1 Põhimõisted

Definitsioon 1

Ringiks nimetatakse algebralist struktuuri $(R;+,\cdot)$, millel on defineeritud kaks binaarset tehet liitmine(+) ja korrutamine(·) nii, et liitmise suhtes on $(R;+)$ abelirühm ja korrutamise suhtes on $(R;\cdot)$ poolrühm ning lisaks sellele on täidetud distributiivsuse aktsioomid:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(b + c) \cdot a = b \cdot a + c \cdot b$$

Definitsioon 2

Integriteetkonnaks nimetatakse nulliteguriteta ühikelemendiga kommutatiivset ringi.

Definitsioon 3

Kaldkorpuseks nimetatakse ühikelemendiga ringi, mille igal nullelemendist erineval elemendil leidub pöördelement.

Definitsioon 4

Korpuseks nimetatakse kommutatiivset kaldkorpust.

Definitsioon 5

Integriteetkonna(korpuse) R karakteristikaks $charR$ nimetatakse ühikelemendi poolt moodutstatud aditiivse tsüklilise rühma $\langle 1\rangle = \{n1 \mid n \in \mathbb{N}\}$ elementide arvu, kui see on lõplik, või 0 vastasel juhul.

Teoreem 1

Lõpliku integriteetkonna karakteristika on algarv.

Tõestus

Et integriteetkond R on lõplik, siis peab $char\ R \in \mathbb{N}$. Olgu karakteristika $char\ R = n$, oletan $n = n_1 n_2$. Siis arvestades, karakteristika on võrrandi $n1 = 0$ vähim naturaalarvuline lahend, saan $0 = (n_1 n_2)1 = (n_1 1)(n_2 1)$. Nüüd et nulliteguri puuduvad, siis $n_1 1 = 0$ või $n_2 1 = 0$, millest $n \mid n_1$ või $n \mid n_2$. Et $n_1 \neq 0$ ja $n_2 \neq 0$, siis järelikult $n_1 = n$ või $n_2 = n$. Seega sain, et iga arvu n tegur on kas arv n või 1, siit karakteristika on algarv. □

Teoreem 2

Iga lõplik integriteetkond, milles on vähemalt 2 elementi on korpus.

Tõestus

Olgu R integriteetkond, et integriteetkond on kommutatiivne, siis näitan, et iga $a \in R^*$ on võrrandil $ax = 1$ täpselt üks lahend. Vaatlen funktsiooni $L : R \to R$, kus $L(x) = ax$. Näitan L on injektsioon. Olgu $L(x_1) = L(x_2)$, siis

$$ax_1 = ax_2 \Rightarrow a(x_1 - x_2) = 0 \Rightarrow^{a \neq 0} x_1 - x_2 = 0 \Rightarrow x_1 = x_2.$$

Seega on L injektsioon, millest $\mid L(R) \mid = \mid R \mid$ ja seega, arvestades R lõplikust ja seda $L(R) \subseteq R$, on selge L on sürjektsioon. Siit $\exists! b : ab = 1$ ja seega on R korpus.□

Teoreem 3

Kui R on integriteetkond, siis leidub selline korpus K, mille alamkorpus K' on isomorfne integriteetkonnaga R.

Tõestus

Vaatlen hulka $\Omega := R \times R^*$. Defineerin liitmise ja korrutamise

$$(a_1, b_1) + (a_2, b_2) := (a_1 b_2 + a_2 b_1, b_1 b_2)$$

$$(a_1, b_1)(a_2, b_2) := (a_1 a_2, b_1 b_2)$$

Ilmneb, et selliselt defineeritud struktuur on integriteetkond. Toon sisse ekvivalentsi klassid(murrud) lugedes $(a, b) \sim (c, d) \rightleftharpoons ad = cb$ ja tähistades $\frac{a}{b}$ paari (a, b) ekvivalentsi klassi. Defineerin tükeldusel $\Omega/\sim$ esindajate abil tehted:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}$$

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

Ilmneb, et need tehted on korrektsed ja saadud struktuur on korpus, kus

$$0 = \frac{0}{1}$$

$$1 = \frac{1}{1}$$

$$-\frac{a}{b} = \frac{-a}{b}$$

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$$

$$K' := \left\{ \frac{a}{1} \mid a \in R \right\}$$

□

Definitsioon 6

Korpust, mis saadi eelmises tõestuses nimetatakse integriteetkonna R jagatiskorpuseks.

2 Polünoomid üle lõplike korpuste

Definitsioon 1
Polünoomi $p(x) \notin K$ üle korpuse K nimetatakse taandumatuks, kui iga polünoom, mis jagab polünoomi $p(x)$ on kas korpuse K pööratav element või jagub $p(x)$.

Definitsioon 2
Ringi R alamhulka I nimetatakse ideaaliks, kui on täidetud järgmised tingimused:

$$\forall i \in I \ \forall r \in R \quad ir \in I, \ ri \in I$$

$$\forall a, b \in I \quad a - b \in I$$

Definitsioon 3
Kommutatiivses ringis nimetatakse peaideaaliks hulka $(a) := \{ar \mid r \in R\}$.

Definitsioon 4
Triviaalseteks ideaalideks kommutatiivses ühikelemendiga ringis nimetatakse (0) ja $(1) = R$.

Definitsioon 5
Kommutatiivset ringi, mille iga ideaal on peaideaal, nimetatakse peaideaaliringiks.

Definitsioon 6
Ideaali I nimetatakse maksimaalseks ringis R, kui iga ideaal $J \neq R$ ja $I \subseteq J$ on võrdne ideaaliga I.

Definitsioon 7
Mittetriviaalset ideaali I nimetatakse algideaaliks ringis R, kui iga $ab \in I$ vähemalt üks teguritest on ideaalis I.

Teoreem 1
Polünoomide ring $K[x]$ üle korpuse K on peaideaaliring.
Tõestus
Olgu meil suvaline ideaal I. Siis on võimalik leida ideaalis vähima astmega polünoom(neid võib olla mitu) $p(x)$. Näitan, et kui $f(x) \in I$, siis $p(x) \mid f(x)$. Olgu polünoomide jäägiga jagamisel saadud tulemus $f(x) = q(x)p(x)+r(x)$, kus $deg\, r(x) < deg\, p(x)$ või $r(x) = 0$. Et $f(x), p(x) \in I$, siis $r(x) = f(x)-q(x)p(x) \in I$. Seega polünoomi $p(x)$ astme minimaalsusest peab $r(x) = 0$ ja siit $p(x) \mid f(x)$. Seega iga ideaal on polünoomide ringis peaideaal.□

Teoreem 2

Polünoomide ringis $K[x]$ üle korpuse K on järgmised kolm väidet ekvivalentsed:

1. *polünoom $p(x)$ on taandumatu üle korpuse K;*
2. *ideaal $(p(x))$ on mittetrivaaalne ja maksimaalne;*
3. *ideaal $(p(x))$ on algideaal;*

Tõestus

$1 \Rightarrow 2$

Olgu $p(x)$ taandumatu ja olgu $(p(x)) \subseteq I$, siis et polünoomide ring on peaideaaliring, siis $I = (q(x))$. Et $p(x) \in (q(x))$, siis $q(x) \mid p(x)$. Nüüd $p(x)$ taandumatusest:

1. $q(x) = 1 \Rightarrow (g(x)) = R$;
2. $q(x) = p(x) \Rightarrow (g(x)) = (p(x))$.

Seega $(p(x))$ on maksimaalne. Et $p(x)$ on taandumatu, siis $p(x) \notin K$ ja seega on ideaal $(p(x))$ mittetriviaalne.

$2 \Rightarrow 3$

Olgu $p(x)$ maksimaalne ideaal ja $f(x)g(x) \in (p(x))$. Kui $f(x) \notin (p(x))$, siis olgu J ideaal, mis sisaldab $p(x)$ ja $f(x)$. Nüüd konstruktsioonist võib võtta $J = \{i(x) + f(x)r(x) \mid i(x) \in (p(x)),\ r(x) \in K[x]\}$. Et $(p(x))$ on maksimaalne ideaal ja $(p(x)) \neq J$, siis $J = K[x] = (1)$. Seega leiduvad polünoomid $i(x) \in (p(x))$ ja $r(x)$ nii, et $i(x) + f(x)r(x) = 1$, siit

$$g(x) = i(x)g(x) + f(x)g(x)r(x) \in (p(x)).$$

Seega sain $f(x) \notin (p(x))$, siis $g(x) \in (p(x))$, millest $(p(x))$ on algideaal, sest $(p(x))$ on mittetriviaalne.

$3 \Rightarrow 1$

Olgu $(p(x))$ algideaal, siis polünoom $p(x) \notin K$, sest muidu oleks tegu triviaalsete ideaalidega. Kui $p(x) = f(x)g(x)$, siis üldsust kitsendamata võib eeldada $f(x) \in (p(x))$, millest $p(x) \mid f(x)$. Et $f(x) \neq 0$, siis $f(x) = \alpha p(x)$ ja $g(x) = \alpha^{-1}$. Seega $p(x)$ on taandumatu.□

3 Lõplikud korpused ja nende lihtlaiendid

Definitsioon 1

Korpuse K laiendiks nimetatakse korpust L, mille alamkorpust L' on isomorfne korpusega K. Laiendit nimetatakse lõplikuks, kui leidub lõplik arv korpuse L elemente $a_1, a_2, \ldots, a_k$ nii, et $L = \left\{ \sum_{i=1}^{k} \lambda_i a_i \mid \lambda_i \in L' \right\}$. Siis nimetatakse L mõõtmeks üle K suurust $[L : K] = k$.

Definitsioon 2

Korpuse K lõplikku laiendit L nimetatakse lihtlaiendiks, kui $L = \{f(c) \mid f \in K[x]\}$, kus c on korpuse L fikseeritud element.

Teoreem 1

Jaagiklassi ringid $\mathbb{Z}_p$ on korpused parajasti siis, kui p on algarv.

Teoreem 2 (Bezout' teoreem)

Kui a on polünoomi $f(x)$ juur (kald)korpuses K, siis tegur $x - a$ jagab polünoomi $f(x)$.

Teoreem 3 (Kroneckeri teoreem)

Kui polünoom $p(x)$ on taandumatu üle korpuse K, siis faktorring $K[x]/(p(x))$ on korpus.

Tõestus

On lihtne veenduda, et tehted

$$(a(x) + I) + (b(x) + I) = (a(x) + b(x)) + I$$

$$(a(x) + I)(b(x) + I) = (a(x)b(x)) + I,$$

kus $I = (p(x))$ on korrektsed. Seega on tegu kommutatiivse ringiga, kus nullelemendiks on $0 + I$ ja ühikelemendiks $1 + I$. Näitan, et iga $f(x) + I \neq 0 + I$ leidub pöördelement. Et $f(x) + I \neq 0 + I$, siis $p(x) \nmid f(x)$. Nüüd $p(x)$ taandumatusest on selge $S\ddot{U}T(f(x), p(x)) = 1$ ja siit omakorda leiduvad polünoomid $u(x)$ ja $v(x)$, nii et $u(x)f(x) + v(x)p(x) = 1$. Vaatlen sama võrdust faktorringis

$$1 + I = (u(x)f(x) + v(x)p(x)) + I = u(x)f(x) + I = (u(x) + I)(f(x) + I).$$

Seega $v(x) + I$ on $f(x) + I$ pöördelement.□

Definitsioon 3

Polünoomi $f(x)$ üle korpuse K lahutuskorpuseks nimetatakse minimaalset (kald)korpust L, milles $f(x)$ lahutub esimese astme teguriteks ja mille alamkorpus L' on isomorfne korpusega K.

Märkus: *Hiljem selgub, et iga korpuse K korral on lahutuskorpus alati korpus, seega on nimetus lahutuskorpus õigustatud.*

Järeldus 3.1

Iga polünoom üle lõpliku korpuse K omab lõplikku lahutuskorpust L, mis on korpuse K lihtlaiend.

Tõestus

Näitan esmalt, et taandumatu polünoom $p(x)$ omab korpuses $K[x]/(p(x))$ juurt x. Olgu $p(x) = \sum_{i=0}^{k} a_i x^i$, siis

$$p(x+I) = \sum_{i=0}^{k} a_i (x+I)^i = \sum_{i=0}^{k} a_i (x^i + I) = \sum_{i=0}^{k} a_i x^i + I = p(x) + I = 0 + I.$$

Seega on $x + I$ tõesti juur. Nüüd vaadeldes üldist juhtu, kui korpuses K on polünoomi $f(x)$ juured $a_1, a_2, \ldots, a_k$, siis polünoom on kujul

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_k) f_1(x)$$

Nüüd kui $f_1(x) \notin K$, siis leidub taandumatu polünoom $p(x)$, mis jagab $f_1(x)$. Nüüd võttes korpuse $L_1 := K[x]/(p(x))$, siis võib polünoomi $f_1(x)$ vaadelda korpuses L_1 ja leida kõik juured $b_1, b_2, \ldots, b_l$, siis omab polünoom kuju

$$f_1(x) = (x - b_1)(x - b_2) \cdots (x - b_l) f_2(x).$$

Kui $f_2(x) \notin L_1$, siis leidub taandumatu tegur $p_1(x)$ ja võib vaadelda korpust $L_2 := L_1[x]/(p_1(x))$ ja jälle on x polünoomi $f_2(x)$ juureks. Analoogselt võib edasi jätkata, protsess on lõplik, sest polünoomil $f(x)$ on ülimalt *deg* $f(x)$ juurt ja iga korpuse laienduse korral leitakse vähemalt üks juur. On ilmne, et viimases laienduses sisaldub korpus K isomorfismi täpsuseni. □

Definitsioon 4

Korpuse K laiendit L nimetatakse algebraliseks, kui leidub polünoom $f(x)$, nii et L on isomorfne korpusega $K[x]/(f(x))$.

Järeldus 3.2

Iga korpuse K lihtlaiend L on algebraline.

Tõestus

Olgu korpus L lihtlaiend üle elemendi c. Lihtlaiendi lõplikusest tulenevalt on elemendi c multiplikatiivne rühm tsükliline. Seega on elemendid $c^0, c, c^2, \ldots, c^k$ rühma moodustajad. On selge, et leidub mitetriviaalne lineaarkombinatsioon

$$\sum_{i=1}^{k+1} \lambda_i c^i = 0, \ \lambda_i \in K.$$

Nüüd vaatlen vähima c astmega lineaarkombinatsiooni, mille kõrgeima astme tegur on 1 ja mille summa $\sum_{i=1}^{l} a_i c^i = 0$. Olgu sellele vastav polünoom $f(x) = \sum_{i=1}^{l} a_i x^i$. Näitan nüüd, et selliseid polünoome on vaid 1. Olgu meil veel üks polünoom $g(x)$, siis teostades jäägiga jagamise saan $g(x) = q(x)f(x) + r(x)$, kus *deg* $r(x) <$ *deg* $f(x)$ või $r(x) = 0$. Et $f(c) = 0$ ja $g(c) = 0$, siis $r(c) = g(c) - q(c)f(c) = 0$, millest $r(x) = 0$ arvestades $f(x)$ minimaalsust. Seega

$f(x) \mid g(x)$. Seega kui $f(c) = g(c) = 0$ ja deg $f(x) = deg\ g(x)$ ja pealiikmete kordajad on võrdsed, siis $f(x) = g(x)$. Vaatlen nüüd sürjektiivse homomorfismi $\varphi : K[x] \to L$, kus $\varphi(g(x)) = g(c)$. Näitan nüüd $Ker\ \varphi = (f(x))$. On ilmne $(f(x)) \subseteq Ker\ \varphi$ teisalt ülaltoodu põhjal on ilmne, et ka vastupidine $Ker\ \varphi \subseteq (f(x))$ kehtib. Seega $Ker\ \varphi = (f(x))$. Nüüd homomorfismi teoremist $L \cong K[x]/(f(x))$.□

Definitsioon 5

Korpuse K lihtlaiendi K[c] unitaarseks e. normeeritud polünoomiks nimetatakse minimaalse astmega polünoomi $f(x)$ mille pealiikme kordaja on 1 ja mille juureks on element c.

Märkus: *Vahel räägitakse ka kopruse K laiendi elemendi α unitaarsest polünoomist, see on minimaalse astmega polünoom $f(x)$, mille juureks on α ja mille pealiikme kordaja on 1. Analoogselt järelduse 3.2 tõestusega saab näidata, et see polünoom $f(x)$ on taandumatu ja jagab kõiki teisi polünoome $g(x)$, mille juureks α on, ja seega on unitaarne polünoom üheselt määratud.*

Järeldus 3.3

Suvalise korpuse K lõpliku laiendi L elemendi α poolt moodustatud ring $K[\alpha] = \{f(c) \mid f(x) \in K[x]\}$ on korpuse K lihtlaiendiks(korpuseks).

Tõestus

Vaatleme sürjektiivset homomorfismi $\varphi : K[x] \to K[\alpha]$, kus $\varphi(f(x)) = f(\alpha)$, siis kujutise tuumaks $Ker\ \varphi$ on unitaarse polünoomi $p(x)$ peaideaal, sest kui $f(\alpha) = 0 \Leftrightarrow p(x) \mid f(x)$. Siit homomorfirmi teoreemist $K[\alpha] \cong K[x]/(p(x))$. Et ring $K[x]/(p(x))$ on $p(x)$ taandumatuse tõttu korpus, siis on $K[\alpha]$ korpuse K lihtlaiend.□

Järeldus 3.4

Kui korpuse K kahe lihtlaiendi K[c] ja K[c] unitaarsed polünoomid on võrdsed, siis $K[c] \cong K[c']$

Tõestus

Et unitaarsed polünoomid on võrdsed, siis $K[c] \cong K[x]/(f(x)) \cong K[c']$.□

Märkus: *Vastupidine järeldus kui $K[c] \cong K[c']$, siis unitaarsed polünoomid on võrdsed pole õige.*

Vaatleme näiteks korpuse $\mathbb{Z}_2$ algebralisi lihtlaiendeid $\mathbb{Z}_2[\alpha]$ ja $\mathbb{Z}_2[\beta]$, kus unitaarsed polünoomid on vastavalt x^3+x^2+1 ja x^3+x+1. On lihtne veenduda et mõlemad polünoomid on taandumatud ja seega on tegu tõesti lihtlaienditega. Teisalt on korpused isomorfsed, sest leidub isomorfism $\varphi : \mathbb{Z}_2[\beta] \to \mathbb{Z}_2[\alpha]$, mis on defineeritud $\varphi(0) = 0,\ \varphi(1) = 1,\ \varphi(\beta) = \alpha+1$ ning ülejäänud osa kujutusest on defineeritud kooskõlas korrutamise ja liitmisega.

x	$\varphi(x)$	x	$\varphi(x)$
0	0	β^3	$\alpha^3+\alpha^2+\alpha+1$
1	1	β^3+1	$\alpha^3+\alpha^2+\alpha$
β	$\alpha+1$	$\beta^3+\beta$	$\alpha^3+\alpha^2$
$\beta+1$	α	$\beta^3+\beta+1$	$\alpha^3+\alpha^2+1$
β^2	α^2+1	$\beta^3+\beta^2$	$\alpha^3+\alpha$
β^2+1	α^2	$\beta^3+\beta^2+1$	$\alpha^3+\alpha+1$
$\beta^2+\beta$	$\alpha^2+\alpha$	$\beta^3+\beta^2+\beta$	α^3+1
$\beta^2+\beta+1$	$\alpha^2+\alpha+1$	$\beta^3+\beta^2+\beta+1$	α^3

□

Teoreem 4 (Lagrange' teoreem)

Igas lõplikus rühma G elemendi g korral $g^{|G|} = 1$

Tõestus

Tõestan järgmise lemma.

Lemma 1

Iga lõpliku rühma G elemendi g järk jagab rühma järku.

Tõestus

Et k G on lõplik. Tähistan elemendi g poolt moodustatud tsüklilist rühma $H = \langle g \rangle$. Siis $ord(g) = |H|$. Nüüd vaatlen hulki $aH := \{ah \mid h \in H\}$. Näitan, et hulgad aH on ekvivalentsi klassid. Olgu $aH \cap bH \neq \emptyset$, siis leidub $c \in aH \cap bH \neq$. Seega $ah_1 = c$, millest arvestades H on alamrühm, siis leidub $h_1^{-1} \in H$, saan $a = ch_1^{-1}$. Siit omakorda $cH \subseteq aH$ ja $aH \subseteq cH$. Analoogselt saab näidata $cH = bH$. Seega sain $aH = bH$. Et iga rühma G element $g \in gH$, siis on tegu ekvivalentsiklassidega. Seega leiduvad elemendid $a_1, a_2, \ldots, a_k$, nii et

$$G = \biguplus_{i=1}^{k} a_i H \Rightarrow ord(G) = \sum_{i=1}^{k} |a_i H|$$

Arvestades nüüd $|a_i H| = |H|$, sest leidub g_i^{-1}, siis $ord(g) \mid ord(G)$.□
Et iga rühma G elemendi g järk jagab $|G|$, siis

$$g^{|G|} = \left(g^{ord(g)}\right)^{\frac{|G|}{ord(g)}} = 1^{\frac{|G|}{ord(g)}} = 1.$$

□

Teoreem 5

Iga lõplik kaldkorpus sisaldab p^n elementi.

Tõestus

Olgu meil kaldkorpus K, vaatleme ühikelemendi aditiivset tsüklilist rühma $H = \langle 1 \rangle$. Eelnevast on teada, et H on p elemendiline alamkorpus, mis on isomorfne $\mathbb{Z}_p$. Nüüd, et korpus on lõplik, siis leidub lõplik moodustajate süsteem $\{a_1, a_2, \ldots, a_k\}$ nii, et iga $k \in K$ korral $k = \sum_{i=1}^{k} \lambda_i a_i$, kus $\lambda_i \in H$. Nüüd on võimalik leida minimaalne moodustajate süsteem $e_1, e_2, \ldots, e_n$. Siis vaadeldes K, kui vektorruumi üle H on $e_1, e_2, \ldots, e_n$ vektoruumi baasiks. Seega $K \cong H^n$ ja siit $|K| = p^n$.□

Teoreem 6 (Polünoomi lahutuskorpuste ühesus)

Iga polünoomil üle korpuse K on isomorfismi täpsuseni üks lahutuskorpus.

Tõestus

Tõestan selle induktsiooniga üle polünoomi astme eeldamata lauhtuskorpustelt kommutatiivsust.

Baas

Kui olgu polünoom $f(x)$ astmega 1 üle korpuse K, siis on polünoomi juur korpuses K ja arvestades lahutuskorpuse minimaalsust on lahutuskorpus $L \cong K$.

Induktsiooni samm

Olgu kõigi polünoomide, mille aste on väiksem kui n lahutuskorpused isomorfismi täpsuseni samad. Vaatlen, nüüd polünoomi $f(x)$, mille aste on n.

Siis mõlemas lahutuskorpuses L ja L' omab polünoomi taandumatu tegur $p(x)$ vähemalt ühte juur, vastavalt a ja a' Nüüd korpuse K kommmutatiivsed lihtlaiendid $K[a]$ ja $K[a']$ on isomorfsed, sest unitaarsed polünoomid on võrdsed. Nüüd võib polünoomi $f(x)$ vaadelda üle korpuse $K_1 \cong K[a]$, siis on polünoomil antud korpuses vähemalt üks juur c ja seega Bezout' teoreemi kohaselt on $f(x) = (x-c)f_1(x)$. Et korpusi L ja L' võib isomorfismi täpsuseni vaadelda korpuse K_1 laienditena, kusjuures mõlemad on võrrandi $f_1(x) = 0$ lahutuskorpuseks, siis induktsiooni eeldusest(K_1 on kommutatiivne) on $f_1(x)$ lahutuskorpused L ja L' üle korpuse K_1 isomorfsed. □

Järeldus 6.1

Polünoomi $f(x)$ üle korpuse K lahutuskorpus on kommutatiivne.

Tõestus

Järelduses 3.1 konstrueeritud lahutuskorpus on konstruktsiooni tõttu kommutatiivne, et kõik teised lahutuskorpused on sellega isomorfsed, siis on lahutuskorpus kommutatiivne. □

Teoreem 7 (Korpuste ühesuse teoreem)

Iga algarvu p ja naturaalarvu n korral leidub isomorfismi täpsuseni üks korpus, milles on p^n elementi.

Tõestus

Vaatlen võrrandi $f(x) = x^{p^n} - x = 0$ (üle korpuse $\mathbb{Z}_p$) lahutuskorpust L. Olgu $S := \{x \in L \mid x^{p^n} - x = 0\}$, siis $|S| = p^n$, sest $f'(x) = p^n x^{p^n-1} - 1 = -1 \neq 0$ ja seega pole võrrandil kordseid juuri. Näitan, et S on alamkorpus. Kui $a, b \in S$, siis $(a+b)^{p^n} = \sum_{i=0}^{p^n} \binom{p^n}{i} a^i b^{p^n-i} = a^{p^n} + b^{p^n}$, sest kui $k \neq 0$ või $k \neq p^n$, siis $p \mid \binom{p^n}{k}$. Siit $(a+b)^{p^n} - (a+b) = (a^{p^n} - a) + (b^{p^n} - b) = 0$, seega $a + b \in S$. Et $(-a)^{p^n} - (-a) = a - (-1)^{p^n} a^{p^n} = a - a^{p^n}$, sest kui $p = 2$, siis $-a = a$, ja kui $p > 2$, siis p^n on paaritu ja $(-1)^{p^n} = -1$, seega sain $-a \in S$. Nüüd $0 = (a^{p^n} - a)(b^{p^n} - b) = ((ab)^{p^n} - ab) - b(a^{p^n} - a) - a(b^{p^n} - b) = ab^{p^n} - ab$, seega $ab \in S$. Nüüd $0 = a^{p^n} - a$, siis $0 = 0a^{-p^n-1} = a^{-1} - a^{-p^n} = -((a^{-1})^{p^n} - a^{-1})$, seega ka $a^{-1} \in S$. Seega olen näidanud, et S on lahutuskorpuse L alamkorpus. Nüüd lahutuskorpuse minimaalsusest $L = S$ ja seega on lahutuskorpuses p^n liiget. Nüüd näitan andud korpuse ühesust. Olgu meil korpus L', milles on p^n elementi, siis iga nullist erineva elemendi multiplikatiivne järk jagab $p^n - 1$ ja seega on iga element võrrandi $x^{p^n} - x = 0$ lahendiks, et ka 0 on võrrandi lahend, siis on L' $x^{p^n} - x = 0$ lahutuskorpus ja siit teoreemi 6 järgi on korpused L ja L'isomorfsed.□

Märkus: *Korpust p^n elemendilist korpust tähistatakse $\mathbb{F}_{p^q}$.*

Järeldus 7.1

Iga lõplik kaldkorpus on korpus.

Tõestus

Olgu meil lõplik p^n elemendiline kaldkorpus K, siis et K^* on rühm, on Lagrange teoreemist selge, et iga $g \in K^*$ korral $g^{p^n-1} - 1 = 0$. Et nullelemendi korral on võrrand $x^{p^n} - x = 0$ triviaalselt täidetud, siis on kõik korpuse K elemendid võrrandi $x^{p^n} - x = 0$ lahendid üle korpuse $\langle 1 \rangle \cong \mathbb{Z}_p$. Et kaldkorpuses on täpselt p^n elementi, siis on korpus minimaalne kaldkorpus, mis sisaldab võrrandi $x^{p^n} - x = 0$ juuri. Seega on kaldkorpus K antud võrrandi lahutuskorpuseks. Et

korpus $\mathbb{Z}_p$ on kommutatiivne, siis korpuste ühesuse teoreemist on kaldkorpus K isomorfne võrrandi lahutuskorpusega L, mis on kommutatiivne ja seega on kaldkorpus K kommutatiivne.□

Järeldus 7.2

Taandumatu k astme polünoomi $p(x)$ üle korpuse $\mathbb{Z}_p$ lahutuskorpus $L \cong \mathbb{F}_{p^k}$.
Tõestus

Vaatleme polünoomi $p(x)$ lahutuskorpuses kahte polünoomi juurt α ja β. Siis on elementide α ja β unitaarseks polünoomiks $\lambda p(x), \lambda \in \mathbb{Z}_p$, sest $p(\alpha) = p(\beta) = 0$ ja $p(x)$ on taandumatu. Seega on lahutuskorpuse elementide poolt moodustatud lihtlaiendid $K[\alpha]$ ja $K[\beta]$ isomorfsed korpusega $\mathbb{F}_{p^k}$, sest korpuses $\mathbb{Z}_p[x]/(p(x))$ on p^k elementi. Siit iga võrrandi p(x) juur on korpuses $\mathbb{F}_{p^k}$ ja lahutuskorpuse minimaalsusest $L \cong \mathbb{F}_{p^k}$. □

4 Lõpliku korpuse multiplikatiivne rühm ja primitiivsed polünoomid

Teoreem 1

Kui kommutatiivses rühmas G on elemendid järkudega n ja n, siis rühmas G leidub element järguga $k = V\ddot{U}K(m,n)$.

Tõestus

Vaatlen, esmalt juhtu, kus $S\ddot{U}T(m,n) = 1$. Olgu elemendid a ja b, nii et $ord(a) = m$ ja $ord(b) = n$. Siis $(ab)^{mn} = a^{mn}b^{mn} = 1$. Teisalt $1 = (ab)^l = a^l b^l$, millest $a^l = b^{-l}$. Seega $a^l = b^{-l} \in \langle b \rangle$, siis $ord(a^l) \mid ord(b)$ ja teisalt $ord(a^l) \mid ord(a)$. Siit arvestades $S\ddot{U}T(m,n) = 1$ on $ord(a^l) = 1$, millest $a^l = 1$. Siit $(ab)^l = 1$, siis $a^l = 1$, millest $m \mid l$ ja analoogselt tõestades $n \mid l$. Siit on selge $ord(ab) = mn$.

Vaatlen üldist juhtu, kus $S\ddot{U}T(m,n) = k$. Olgu elemendid a ja b, nii et $ord(a) = m$ ja $ord(b) = n$. Nüüd vaatlen elementi a^k, siis $ord(a^k) = \frac{m}{k} = m_1$. Siit on selge, et $S\ddot{U}T(m_1,n) = 1$ ja seega leidub element, mille järk on $m_1 n = V\ddot{U}T(m,n)$. □

Teoreem 2

Lõpliku korpuse K multiplikatiivne rühm on tsükliline.

Tõestus

Eelneva teoreemi põhjal leidub rühma K^* element a, mille järku jagavad kõik teised elemendid st. leidub maksimaalse järguga element. Olgu meil multiplikatiivses rühmas n elementi ja olgu a järk m. Siis on võrrandil $x^m - 1 = 0$ kopruses K täpselt n lahendit, sest iga $g \in K^*$ korral $ord(g) \mid m \Rightarrow g^m = 1$. Siit on selge $m \geq n$, teisalt $m \leq n$ ja siit $m = n$. Ühesõnaga a on korpuse tsüklilise rühma moodustaja.□

Järeldus 2.1

Korpus $\mathbb{F}_{p^k}$ on korpuse $\mathbb{F}_{p^n}$ alamkorpus parajasti siis, kui $k \mid n$.

Tõestus

Et korpus $\mathbb{F}_{p^k}$ oleks korpuse $\mathbb{F}_{p^n}$ alamkorpus on tarvilik, et $p^k - 1 \mid p^n - 1$, sest alamkorpuse moodustaja järk peab jagama korpuse moodustaja järku. Kuid see tingimus on ka piisav. Olgu korpuse moodustaja α ja $v(p^k - 1) = p^n - 1$, siis elemendi $\beta = \alpha^v$ järk on $p^k - 1$, sest $1 = \alpha^{p^n - 1} = (\alpha^v)^{p^k - 1}$ ning väiksem järk kui $p^k - 1$ läheks α järguga vastuollu. Nüüd tsüklilises rühma $\langle \beta \rangle$ iga element on võrrandi $x^{p^k} - x = 0$ lahend, sest $\beta^{p^k} = \alpha^{vp^k} = \alpha^v = \beta$. Et võrrandi $x^{p^k} - x = 0$ lahendid on kinnised ka liitmise ja lahutamise suhtes(osa 3 teoreemi 7 tõestus), siis hulk $\langle \beta \rangle \bigcup \{0\}$ on polünoomi $x^{p^k} - x = 0$ lahutuskorpus ja seega isomorfne $\mathbb{F}_{p^k}$.

Näitan $p^k - 1 \mid p^n - 1$ on tarvilik ja piisav $k \mid n$. Piisavus on ilmne, sest $p^n - 1 = (p^k)^l - 1 = (p^k - 1)(1 + p^k + p^{2k} + \cdots + p^{(l-1)k})$. Tarvilikkuse tõestan induktsiooniga n järgi. Kui $n = 1$ on väide triviaalne. Kui väide on õige juhul $n < n_0$, siis $p^{n_0} - 1 = v(p^k - 1)$ järeldub $p^{n_0} = vp^k + (1 - v)$. Siit omakorda $p^k \mid v - 1$, millest $v = p^k v_1 + 1$. Siit saan $p^{n_0 - k} - 1 = v_1(p^k - 1)$ ja siit ind. eeldusest $k \mid n_0 - k$ ja seega $k \mid n_0$.□

Järeldus 2.2

Taandumatu k astme polünoom $p(x)$ jagab polünoomi $x^{p^n} - x$ parajasti siis, kui $k \mid n$.

Tõestus

Et taandumatu polünoomi $p(x)$ lahutuskorpus $L \cong \mathbb{F}_{p^k}$, siis $p(x) \mid x^{p^n} - x$ pajajasti siis, kui $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^n}$. Siit eelneva põhjal $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^n}$ parajasti siis, kui $k \mid n$.□

Definitsioon 1

Lõpliku korpuse primitiivseks elemendiks nimetatakse tsüklilise rühma moodustajaid.

Teoreem 3

Kui f on korpuses $\mathbb{Z}_p$ n astme taandumatu polünoom ja α on polünoomi juureks lahutuskorpuses, siis polünoomi juurteks veel on $\alpha^p, \alpha^{p^2} \dots, \alpha^{p^{n-1}}$.

Tõestus

Olgu polünoom kujul $f(x) = \sum_{i=0}^{n} a_i x^i$, siis

$$0 = f(x)^{p^l} = (\sum_{i=0}^{n} a_i \alpha^i)^{p^l} = \sum_{i_1+i_2+\dots+i_n=p^l} \binom{p^l}{i_1, i_2, \dots i_k} \prod_{j=1}^{n} a_j^{i_j} (\alpha^i)^{i_j}$$

Et $p \mid \binom{p^l}{i_1, i_2, \dots i_k}$, kui ei leidu $i_j = p^l$(siis on multinoomkordaja 1). Seda arvestades:

$$0 = \sum_{l=1}^{n} a_j^{p^l} \alpha^{j p^l} = \sum_{l=1}^{n} a_j \alpha^{p^l j} = f(a^{p^l})$$

Seega arvestades nüüd $ord(\alpha) \mid p^n - 1$, siis pole mõtet lasta l suuremaks kui $n - 1$.□

Definitsioon 2

Taandumatut polünoomi üle $\mathbb{Z}_p$ nimetatakse primitiivseks, kui üks tema juurtest on primitiivne.

Teoreem 4

Primitiivse polünoomi üle Z_p kõik juured on primitiivsed.

Tõestus

Olgu primitiivse polünoomi $f(x)$ astmega n primitiivseks juureks α.Siis eelneva teoreemi 3 põhjal on seda ka $\alpha^p, \alpha^{p^2} \dots, \alpha^{p^{n-1}}$. Et α on primitiivne, siis on ülatoodud juured omavahel erinevad. Seega on kõik juured kujul α^{p^l}. Et tsükliline rühm $\langle \alpha \rangle \cong \mathbb{Z}_{p^n-1}$, siis loomulik isomorfism on $\alpha \leftrightarrow 1$ ja siit $\alpha^{p^l} \leftrightarrow p^l$. Et $S\ddot{U}T(p^l, p^n - 1) = 1$, siis on p^l rühma $\mathbb{Z}_{p^n-1}$ moodustaja ning seega on näidatud, et primitiivse võrrandi iga juur on primitiivne.□

Definitsioon 3

n astme tsüklotoomseks polünoomiks nimetatakse polünoomi $Q_n(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{\varphi(n)})$, kus a_i on primitiivne võrrandi $x^n - 1 = 0$ juur.

Teoreem 5

Tsüklotoomsel n astme poünoomil on järgmised omadused:

1. $Q_n = \prod_{1\leq d\leq n, d\perp n} (x-\alpha^d)$, *kus* α *on primitiivne* n *astme ühejuur;*

2. $x^n - 1 = \prod_{d|n} Q_d$;

3. $Q_n = \prod_{d|n} (x^d-1)^{\mu(\frac{n}{d})}$;

4. *tsüklotoomset polünoomi võib vaadelda kui polünoomi üle iga korpuse* $\mathbb{Z}_p$;

5. $Q_{p^n} = 1 + x^{p^{n-1}} + x^{2p^{n-1}} + \cdots + x^{(p-1)p^{n-1}}$, *kus* $p \in \mathbb{P}$.

Teoreem 6

Taandumatu n *astme polünoom* $f(x)$ *üle* $\mathbb{Z}_p$ *on primitiivne parajasti siis, kui polünoom* $f(x)$ *jagab tsüklotoomset polünoomi* $Q_{p^n-1}(x)$.
Tõestus

Tarvilikkus

Olgu $f(x)$ n astme primitiivne polünoom, siis polünoomi juure α järk on p^n-1, seega $\alpha^{p^n-1} = 1$, siit kõik α astmed on juurteks võrrandile $x^{p^n} - 1 = 0$ ja seega on α primitiivne $p^n - 1$ ühejuur. Teoreemist 4 on selge, et ka võrrandi ülejäänud juurte järk on $p^n - 1$ ja seega on nad primitiivsed ühejuured. Seega vastavalt tsüklotoomse polünoomi definitsioonile $f(x) \mid Q_{p^n-1}(x)$ võrrandi $f(x)$ lahutuskorpuses. Et mõlemad polünoomid on ka polünoomid üle $\mathbb{Z}_p$, siis toimub jagumine ka selles korpuses.
Piisavus

Jagagu n astme polünoom $f(x)$ tsüklotoomset polünoomi $Q_{p^n-1}(x)$, siis iga polünoomi $f(x)$ lahutuskorpus on (alam)korpuseks tsüklotoomse polünoomi lahutuskorpusele. Polünoomi $f(x)$ juur α on võrrandi $x^{p^n-1} - 1 = 0$ primitiivne juur ja seega juure järk on $p^n - 1$. Siit on selge, et α on polünoomi $f(x)$ lahutuskorpuse primitiivne element, sest $f(x)$ lahutuskorpuses on elemente ülimalt p^n. Näitan veel, et $f(x)$ on on taandumatu polünoom. Olgu $f(x)$ taandumatu tegur $g(x)$, mille juureks on β. Siis, juure primitiivsusest ja teoreemist kolm saan, et polünoomi $g(x)$ erinevateks juurteks on $\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}$. Siit $deg\ g(x) = n$, seega on $f(x)$ taandumatu ja primitiivne.□

Märkus: *On olemas taandumatuid polünoome, mille juured pole primitiivsed.*

Vaatleme näiteks polünoomi $x^4 + x^3 + x^2 + x + 1$ üle korpuse $\mathbb{Z}_2$. Siis tsüklotoomne polünoom Q_{15} on kujul

$$Q_{15} = \frac{(x-1)(x^{15}-1)}{(x^3-1)(x^5-1)} = x^8+x^7+x^5+x^4+x^3+x+1 = (x^4+x+1)(x^4+x^3+1)$$

Polünoom $x^4 + x^3 + x^2 + x + 1$ on taandumatu, sest ta ei jagu taandumatute polünoomidega x, $x-1$ ja x^2+x+1. Nüüd on selge, et polünoom $x^4+x^3+x^2+x+1$ ei jaga tsüklotoomset polünoomi ja seega pole polünoom primitiivne. Näiteks primitiivse polünoomi $x^4 + x + 1$ lahutuskorpuses $\mathbb{Z}_2[\alpha]$ on polünoomi juurteks $\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$, mis pole tõesti korpuse primitiivsed elemendid, sest nende järk on 5.□