) = \mathrm{Gal}(N/L)$. Samkvæmt Setningu 5 þýðir það einmitt að $\tau \circ \mathrm{Gal}(N/L) \circ \tau^{-1} = \mathrm{Gal}(N/L)$. Þetta sannar fyrri hluta setningarinnar.

Nú sé L normleg útvíkkun á K. Þar sem N er aðskiljanleg útvíkkun á K, þá er L augljóslega aðskiljanleg útvíkkun á K og þar með Galois útvíkkun á K. Samkvæmt ofansögðu þá er $\tau(L) = L$ fyrir sérhvert $\tau \in \mathrm{Gal}(N/K)$, svo að τ gefur af sér K-einsmótun $\tau_L : L \to L$ — einskorðun τ við L. Vörpunin $\mathrm{Gal}(N/K) \to \mathrm{Gal}(L/K)$, $\tau \mapsto \tau_L$, er greinilega grúpumótun. Af ofansögðu er ljóst að sérhverja K-einsmótun $\sigma : L \to L$ má framlengja í K-einsmótun $\tau : N \to N$. Það þýðir að þessi grúpumótun er átæk. Að τ sé í kjarna hennar þýðir að $\tau(x) = x$ fyrir sérhvert $x \in L$. Samkvæmt Setningu 4 er því kjarni hennar jafn $\mathrm{Gal}(N/L)$.

Setning 7. Ef N er endanleg Galois útvíkkun á K þá er

$$\sharp(\mathrm{Gal}(N/K)) = [N : K]$$

Sönnun. Látum $\overline{K}$ vera algebrulega lokun á K sem inniheldur N. Þar sem N er aðskiljanleg útvíkkun á K, þá er fjöldi K-mótana $\varphi : N \to \overline{K}$ jafn

$[N : K]$ samkvæmt Setningu 12 í Kafla 2. Þar sem N er normleg útvíkkun á K, þá er $\varphi(N) = N$ fyrir sérhverja slíka K-mótun φ samkvæmt Setningu 1 í Kafla 2. Fjöldi K-mótana $\varphi : N \to \overline{K}$ er því jafn fjölda K-mótana $\sigma : N \to N$, þ.e.a.s. jafn $\sharp(\mathrm{Gal}(N/K))$.

Setning 8. Ef N er endanleg Galois útvíkkun á K og L er hlutútvíkkun á K í N þá er

$$(\mathrm{Gal}(N/K) : \mathrm{Gal}(N/L)) = [L : K]$$

Sönnun. Þar sem $\sharp(\mathrm{Gal}(N/K)) = \sharp(\mathrm{Gal}(N/L)) \cdot (\mathrm{Gal}(N/K) : \mathrm{Gal}(N/L))$ og $[N : K] = [N : L][L : K]$, þá er þetta afleiðing af Setningu 7.

Setning 8 gildir reyndar líka fyrir óendanlegar Galois útvíkkanir N á K ef $[L : K]$ er endanlegt.

Setning 9. N sé endanleg Galois útvíkkun á K og H sé hlutgrúpa í $\mathrm{Gal}(N/K)$. Látum

$$L = \{x \in N \mid \sigma(x) = x \text{ fyrir sérhvert } \sigma \in H\}$$

Þá er L hlutútvíkkun á K í N og $\mathrm{Gal}(N/L) = H$.

Sönnun. Við höfum þegar séð að L er hlutútvíkkun á K í N. Ef $\sigma \in H$ þá er augljóslega $\sigma(x) = x$ fyrir sérhvert $x \in L$. Samkvæmt Setningu 4 er því $H \subseteq \mathrm{Gal}(N/L)$.

Samkvæmt Setningu 18 í Kafla 2 er til stak $s \in N$ með $N = L(s)$. Látum $f = \prod_{\tau \in H}(X - \tau(s))$. Fyrir sérhvert $\sigma \in H$ er þá

$$\sigma(f) = \prod_{\tau \in H}(X - \sigma(\tau(s))) = \prod_{\tau' \in H}(X - \tau'(s)) = f$$

Samkvæmt skilgreiningunni á L þá þýðir þetta að $f \in L[X]$. Látum nú p vera lágmargliðu s yfir L. Þar sem s er greinilega rót á f, þá gengur p upp í f. Þar sem gráða p er jöfn $[N : L]$ og gráða f er jöfn $\sharp(H)$, þá leiðir af þessu að $[N : L] \leq \sharp(H)$, þ.e.a.s. $\sharp(\mathrm{Gal}(N/L)) \leq \sharp(H)$. Þar sem $H \subseteq \mathrm{Gal}(N/L)$, þá leiðir af þessu að $H = \mathrm{Gal}(N/L)$.

Athugasemd. Margliðan f í sönnuninni er reyndar lágmargliða s yfir L. Lágmargliðan gengur nefnilega upp í f og samkvæmt lokaniðurstöðunni þá hefur hún sömu gráðu og f.

Ef N er óendanleg Galois útvíkkun á K þá er setningin ekki rétt fyrir allar hlutgrúpur H í $\mathrm{Gal}(N/K)$. Sýna má að hún sé rétt fyrir hlutgrúpuna H þá og því aðeins að H sé sniðmengi allra þeirra hlutgrúpna U í $\mathrm{Gal}(N/K)$ sem innihalda H og hafa endanlegan vísi í $\mathrm{Gal}(N/K)$.

Við tökum nú saman helztu niðurstöðurnar í endanlega tilfellinu.

Meginsetning. N sé endanleg Galois útvíkkun á K með Galois grúpu G. Gagnkvæm samsvörun er þá á milli hlutútvíkkana L á K í N og hlutgrúpna H í G. Hún er gefin með

$$H = \{\sigma \in G \,|\, \sigma(x) = x \text{ fyrir sérhvert } x \in L\}$$

og

$$L = \{x \in N \,|\, \sigma(x) = x \text{ fyrir sérhvert } \sigma \in H\}$$

Ennfremur gildir:

(i) L er Galois útvíkkun á K þá og því aðeins að H sé normleg hlutgrúpa í G. Galois grúpa L yfir K er þá einsmóta deildagrúpunni G/H.

(ii) $L_1 \subseteq L_2$ þá og því aðeins að $H_2 \subseteq H_1$.

(iii) $[L : K] = (G : H)$

Í atriði (ii) er, að sjálfsögðu, gert ráð fyrir að L_1 samsvari H_1 og að L_2 samsvari H_2. Reglan í því hefur ekki komið áður fram en hún er augljós afleiðing af skilgreiningum. Hún er reyndar mikilvægara en virðist í fljótu bragði.

Þar sem $L_1 \cap L_2$ er stærsta hlutútvíkkunin á K í N sem innihaldin er í bæði L_1 og L_2, þá er, samkvæmt atriði (ii), samsvarandi hlutgrúpa í G minnsta hlutgrúpan í G sem inniheldur bæði H_1 og H_2. Það er ekki alltaf auðvelt að lýsa þessari hlutgrúpu. En stundum er mengið $\{\sigma_1\sigma_2 \,|\, \sigma_1 \in H_1 \text{ og } \sigma_2 \in H_2\}$ hlutgrúpa í G og þá greinilega minnsta hlutgrúpan í G sem inniheldur bæði H_1 og H_2. Þetta er til dæmis tilfellið ef H_1 eða H_2 er normleg hlutgrúpa í G.

Eins fæst að $H_1 \cap H_2$ samsvarar minnstu hlutútvíkkun á K í N sem inniheldur bæði L_1 og L_2. Þessari útvíkkun má lýsa sem $K(L_1 \cup L_2)$ en hún er venjulega táknuð L_1L_2.

Þegar hefur komið fram að klofningskroppur fyrir aðskiljanlega margliðu yfir K er endanleg Galois útvíkkun á K. Galois grúpa klofningskroppsins yfir K er þá kölluð Galois grúpa margliðunnar yfir K.

Látum N vera klofningskropp fyrir aðskiljanlega margliðu f yfir K og látum G vera Galois grúpu f yfir K, þ.e.a.s. $G = \mathrm{Gal}(N/K)$. Margliðan f klofnar yfir N, segjum

$$f = a(X - s_1) \cdots (X - s_n)$$

með $a \in K$ og $s_1, \ldots, s_n \in N$. Ræturnar $s_1, \ldots, s_n$ eru þá allar mismunandi og $N = K(s_1, \ldots, s_n)$. Nú sé $\sigma \in G$. Þar sem σ varpar rót á f í rót á f, þá

gefur σ af sér umröðun í menginu $\{s_1, \ldots, s_n\}$. Þar sem $N = K(s_1, \ldots, s_n)$, þá ákvarðast σ líka algjörlega af þessari umröðun. Þetta þýðir að við getum litið á G sem hlutgrúpu í grúpu allra umraðana í menginu $\{s_1, \ldots, s_n\}$. Það er hinn upprunalegi hugsanaháttur í Galois fræðum.

4 Notkunardæmi

Í þessum kafla táknar K alltaf kropp.

Norm og spor

Í þessum undirkafla táknar L alltaf endanlega útvíkkun á K. Við látum $n = [L : K]$.

Lítum á L sem vigurrúm yfir K. Fyrir sérhvert stak c í L er vörpunin $\mu_c : L \to L$, $x \mapsto cx$, — margföldun með c — K-línuleg vörpun. Ákveða μ_c er kölluð norm c og er táknuð $\mathrm{N}_{L/K}(c)$. Spor μ_c er kallað spor c og er táknað $\mathrm{Sp}_{L/K}(c)$.

Setning 1. Við höfum

$$\mathrm{N}_{L/K}(c_1c_2) = \mathrm{N}_{L/K}(c_1)\mathrm{N}_{L/K}(c_2)$$

og

$$\mathrm{Sp}_{L/K}(c_1 + c_2) = \mathrm{Sp}_{L/K}(c_1) + \mathrm{Sp}_{L/K}(c_2) \quad \text{og} \quad \mathrm{Sp}_{L/K}(ac) = a\mathrm{Sp}_{L/K}(c)$$

fyrir sérhver $c, c_1, c_2 \in L$ og sérhvert $a \in K$.

Sönnun. Þar sem $\mu_{c_1c_2} = \mu_{c_1} \circ \mu_{c_2}$, $\mu_{c_1+c_2} = \mu_{c_1} + \mu_{c_2}$ og $\mu_{ac} = a\mu_c$, þá er þetta einföld afleiðing af þekktum setningum um ákveður og spor K-línulegra varpana.

Í sönnun Setningar 1 kemur fram að vörpunin $L \to \mathrm{End}_K(L)$, $c \mapsto \mu_c$, er mótun K-algebra. Ljóst er að þessi vörpun er eintæk. Af því leiðir að fyrir margliðu f yfir K er $f(\mu_c) = 0$ þá og því aðeins að $f(c) = 0$. Sér í lagi er lágmargliða μ_c jöfn lágmargliðu c yfir K.

Setning 2. Gefið sé stak c í L. Látum $X^m + a_{m-1}X^{m-1} + \cdots + a_0$ vera lágmargliðu c. Þá gengur m upp í n og

$$\mathrm{N}_{L/K}(c) = (-1)^n a_0^k \quad \text{og} \quad \mathrm{Sp}_{L/K}(c) = -ka_{m-1}$$

þar sem $k = n/m$.

Sönnun. Látum $f = X^n + b_{n-1}X^{n-1} + \cdots + b_0$ vera kennimargliðu μ_c. Þá er $\mathrm{N}_{L/K}(c) = \det(\mu_c) = (-1)^n b_0$ og $\mathrm{Sp}_{L/K}(c) = \mathrm{Sp}(\mu_c) = -b_{n-1}$. Látum nú p vera lágmargliðu c og þá líka lágmargliðu μ_c. Samkvæmt setningu Cayleys og Hamiltons eru það sömu frummargliðurnar yfir K sem ganga upp

í lágmargliðu μ_c og kennimargliðu μ_c. Þar sem p er frummargliða yfir K, þá þýðir það að f er veldi af p, svo að $f = p^k$. Sér í lagi er $b_0 = a_0^k$ og $b_{n-1} = ka_{m-1}$.

Setning 3. L sé Galois útvíkkun á K með Galois grúpu G. Gefið sé stak c í L. Þá er

$$\mathrm{N}_{L/K}(c) = \prod_{\sigma \in G} \sigma(c) \quad \text{og} \quad \mathrm{Sp}_{L/K}(c) = \sum_{\sigma \in G} \sigma(c)$$

Sönnun. Látum $H = \mathrm{Gal}(L/K(c))$. Þá er $H = \{\sigma \in G \mid \sigma(c) = c\}$. Af því sést að $\sigma_2(c) = \sigma_1(c)$ þá og því aðeins að til sé $\rho \in H$ með $\sigma_2 = \sigma_1 \circ \rho$, þ.e.a.s. $\sigma_2 H = \sigma_1 H$. Samkvæmt athugasemd við Setningu 3 í Kafla 3 þá er margliðan $p = \prod_{\tau H \in G/H}(X - \tau(c))$ því lágmargliða c yfir K. (Margfaldað er yfir stökin í G/H. Fyrir sérhvert slíkt stak er valinn fulltrúi τ í G.) Ef $\rho \in H$ þá er $\rho(c) = c$, svo að $\tau(\rho(c)) = \tau(c)$. Því fæst einnig að $p = \prod_{\tau H \in G/H}(X - \tau(\rho(c)))$.

Látum f vera kennimargliðu μ_c. Eins og í sönnun Setningar 2 sést að f er veldi af p, segjum $f = p^k$. Þá er $n = km$ þar sem m er gráða p, þ.e.a.s. $m = [K(c) : K]$. Af þessu sést að $k = [L : K(c)]$, þ.e.a.s. $k = \sharp(H)$. Með því að margfalda yfir stökin í H fæst því

$$f = p^{\sharp(H)} = \prod_{\rho \in H} \prod_{\tau H \in G/H} (X - \tau(\rho(c))) = \prod_{\sigma \in G} (X - \sigma(c))$$

Setningin er nú afleiðing af þessari lýsingu á f.

Meginsetning algebrunnar

Setning 4. K sé kroppur með kennitölu $\neq 2$ þannig að eftirfarandi gildi:

(i) Sérhver margliða af ójafnri gráðu yfir K hefur rót í K.

(ii) Sérhvert stak í K er í K^2 eða $-K^2$.

(iii) Ef $x, y \in K$ þá er $x^2 + y^2 \in K^2$.

Látum $L = K(\sqrt{-1})$. Þá er L algebruleg lokun á K.

(Hér er $K^2 = \{x^2 \mid x \in K\}$.)

Sönnun. Sanna þarf að L hafi enga eiginlega endanlega útvíkkun, þ.e.a.s. að K hafi enga endanlega útvíkkun, sem inniheldur L, nema L. Þar sem kennitala K er ekki 2, þá leiðir af (i) að K er fullkominn, svo að sérhver endanleg útvíkkun á K er aðskiljanleg. Með því að athuga normlegar lokanir yfir K sést að það nægir að sanna að K hefur enga endanlega Galois útvíkkun, sem inniheldur L, nema L.

N sé endanleg Galois útvíkkun á K með Galois grúpu G. Látum H vera Sylow 2-hlutgrúpu í G og látum M vera samsvarandi hlutútvíkkun á K í N.

Þá er gráðan $[M : K]$ ójöfn, því að $[M : K] = (G : H)$. Sér í lagi hefur sérhvert stak í M ójafna gráðu yfir K. En samkvæmt (i) er lágmargliða staksins þá línuleg, svo að stakið er í K. Þetta sýnir að $M = K$, þ.e.a.s. $H = G$, svo að G er 2-grúpa.

Nú sé N endanleg Galois útvíkkun á K sem inniheldur L. Látum $G = \mathrm{Gal}(N/K)$ og $H = \mathrm{Gal}(N/L)$. Samkvæmt ofansögðu er G þá 2-grúpa og H því líka. Ef $\sharp(H) > 1$ þá væri því til hlutgrúpa í H með vísi 2 í H. Það þýddi að til væri hlutútvíkkun á L í N af gráðu 2. Það nægir því að sanna að L hafi enga útvíkkun af gráðu 2. Þar sem kennitala L er ekki 2, þá er það jafngilt því að $L = L^2$. (Heimaverkefni.)

Ef $L = K$ þá er $-1 \in K^2$, svo að samkvæmt (ii) er $K = K^2$, þ.e.a.s. $L = L^2$. Þá sé $L \neq K$. Gefið sé $c \in L$. Skrifum $c = a + b\sqrt{-1}$ með $a, b \in K$. Þá er $\mathrm{N}_{L/K}(c) = a^2 + b^2$. Samkvæmt (iii) er því $\mathrm{N}_{L/K}(c) \in K^2$. Af (ii) leiðir þá að $c \in L^2$. (Heimaverkefni.)

Það er einföld afleiðing af milligildissetningunni fyrir samfelld föll á $\mathbf{R}$ að $\mathbf{R}$ uppfyllir skilyrði setningarinnar. Af setningunni leiðir því að $\mathbf{C}$ er algebruleg lokun á $\mathbf{R}$.

K sé kroppur sem uppfyllir skilyrði setningarinnar. Af skilyrði (iii) leiðir að ef -1 er summa staka í K^2 þá er -1 í K^2 og því $L = K$. Samkvæmt setningunni er K þá algebrulega lokaður. Ef kennitala K er $p > 0$ þá er þetta alltaf tilfellið því að -1 er summa $p - 1$ eintaka af 1^2. Ef hinsvegar -1 er ekki summa staka í K^2 þá má skilgreina röðun $\leq$ í K með því að setja $a \leq b$ þá og því aðeins að $b - a \in K^2$.

Endanlegir kroppar

Í þessum undirkafla er p frumtala.

L sé endanlegur kroppur með kennitölu p. Þar sem $\{n \cdot 1_L \mid n \in \mathbf{Z}\}$ er einsmóta $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$, þá getum við litið á L sem útvíkkun á $\mathbf{F}_p$. Þar sem L er endanlegur kroppur, þá er L endanleg útvíkkun á $\mathbf{F}_p$. Af því leiðir að $\sharp(L) = p^n$ þar sem $n = [L : \mathbf{F}_p]$.

Setning 5. Ef kroppur hefur nákvæmlega $q = p^n$ stök þá er hann klofningskroppur fyrir margliðuna $X^q - X$ yfir $\mathbf{F}_p$. Sér í lagi eru sérhverjir tveir kroppar með nákvæmlega q stök einsmóta.

Sönnun. (Heimaverkefni.)

Veljum okkur algebrulega lokun Ω á $\mathbf{F}_p$. Af setningunni leiðir að fyrir sérhvert $n \geq 1$ er til einn og aðeins einn hlutkroppur í Ω sem hefur nákvæmlega

$q = p^n$ stök. Hann samanstendur af öllum $x \in \Omega$ þannig að $x^q = x$. Þessi kroppur er táknaður $\mathbf{F}_q$.

Setning 6. Ef $q = p^n$ þá er $\mathbf{F}_q$ Galois útvíkkun á $\mathbf{F}_p$. Galois grúpan $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$ er rásuð, spönnuð af mótuninni $\mathbf{F}_q \to \mathbf{F}_q$, $x \mapsto x^p$.

Sönnun. Þar sem $\mathbf{F}_q$ er klofningskroppur fyrir aðskiljanlega margliðu yfir $\mathbf{F}_p$, þá er $\mathbf{F}_q$ Galois útvíkkun á $\mathbf{F}_p$. Þar sem $\mathbf{F}_p$ er fastakroppur mótunarinnar í setningunni, þá er Galois grúpan spönnuð af þessari mótun.

Mótunin $\varphi : \Omega \to \Omega$, $x \mapsto x^p$, er kölluð mótun Frobeniusar. Mótunin í Setningu 6 er þá einskorðun φ við $\mathbf{F}_q$. Ef $m \geq 1$ þá er greinilega $\varphi^m(x) = x^{p^m}$ fyrir sérhvert $x \in \Omega$. Því fæst almennt að $\mathbf{F}_{p^m}$ er fastakroppur φ^m. Eftirfarandi útvíkkun á Setningu 6 er afleiðing af þessu.

Setning 7. Ef $m|n$ þá er $\mathbf{F}_{p^n}$ Galois útvíkkun á $\mathbf{F}_{p^m}$ og Galois grúpan $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_{p^m})$ er rásuð, spönnuð af mótuninni $\mathbf{F}_{p^n} \to \mathbf{F}_{p^n}$, $x \mapsto x^{p^m}$.

Athugasemd. Þar sem $[\mathbf{F}_{p^n} : \mathbf{F}_p] = n$ og $[\mathbf{F}_{p^m} : \mathbf{F}_p] = m$, þá getur $\mathbf{F}_{p^n}$ ekki verið útvíkkun á $\mathbf{F}_{p^m}$ nema $m|n$.

Einingarrætur

Í þessum undirkafla er n náttúrleg tala.

Stak u í K er sagt vera n-ta einingarrót ef $u^n = 1$, þ.e.a.s. ef u er rót á margliðunni $X^n - 1$. Mengi allra n-tu einingarróta í K er táknað $\mu_n(K)$. Ljóst er að $\mu_n(K)$ er hlutgrúpa í margföldunargrúpu K. Af því leiðir að $\mu_n(K)$ er rásuð.

Ef kennitala K er $p > 0$ og p gengur upp í n, segjum $n = pm$, þá er $u^n - 1 = (u^m - 1)^p$, svo að $u^n = 1$ þá og því aðeins að $u^m = 1$. Þetta þýðir að það nægir þá að athuga n þannig að p gengur ekki upp í n.

Í því sem eftir fer í þessum undirkafla munum við alltaf gera ráð fyrir að kennitala K gangi ekki upp í n. Þá er margliðan $X^n - 1$ aðskiljanleg.

Sagt er að K hafi allar n-tu einingarrætur ef margliðan $X^n - 1$ klofnar yfir K. Þar sem $X^n - 1$ er aðskiljanleg, þá þýðir þetta að K hefur n mismunandi n-tu einingarrætur. Stak sem spannar grúpuna $\mu_n(K)$ er þá sagt vera frumstæð n-ta einingarrót.

u sé frumstæð n-ta einingarrót í K. Sérhver n-ta einingarrót í K er þá af taginu u^k þar sem k er ótvírætt ákvarðað módúló n. Þetta gefur því af sér einsmótun grúpna $\mu_n(K) \cong \mathbf{Z}/n\mathbf{Z}$. Þessi einsmótun er háð valinu á frumstæðu n-tu einingarrótinni u.

Ef v er einhver n-ta einingarrót í K, segjum $v = u^k$, þá er v frumstæð n-ta einingarrót þá og því aðeins að k spanni $\mathbf{Z}/n\mathbf{Z}$ sem grúpu, þ.e.a.s. þá og því aðeins að k sé eining í baugnum $\mathbf{Z}/n\mathbf{Z}$. Fjöldi frumstæðra n-tu einingarróta í K er því jafn fjölda eininga í baugnum $\mathbf{Z}/n\mathbf{Z}$. Þessi fjöldi er táknaður $\varphi(n)$. Fallið φ er nefnt Euler fallið.

Fyrir gefna n-tu einingarrót v er til ein og aðeins ein grúpumótun $\mu_n(K) \to \mu_n(K)$ sem varpar u í v. Ef $v = u^k$ þá er hún gefin með $w \mapsto w^k$. Hálfgrúpa allra grúpumótana $\mu_n(K) \to \mu_n(K)$ er því einsmóta margföldunarhálfgrúpu baugsins $\mathbf{Z}/n\mathbf{Z}$. Grúpa allra grúpueinsmótana $\mu_n(K) \to \mu_n(K)$ er þar með einsmóta grúpu allra eininga í $\mathbf{Z}/n\mathbf{Z}$. Sér í lagi hefur þessi grúpa nákvæmlega $\varphi(n)$ stök. Athugum að þessi einsmótun er óháð valinu á frumstæðu n-tu einingarrótinni u.

Ef $n = q^e$ þar sem q er frumtala og $e \geq 1$ þá er stak k í $\mathbf{Z}/n\mathbf{Z}$ eining þá og því aðeins að það sé ekki margfeldi af q. Því fæst að $\varphi(q^e) = q^e - q^{e-1} = q^e(1 - \frac{1}{q})$.

Ef $n = n_1 n_2$ með ósamþátta n_1 og n_2 þá er $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z}$ samkvæmt kínversku leifasetningunni. Af því fæst að $\varphi(n) = \varphi(n_1)\varphi(n_2)$.

Af öllu þessu sést að almennt gildir

$$\varphi(n) = n(1 - \tfrac{1}{q_1}) \cdots (1 - \tfrac{1}{q_r})$$

ef $n = q_1^{e_1} \cdots q_r^{e_r}$ með mismunandi frumtölum $q_1, \ldots, q_r$ og $e_1, \ldots, e_r \geq 1$.

Setning 8. L sé klofningskroppur fyrir $X^n - 1$ yfir K. Þá er L Galois útvíkkun á K. Galois grúpan $\mathrm{Gal}(L/K)$ er víxlin. Hún er, nánar tiltekið, einsmóta hlutgrúpu í grúpu allra eininga í baugnum $\mathbf{Z}/n\mathbf{Z}$.

Sönnun. L er klofningskroppur fyrir aðskiljanlega margliðu yfir K, svo að L er Galois útvíkkun á K. L hefur allar n-tu einingarrætur og er spönnuð af þeim yfir K. Sérhver K-einsmótun $L \to L$ gefur af sér einsmótun $\mu_n(L) \to \mu_n(L)$. Hún ákvarðast líka af einsmótuninni $\mu_n(L) \to \mu_n(L)$, svo að $\mathrm{Gal}(L/K)$ er einsmóta hlutgrúpu í grúpu allra einsmótana $\mu_n(L) \to \mu_n(L)$.

K hafi allar n-tu einingarræturnar. Margliðan Φ_n er þá skilgreind sem margfeldi margliðanna $X - u$ þar sem u er frumstæð n-ta einingarrót í K. Gráða Φ_n er því jöfn $\varphi(n)$.

Sérhver n-ta einingarrót í K er frumstæð d-ta einingarrót fyrir einhvern deili d í n. Því fæst að

$$X^n - 1 = \prod_{d|n} \Phi_d$$

Þetta gefur aðferð til að reikna Φ_n ef Φ_d er þekkt fyrir sérhvern eiginlegan deili d í n. Þar sem $\Phi_1 = X - 1$, þá sést af þessu með þrepun að $\Phi_n \in \mathbf{Z}[X]$ ef kennitala K er 0 og $\Phi_n \in \mathbf{F}_p[X]$ ef kennitala K er $p > 0$.

Við munum líta á Φ_n sem margliðu yfir $\mathbf{Z}$. Hún er þá kölluð n-ta hringskiptingarmargliðan. (Tilsvarandi margliða yfir $\mathbf{F}_p$ fæst einfaldlega með að reikna módúló p.)

Setning 9. $\Phi_n \in \mathbf{Z}[X]$ er frummargliða yfir $\mathbf{Q}$.

Sönnun. Samkvæmt Lemma Gauss er til frumþáttun á Φ_n yfir $\mathbf{Q}$ þannig að allir frumþættirnir séu heiltölumargliður. Þar sem Φ_n er stöðluð, má gera ráð fyrir að allir frumþættirnir séu líka staðlaðir. Sér í lagi má skrifa $\Phi_n = fg$ þar sem f er stöðluð heiltölumargliða sem er óþáttanleg yfir $\mathbf{Q}$ og g er stöðluð heiltölumargliða. Látum $u \in \mathbf{C}$ vera rót á f. Þá er u frumstæð n-ta einingarrót og f er lágmargliða u yfir $\mathbf{Q}$.

Gefin sé rót v á f og frumtala q sem gengur ekki upp í n. Gerum ráð fyrir að v^q sé ekki rót á f. Þar sem v^q er frumstæð n-ta einingarrót, þá er v^q rót á $\Phi_n = fg$, svo að v^q er þá rót á g. En þá er v rót á margliðunni $g(X^q)$, svo að $f(X)$ gengur upp í $g(X^q)$, segjum $g(X^q) = f(X)h(X)$. Þar sem $g(X^q) \in \mathbf{Z}[X]$ og $f(X) \in \mathbf{Z}[X]$ er stöðluð, þá er $h(X) \in \mathbf{Z}[X]$. Nú er $g(X^q) \equiv g(X)^q$ og þar með $g(X)^q \equiv f(X)h(X)$ módúló q. Ef $k(X)$ er frumþáttur í $f(X)$ módúló q þá er $k(X)$ þar með einnig frumþáttur í $g(X)$ módúló q. En þá er $k(X)$ a.m.k. tvöfaldur frumþáttur í $\Phi_n = fg$ módúló q. Það fær ekki staðist, því að Φ_n er aðskiljanleg módúló q. Því hlýtur v^q að vera rót á f.

Með þrepun fæst að ef $k = q_1 \cdots q_r$ með frumtölum $q_1, \ldots, q_r$, sem ekki ganga upp í n, þá er u^k rót á f. En sérhverja frumstæða n-tu einingarrót (í $\mathbf{C}$) má skrifa sem u^k, þar sem k er ósamþátta n, svo að sérhver frumstæð n-ta einingarrót er rót á f. Það þýðir að Φ_n gengur upp í f. Þetta sýnir að $f = \Phi_n$.

Setning 10. u sé frumstæð n-ta einingarrót í $\mathbf{C}$. Þá er $\mathbf{Q}(u)$ Galois útvíkkun á $\mathbf{Q}$. Galois grúpan $\mathrm{Gal}(\mathbf{Q}(u)/\mathbf{Q})$ er einsmóta grúpu allra eininga í baugnum $\mathbf{Z}/n\mathbf{Z}$.

Sönnun. Látum $L = \mathbf{Q}(u)$. Sérhver n-ta einingarrót (í $\mathbf{C}$) er veldi af u, svo að L er klofningskroppur fyrir $X^n - 1$ yfir $\mathbf{Q}$. Samkvæmt Setningu 8 er L því Galois útvíkkun á $\mathbf{Q}$ og $\mathrm{Gal}(L/\mathbf{Q})$ er einsmóta hlutgrúpu í grúpu allra eininga í $\mathbf{Z}/n\mathbf{Z}$. En af Setningu 9 leiðir að $[L : \mathbf{Q}] = \varphi(n)$ sem er jafnt fjölda eininga í $\mathbf{Z}/n\mathbf{Z}$.

Rótardráttur

Í þessum undirkafla er n náttúrleg tala þannig að kennitala K gengur ekki upp í n. Við gerum líka ráð fyrir að K hafi allar n-tu einingarræturnar.

Setning 11. Gefið sé stak a í K, $a \neq 0$. Látum L vera klofningskropp fyrir margliðuna $X^n - a$ yfir K. Þá er L Galois útvíkkun á K. Galois grúpan $\mathrm{Gal}(L/K)$ er rásuð og fjöldatala hennar gengur upp í n.

Sönnun. $s \in L$ sé rót á $X^n - a$ og $u \in K$ sé frumstæð n-ta einingarrót. Þá eru stökin $s, us, \ldots, u^{n-1}s$ allar rætur $X^n - a$, svo að $L = K(s)$. K-einsmótun $L \to L$ hlýtur að varpa s yfir í eitthvert $u^k s$, þar sem k er ótvírætt ákvarðað módúló n. Hún ákvarðast líka af gildi s. Þetta gefur því eintæka grúpumótun $\mathrm{Gal}(L/K) \to \mathbf{Z}/n\mathbf{Z}$.

Setning 12. L sé Galois útvíkkun á K þannig að Galois grúpan $\mathrm{Gal}(L/K)$ sé rásuð og hafi fjöldatölu n. Þá er til stak a í K, $a \neq 0$, þannig að $L = K(s)$ með rót s á margliðunni $X^n - a$. Auk þess er $X^n - a$ frummargliða yfir K.

Sönnun. $\sigma \in \mathrm{Gal}(L/K)$ spanni $\mathrm{Gal}(L/K)$ og $u \in K$ sé frumstæð n-ta einingarrót. Þar sem varpanirnar $\sigma^0, \ldots, \sigma^{n-1} : L \to L$ eru línulega óháðar yfir L (heimaverkefni), þá er til $x \in L$ þannig að $s = \sum_{i=0}^{n-1} u^{-i}\sigma^i(x) \neq 0$. Augljósir reikningar sýna nú að $\sigma(s) = us$ og með þrepun fæst að $\sigma^j(s) = u^j s$. Látum $a = s^n$. Þá fæst að $\sigma(a) = a$, svo að $a \in K$. Auk þess fæst að stökin $s, \sigma(s), \ldots, \sigma^{n-1}(s)$ eru öll mismunandi, svo að id_L er eina stakið í $\mathrm{Gal}(L/K)$ sem lætur s fast. Af því leiðir að $L = K(s)$. Þar sem s er rót á $X^n - a$ og $[K(s) : K] = n$, þá hlýtur $X^n - a$ að vera lágmargliða s yfir K.

Leysanlegar jöfnur

Útvíkkun L á K er sögð vera einföld rótaútvíkkun á K ef $L = K(s)$ þar sem s er rót á margliðu af taginu $X^n - a$ yfir K.

Útvíkkun L á K er sögð vera rótaútvíkkun á K ef til er turn $K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m = L$ af af útvíkkunum á K þannig að L_i sé einföld rótaútvíkkun á L_{i-1}, $i = 1, \ldots, m$. Það þýðir að $L = K(s_1, \ldots, s_m)$ þannig að fyrir sérhvert $i = 1, \ldots, m$ sé til náttúrleg tala n_i þannig að $s_i^{n_i} \in K(s_1, \ldots, s_{i-1})$. Við segjum þá að $(s_1, \ldots, s_m)$ sé rótaruna fyrir L yfir K.

Setning 13. L sé rótaútvíkkun á K og N sé normleg lokun L yfir K. Þá er N líka rótaútvíkkun á K.

Sönnun. Látum $\overline{K}$ vera algebrulega lokun á K sem inniheldur N og látum $\varphi_1, \ldots, \varphi_n$ vera allar K-mótanir frá L yfir í $\overline{K}$. Ef $(s_1, \ldots, s_m)$ er rótaruna fyrir L yfir K þá er

$$(\varphi_1(s_1), \ldots, \varphi_1(s_m), \ldots, \varphi_n(s_1), \ldots, \varphi_n(s_m))$$

rótaruna fyrir N yfir K.

$f \neq 0$ sé margliða yfir K. Sagt er að jafnan $f(x) = 0$ sé leysanleg (með rótardrætti) yfir K ef til er rótaútvíkkun L á K þannig að f klofnar yfir L.

(Annar möguleiki væri að segja að jafnan $f(x) = 0$ væri leysanleg (með rótardrætti) yfir K ef til væri rótaútvíkkun L á K þannig að f hefði rót í L. Samkvæmt Setningu 13 mættum við þá gera ráð fyrir að L væri normleg útvíkkun á K. Fyrir frummargliðu f yfir K fengjum við því jafngilda skilgreiningu.)

Í því sem eftir er undirkaflans munum við gera ráð fyrir að kennitala K sé 0.

Næsta setning er setning Galois.

Setning 14. $f \neq 0$ sé margliða yfir K og G sé Galois grúpa f yfir K. Jafnan $f(x) = 0$ er leysanleg yfir K þá og því aðeins að grúpan G sé leysanleg.

Sönnun. Jafnan $f(x) = 0$ sé leysanleg yfir K. Þá er, samkvæmt Setningu 13, til Galois rótaútvíkkun L á K þannig að f klofnar yfir L. Látum $(s_1, \ldots, s_m)$ vera rótarunu fyrir L yfir K og skrifum $L_i = K(s_1, \ldots, s_i)$, $i = 0, 1, \ldots, m$. Látum $n_1, \ldots, n_m$ vera náttúrlegar tölur þannig að $s_i^{n_i} \in L_{i-1}$ og látum n vera minnsta samfeldi $n_1, \ldots, n_m$. Látum u vera frumstæða n-tu einingarrót. Þá er $L(u)$ rótaútvíkkun á K því að $(u, s_1, \ldots, s_m)$ er rótaruna fyrir $L(u)$ yfir K. Auk þess er $L(u)$ Galois útvíkkun á K því að ef L er klofningskroppur fyrir margliðuna g yfir K þá er $L(u)$ klofningskroppur fyrir margliðuna $(X^n - 1)g$ yfir K. Þetta sýnir að við megum gera ráð fyrir að s_1 sé frumstæð n-ta einingarrót og að L_{i-1} hafi allar n_i-tu einingarræturnar ef $i > 1$.

Látum þá $H = \mathrm{Gal}(L/K)$. Turninum $K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m = L$ samsvarar þá turn $H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{\mathrm{id}_L\}$ af hlutgrúpum í H. Samkvæmt Setningu 8 er $L_1 = K(u)$ Galois útvíkkun á K og Galois grúpan $\mathrm{Gal}(L_1/K)$ er víxlin. Það þýðir að H_1 er normleg hlutgrúpa í H og að deildagrúpan H/H_1 er víxlin. Nú sé $i > 1$ og $a_i = s_i^{n_i} \in L_{i-1}$. Þá er L_i hlutútvíkkun í klofningskroppi fyrir margliðuna $X^{n_i} - a_i$ yfir L_{i-1}. Af Setningu 11 leiðir því að L_i er Galois útvíkkun á L_{i-1} og að Galois grúpan $\mathrm{Gal}(L_i/L_{i-1})$ er víxlin. Það þýðir að H_i er normleg hlutgrúpa í H_{i-1} og að deildagrúpan H_{i-1}/H_i er víxlin. Þetta sýnir að grúpan H er leysanleg.

Látum nú $N \subseteq L$ vera klofningskropp fyrir f yfir K. Þá er $G = \mathrm{Gal}(N/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(N/L) = H/\mathrm{Gal}(N/L)$ einsmóta deildagrúpu af leysanlegri grúpu og því leysanleg.

Nú sé G leysanleg. Látum N vera klofningskropp fyrir f yfir K. Þá er $G = \mathrm{Gal}(N/K)$. Látum $n = \sharp(G)$ og látum u vera frumstæða n-tu einingarrót. Látum $L = N(u)$. Þá er L Galois útvíkkun á K því að L er klofningskroppur fyrir margliðuna $(X^n - 1)f$ yfir K. Látum $H = \mathrm{Gal}(L/K)$. Þá er grúpan H

leysanleg því að $\mathrm{Gal}(L/N)$ er víxlin samkvæmt Setningu 8 og $H/\mathrm{Gal}(L/N) \cong G$, sem er leysanleg samkvæmt forsendu. Látum $H_1 = \mathrm{Gal}(L/K(u))$. Þá er H_1 hlutgrúpa í leysanlegri grúpu og því leysanleg. Það er því til turn $H_1 \supseteq \cdots \supseteq H_m = \{\mathrm{id}_L\}$ af hlutgrúpum í H_1 þannig að H_i er normleg hlutgrúpa í H_{i-1} og þannig að H_{i-1}/H_i er rásuð, $i = 2, \ldots, m$. Turninum $H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{\mathrm{id}_L\}$ af hlutgrúpum í H samsvarar turn $K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m = L$ af útvíkkunum á K og $L_1 = K(u)$. Ef $i > 1$ þá er L_i einföld rótaútvíkkun á L_{i-1} samkvæmt Setningu 12. L er því rótaútvíkkun á K og jafnan $f(x) = 0$ þar með leysanleg yfir K.

Í seinni hluta sönnunar setningar Galois hefðum við getað valið turninn $H_1 \supseteq \cdots \supseteq H_m = \{\mathrm{id}_L\}$ af hlutgrúpum í H_1 þannig að $\sharp(H_i/H_{i-1})$ væri frumtala p_i, $i = 2, \ldots, m$. Fyrir framhald sönnunarinnar hefðum við þá einungis þurft að L_1 hefði allar p_i-tu einingarræturnar, $i = 2, \ldots, m$.

Ef nú p er stærst frumtalnanna $p_2, \ldots, p_m$ þá má nota sömu röksemdir á margliðuna $X^p - 1$ yfir K í stað f. Þar sem gráða klofningskropps fyrir þessa margliðu yfir K er minni en p, þá fæst eftirfarandi setning með þrepun.

Setning 15. $f \neq 0$ sé margliða yfir K. Ef jafnan $f(x) = 0$ er leysanleg yfir K þá er til rótaútvíkkun L á K þannig að f klofnar yfir L og rótaruna $(s_1, \ldots, s_m)$ fyrir L yfir K þannig að fyrir sérhvert $i = 1, \ldots, m$ gildir að s_i er rót á frummargliðu $X^{p_i} - a_i$ yfir $K(s_1, \ldots, s_{i-1})$ þar sem p_i er frumtala og $K(s_1, \ldots, s_{i-1})$ hefur allar p_i-tu einingarræturnar.

Almenna jafnan af n-tu gráðu

Látum $X_1, \ldots, X_n$ vera óháðar breytur yfir K. Fyrir sérhvert stak σ í umraðanagrúpunni S_n er þá til ein og aðeins ein K-mótun $K(X_1, \ldots, X_n) \to K(X_1, \ldots, X_n)$ sem varpar X_i í $X_{\sigma(i)}$, $i = 1, \ldots, n$. Við táknum þessa K-mótun líka með σ. Þetta gefur okkur þá túlkun á S_n sem hlutgrúpu í $\mathrm{Aut}_K(K(X_1, \ldots, X_n))$. Látum M vera fastakroppinn. Við vitum (heimaverkefni) að $K(X_1, \ldots, X_n)$ er þá Galois útvíkkun á M og að Galois grúpan er S_n.

Látum

$$\begin{aligned} Y_1 &= X_1 + \cdots + X_n \\ Y_2 &= X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n \\ &\vdots \\ Y_n &= X_1 \cdots X_n \end{aligned}$$

vera einföldu samhverfu margliðurnar í breytunum $X_1, \ldots, X_n$. Þá er ljóst að $K(Y_1, \ldots, Y_n) \subseteq M$ og að $K(X_1, \ldots, X_n)$ er klofningskroppur fyrir margliðuna $X^n - Y_1 X^{n-1} + \cdots + (-1)^n Y_n$ yfir $K(Y_1, \ldots, Y_n)$. Af því síðarnefnda leiðir að $[K(X_1, \ldots, X_n) : K(Y_1, \ldots, Y_n)] \leq n!$. En $[K(X_1, \ldots, X_n) : M] = n!$, svo að því hlýtur $M = K(Y_1, \ldots, Y_n)$.

Þetta þýðir að sérhvert samhverft rætt fall í $X_1, \ldots, X_n$ má skrifa sem rætt fall í $Y_1, \ldots, Y_n$. (Raunar má líka sýna að sérhverja samhverfa margliðu í $X_1, \ldots, X_n$ megi skrifa sem margliðu í $Y_1, \ldots, Y_n$.)

Látum nú $U_1, \ldots, U_n$ vera nýjar óháðar breytur yfir K og skrifum $\widetilde{K}$ fyrir $K(U_1, \ldots, U_n)$. Jafnan

$$x^n - U_1 x^{n-1} + \cdots + (-1)^n U_n = 0$$

er þá nefnd almenna n-tu gráðu jafnan yfir K.

Látum $\widetilde{L}$ vera klofningskropp fyrir margliðuna

$$X^n - U_1 X^{n-1} + \cdots + (-1)^n U_n$$

yfir $\widetilde{K}$ og látum $V_1, \ldots, V_n \in \widetilde{L}$ vera rætur hennar. Þá er

$$X^n - U_1 X^{n-1} + \cdots + (-1)^n U_n = (X - V_1) \cdots (X - V_n)$$

svo að

$$\begin{aligned} U_1 &= V_1 + \cdots + V_n \\ U_2 &= V_1 V_2 + V_1 V_3 + \cdots + V_{n-1} V_n \\ &\vdots \\ U_n &= V_1 \cdots V_n \end{aligned}$$

Sér í lagi er $K[U_1, \ldots, U_n] \subseteq K[V_1, \ldots, V_n]$.

Þar sem $U_1, \ldots, U_n$ eru óháðar breytur yfir K, þá er til ein og aðeins ein K-mótun $K[U_1, \ldots, U_n] \to K[Y_1, \ldots, Y_n]$ sem varpar U_i í Y_i, $i = 1, \ldots, n$. Á sama hátt er til ein og aðeins ein K-mótun $K[X_1, \ldots, X_n] \to K[V_1, \ldots, V_n]$ sem varpar X_i í V_i, $i = 1, \ldots, n$. Auk þess er örvaritið

$$\begin{array}{ccc} K[U_1, \ldots, U_n] & \subseteq & K[V_1, \ldots, V_n] \\ \downarrow & & \uparrow \\ K[Y_1, \ldots, Y_n] & \subseteq & K[X_1, \ldots, X_n] \end{array}$$

greinilega víxlið. Af því leiðir að K-mótunin $K[U_1, \ldots, U_n] \to K[Y_1, \ldots, Y_n]$ er eintæk og þar með gagntæk. Hún gefur því af sér einsmótun $\widetilde{K} \to K(Y_1, \ldots, Y_n)$.

Látum nú Ω vera algebrulega lokun á $K(X_1, \ldots, X_n)$. Þá má framlengja K-mótunina $\widetilde{K} \to K(Y_1, \ldots, Y_n)$ í K-mótun $\varphi : \widetilde{L} \to \Omega$. Þar sem $\varphi(U_i) = Y_i$, $i = 1, \ldots, n$, og V_j er rót á margliðunni $X^n - U_1 X^{n-1} + \cdots + (-1)^n U_n$, þá er $\varphi(V_j)$ rót á margliðunni $X^n - Y_1 X^{n-1} + \cdots + (-1)^n Y_n = (X - X_1) \cdots (X - X_n)$. Af þessu sést að φ gefur af sér gagntæka vörpun $\{V_1, \ldots, V_n\} \to \{X_1, \ldots, X_n\}$ og þar með einsmótun $\widetilde{L} \to K(X_1, \ldots, X_n)$. Þar sem röð $V_1, \ldots, V_n$ skiptir ekki máli, megum við gera ráð fyrir að $\varphi(V_j) = X_j$, $j = 1, \ldots, n$.

Þetta sýnir að $\widetilde{L}$ er Galois útvíkkun á $\widetilde{K}$ og að Galois grúpan er einsmóta S_n. Við höfum því sannað eftirfarandi setningu.

Setning 16. Almenna n-tu gráðu jafnan yfir K er aðskiljanleg og Galois grúpa hennar er einsmóta umraðanagrúpunni S_n.

Næsta setning er setning Abels.

Setning 17. Ef kennitala K er 0 og $n > 4$ þá er almenna n-tu gráðu jafnan yfir K ekki leysanleg.

Sönnun. Ef $n > 4$ þá er S_n ekki leysanleg.

Látum $D = \prod_{i<j}(V_i - V_j)^2$. Þá er D greinilega samhverf margliða í $V_1, \ldots, V_n$. Því má skrifa D sem rætt fall (raunar margliðu) í $U_1, \ldots, U_n$. Þetta stak D heitir aðgreinir almennu n-tu gráðu jöfnunnar yfir K. Ef kennitala K er ekki 2 þá má sýna að hlutútvíkkunin á $\widetilde{K}$ í $\widetilde{L}$, sem samsvarar hlutgrúpunni A_n í S_n, er $\widetilde{K}(\sqrt{D})$.