802656S ALGEBRALLISET LUVUT OSA I
ALGEBRAIC NUMBERS PART I

Tapani Matala-aho
MATEMATIIKKA/LUTK/OULUN YLIOPISTO

KEVÄT 2020

Algebrallisten lukujen teoria on kiinteä osa matematiikan lukuteoriaa.

Aluksi kerrataan renkaiden ja kuntien perusteita, joista edetään kuntalaajennuksiin. Erityiseen tarkasteluun otetaan jaollisuus kokonaisalueessa, jonka sovelluksiin törmätään polynomialgebrassa ja kokonaisten algebrallisten lukujen teoriassa.
Algebrallisten lukujen teoria lepää vahvasti polynomialgebraan, josta käsitellään polynomien nollakohtia ja jaollisuutta.
Algebrallisen luvun määritelmä yleistetään kuntalaajennuksien algebrallisiin alkioihin, joista edetään algebrallisiin kuntiin. Tärkeinpinä algebrallisina kuntina saadaan lukukunnat, jotka ovat äärellisesti generoituja kompleksisten algebrallisten lukujen kunnan A alikuntia. Erityisesti tutkitaan neliökuntia.
Edelleen tarkastellaan kokonaisten algebrallisten lukujen jaollisuutta ja tekijöihinjakoa, joita sovelletaan Diofantoksen yhtälöiden ratkaisemiseen.

First we revise some basics of rings and fields which are needed to proceed ahead field extensions. In particular, divisibility in an integral domain is carefully studied yielding to applications in the theory of polynomial algebra and algebraic integers. The theory of algebraic numbers is strongly based on polynomial algebra, where the properties of zeros and divisibility of polynomials are considered. The definition of an algebraic number will be generalized to the algebraic elements of field extensions going forward to algebraic fields.Considered as most important algebraic fields we get number fields which are finitely generated subfields of the field A of all complex algebraic numbers. In particular, we study quadratic number fields.
Further, we shall consider the divisibility and factorization of algebraic integers with some applications to Diophantine equations.

Esitiedot:
Algebran ja Lineaarialgebran aineopintokurssit sekä Lukuteorian perusteet.
Kurssilla käytetään Lukuteorian perusteet kurssin merkintöjä.
Notations and basics of Number Theory from the course: Basics of Number Theory.

I.N. Stewart and D.O. Tall: Algebraic number theory.
Daniel Marcus: Number fields.
J.B. Fraleigh: Abstract algebra.
Michael Artin: Algebra.
Number Theory Web/LINK
American Mathematical Monthly/LINK

Määritelmä 1

Algebralliset luvut saadaan rationaalikertoimisten ei-vakiopolynomien nollakohtina./ Algebraic numbers are zeros of non-constant polynomials with rational coefficients.

Esimerkki 1

Luvut/Numbers

$$-1; \tag{2.1}$$

$$i; \tag{2.2}$$

$$2^{1/3} + 3^{1/2} \tag{2.3}$$

ovat algebrallisia lukuja/are algebraic numbers.

Esimerkki 2

$$e^{i\pi/m}, \quad m \in \mathbb{Z} \setminus \{0\}; \tag{2.4}$$

$$\sin(\pi/m),\ \cos(\pi/m),\ \tan(\pi/m), \quad m \in \mathbb{Z} \setminus \{0\}; \tag{2.5}$$

ovat algebrallisia lukuja.

Esimerkki 3

Myös polynomiyhtälön/Also roots of the polynomial equation

$$2^{1/3}x^4 + 3^{1/2}x + 1 = 0 \tag{2.6}$$

juuret ovat algebrallisia lukuja/are algebraic numbers.

Merkintä 1

Olkoon $f : A \to B$ *ja* $C \subseteq B$. *Tällöin joukon* C *alkukuva/pre-image on joukko*

$$f^{-1}(C) = \{x \in A | \ f(x) \in C\}. \tag{2.7}$$

Erityisesti

$$f^{-1}(\{0\}) = \{x \in A | \ f(x) = 0\}. \tag{2.8}$$

Gauss todisti, että kompleksikertoimisella ei-vakiopolynomilla on aina asteen verran kompleksisia nollakohtia.

Lause 1

ALGEBRAN PERUSLAUSE/FUNDAMENTAL THEOREM OF ALGEBRA.
Olkoon/Let $d = \deg p(x) \in \mathbb{Z}^+$ *ja*

$$p(x) = p_0 + p_1 x + \ldots + p_d x^d \ \in \mathbb{C}[x], \tag{2.9}$$

tällöin/then

$$\#p^{-1}(\{0\}) = \deg p(x) = d \tag{2.10}$$

eli/or

$$p(x) = p_d(x - \alpha_1)\cdots(x - \alpha_d), \quad \alpha_1, \ldots, \alpha_d \ \in \mathbb{C}. \tag{2.11}$$

Tällä kurssilla keskitytäänkin kompleksisiin algebrallisiin lukuihin/complex algebraic numbers.

Olkoon K kunta/field ja $d \in \mathbb{Z}^+$. Polynomi

$$p(x) = p_0 + p_1 x + \ldots + x^d \ \in K[x], \quad d = \deg p(x) \geq 1, \tag{3.1}$$

on pääpolynomi/monic polynomial. Käytetään astetta d olevien pääpolynomien joukolle merkintää

$$K[x]_d = \{p(x) = p_0 + p_1 x + \ldots + x^d \ \in K[x]\}. \tag{3.2}$$

Määritellään (kompleksiset) algebralliset luvut rationaalilukujen kunnan suhteen.

Määritelmä 2

Joukko

$$\mathbb{A}_d = \{\alpha \ \in \mathbb{C} |\ p(\alpha) = 0,\ p(x) \in \mathbb{Q}[x]_d\} \tag{3.3}$$

on korkeintaan astetta d olevien algebrallisten lukujen joukko. Edelleen

$$\mathbb{A} = \cup_{d=1}^{\infty} \mathbb{A}_d \tag{3.4}$$

on kaikkien (kompleksisten) algebrallisten lukujen joukko.

Määritelmä 3

Olkoon $K \subseteq \mathbb{C}$ *ja* $p(x) \in K[x]$. *Tällöin*

$$Z(p) = p^{-1}(\{0\}) = \{\alpha \in \mathbb{C} | \ p(\alpha) = 0\} \tag{3.5}$$

on polynomin $p(x)$ *nollajoukko/zero set.*

Lause 2

$$\mathbb{A}_1 = \mathbb{Q}. \tag{3.6}$$

Todistus.

Merkintä 2

Olkoon $D \in \mathbb{Z}$. Tällöin

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} |\ a, b \in \mathbb{Q}\}. \tag{3.7}$$

Lause 3

$$\mathbb{A}_2 = \bigcup_{D \in \mathbb{Z}} \mathbb{Q}(\sqrt{D}). \tag{3.8}$$

Todistus.

Tällä kurssilla tarkastellaan ykkösellisiä kommutatiivisia renkaita.
Olkoon R joukko, jossa on ainakin kaksi alkiota, $\#R \geq 2$. Oletetaan, että joukossa R on määritelty laskutoimitus/binary operation $+$ eli kuvaus/or mapping

$$+ : R \times R \to R, \quad (a, b) \to a + b,$$

missä $a + b \in R$, kun $a \in R$ ja $b \in R$ sekä

Tällä kurssilla tarkastellaan ykkösellisiä kommutatiivisia renkaita.
Olkoon R joukko, jossa on ainakin kaksi alkiota, $\#R \geq 2$. Oletetaan, että joukossa R on määritelty laskutoimitus/binary operation $+$ eli kuvaus/or mapping

$$+ : R \times R \to R, \quad (a, b) \to a + b,$$

missä $a + b \in R$, kun $a \in R$ ja $b \in R$ sekä

laskutoimitus $*$ eli kuvaus

$$* : R \times R \to R, \quad (a, b) \to a * b,$$

missä $a * b \in R$, kun $a \in R$ ja $b \in R$.

Commutative ring with unity

Määritelmä 4

Kolmikko $(R, +, *)$ on ykkösellinen kommutatiivinen rengas/a commutative ring with unity , jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

Commutative ring with unity

Määritelmä 4

Kolmikko $(R, +, *)$ on ykkösellinen kommutatiivinen rengas/a commutative ring with unity , jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun/Addition aksiomit:

Commutative ring with unity

Määritelmä 4

Kolmikko $(R, +, *)$ on ykkösellinen kommutatiivinen rengas/a commutative ring with unity , jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun/Addition aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in R$ (liitännäisyys/associativity).

Commutative ring with unity

Määritelmä 4

Kolmikko $(R, +, *)$ on ykkösellinen kommutatiivinen rengas/a commutative ring with unity , jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun/Addition aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in R$ (liitännäisyys/associativity).

(b) $a + b = b + a$ kaikilla $a, b \in R$ (vaihdannaisuus/commutativity).

Commutative ring with unity

Määritelmä 4

Kolmikko $(R, +, *)$ on ykkösellinen kommutatiivinen rengas/a commutative ring with unity , jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun/Addition aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in R$ (liitännäisyys/associativity).

(b) $a + b = b + a$ kaikilla $a, b \in R$ (vaihdannaisuus/commutativity).

(c) On olemassa nolla-alkio/zero-element $0 \in R$, jolle $0 + a = a$ kaikilla $a \in R$.

Commutative ring with unity

Määritelmä 4

Kolmikko $(R, +, *)$ on ykkösellinen kommutatiivinen rengas/a commutative ring with unity , jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun/Addition aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in R$ (liitännäisyys/associativity).

(b) $a + b = b + a$ kaikilla $a, b \in R$ (vaihdannaisuus/commutativity).

(c) On olemassa nolla-alkio/zero-element $0 \in R$, jolle $0 + a = a$ kaikilla $a \in R$.

(d) Kaikilla $a \in R$ on olemassa vasta-alkio/inverse $-a \in R$, jolle $a + (-a) = 0$.

Ykkösellinen kommutatiivinen rengas

2. Kertolaskun aksiomit:

Ykkösellinen kommutatiivinen rengas

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in R$ (liitännäisyys).

Ykkösellinen kommutatiivinen rengas

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in R$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in R$ (vaihdannaisuus).

Ykkösellinen kommutatiivinen rengas

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in R$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in R$ (vaihdannaisuus).

(c) On olemassa ykkösalkio/unit-element $1 \in R$, jolle $1 * a = a$ kaikilla $a \in K$.

Ykkösellinen kommutatiivinen rengas

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in R$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in R$ (vaihdannaisuus).

(c) On olemassa ykkösalkio/unit-element $1 \in R$, jolle $1 * a = a$ kaikilla $a \in K$.

3. Osittelulaki/distribution law:

Ykkösellinen kommutatiivinen rengas

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in R$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in R$ (vaihdannaisuus).

(c) On olemassa ykkösalkio/unit-element $1 \in R$, jolle $1 * a = a$ kaikilla $a \in K$.

3. Osittelulaki/distribution law:

(a) $a * (b + c) = a * b + a * c$ kaikilla $a, b, c \in R$.

Määritelmän 4 mukaista joukkoa R kutsutaan ykköselliseksi kommutatiiviseksi renkaaksi

Määritelmän 4 mukaista joukkoa R kutsutaan ykköselliseksi kommutatiiviseksi renkaaksi
ja annettuja ehtoja sanotaan rengas-aksiomeiksi/ring-axioms.

Määritelmän 4 mukaista joukkoa R kutsutaan ykköselliseksi kommutatiiviseksi renkaaksi
ja annettuja ehtoja sanotaan rengas-aksiomeiksi/ring-axioms.

Aksiomit 1a–d sanovat, että $(R, +)$ on Abelin ryhmä/Abelian group, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.

Määritelmän 4 mukaista joukkoa R kutsutaan ykköselliseksi kommutatiiviseksi renkaaksi
ja annettuja ehtoja sanotaan rengas-aksiomeiksi/ring-axioms.

Aksiomit 1a–d sanovat, että $(R, +)$ on Abelin ryhmä/Abelian group, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.
Voidaankin sanoa, että $(R, +)$ on renkaan R yhteenlaskuryhmä, jonka neutraalialkio on nolla-alkio 0.

Määritelmän 4 mukaista joukkoa R kutsutaan ykköselliseksi kommutatiiviseksi renkaaksi
ja annettuja ehtoja sanotaan rengas-aksiomeiksi/ring-axioms.

Aksiomit 1a–d sanovat, että $(R, +)$ on Abelin ryhmä/Abelian group, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.
Voidaankin sanoa, että $(R, +)$ on renkaan R yhteenlaskuryhmä, jonka neutraalialkio on nolla-alkio 0.

Mutta $R = (R, *)$ EI/NOT ole kertolaskun $*$ suhteen (välttämättä/necessarily) ryhmä/group.

Määritelmän 4 mukaista joukkoa R kutsutaan ykköselliseksi kommutatiiviseksi renkaaksi
ja annettuja ehtoja sanotaan rengas-aksiomeiksi/ring-axioms.

Aksiomit 1a–d sanovat, että $(R, +)$ on Abelin ryhmä/Abelian group, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.
Voidaankin sanoa, että $(R, +)$ on renkaan R yhteenlaskuryhmä, jonka neutraalialkio on nolla-alkio 0.

Mutta $R = (R, *)$ EI/NOT ole kertolaskun $*$ suhteen (välttämättä/necessarily) ryhmä/group. Kertolaskun neutraalialkio on ykkös-alkio 1.

Merkintä 3

Yleensä kertolasku $*$ jätetään merkitsemättä eli tehdään samaistus:

$$a * b = ab.$$

Määritelmä 5

Olkoon R ykkösellinen rengas. Joukko

$$R^* = \{\textit{yksiköt}\} = \{u \in R \mid \exists\ u^{-1} \in R :\ uu^{-1} = 1\} \tag{4.1}$$

on renkaan R yksikköryhmä (unit group).

Usein käytetään esitystä

$$R^* = \{u \in R \mid \exists\ v \in R :\ uv = 1\}, \tag{4.2}$$

jolloin pätee

$$u \in R^* \quad \Rightarrow \quad 1 = uv, \quad u, v \in R^*. \tag{4.3}$$

Jos $R = K$ kunta/field, niin $K^* = K \backslash \{0\}$.

Määritelmä 6

Renkaan R alkio $a \neq 0$ on nollantekijä (zero divisor), jos $\exists\ b \in R \backslash \{0\}$ s.e. $ab = 0$ tai $ba = 0$.

Määritelmä 7

Kommutatiivinen ykkösellinen rengas D on kokonaisalue/integral domain, mikäli D:ssä ei ole nollantekijöitä eli ehdosta $ab = 0,\ a, b \in D$ aina seuraa $a = 0$ tai $b = 0$.

Määritelmä 8

Kolmikko $(K, +, *)$ on kunta, jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

Määritelmä 8

Kolmikko $(K, +, *)$ on kunta, jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun aksiomit:

Määritelmä 8

Kolmikko $(K, +, *)$ on kunta, jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in K$ (liitännäisyys).

Määritelmä 8

Kolmikko $(K, +, *)$ on kunta, jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a + b = b + a$ kaikilla $a, b \in K$ (vaihdannaisuus).

Määritelmä 8

Kolmikko $(K, +, *)$ on kunta, jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a + b = b + a$ kaikilla $a, b \in K$ (vaihdannaisuus).

(c) On olemassa nolla-alkio $0 \in K$, jolle $0 + a = a$ kaikilla $a \in K$.

Määritelmä 8

Kolmikko $(K, +, *)$ on kunta, jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun aksiomit:

(a) $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a + b = b + a$ kaikilla $a, b \in K$ (vaihdannaisuus).

(c) On olemassa nolla-alkio $0 \in K$, jolle $0 + a = a$ kaikilla $a \in K$.

(d) Kaikilla $a \in K$ on olemassa vasta-alkio $-a \in K$, jolle $a + (-a) = 0$.

2. Kertolaskun aksiomit:

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in K$ (liitännäisyys).

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in K$ (vaihdannaisuus).

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in K$ (vaihdannaisuus).

(c) On olemassa ykkösalkio $1 \in K$, jolle
$1 * a = a$ kaikilla $a \in K$.

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in K$ (vaihdannaisuus).

(c) On olemassa ykkösalkio $1 \in K$, jolle
$1 * a = a$ kaikilla $a \in K$.

(d) Kaikilla $a \in K^* = K \setminus \{0\}$ on olemassa käänteisalkio $a^{-1} \in K^*$, jolle
$a * a^{-1} = 1$.

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in K$ (vaihdannaisuus).

(c) On olemassa ykkösalkio $1 \in K$, jolle $1 * a = a$ kaikilla $a \in K$.

(d) Kaikilla $a \in K^* = K \setminus \{0\}$ on olemassa käänteisalkio $a^{-1} \in K^*$, jolle $a * a^{-1} = 1$.

3. Osittelulaki:

2. Kertolaskun aksiomit:

(a) $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in K$ (liitännäisyys).

(b) $a * b = b * a$ kaikilla $a, b \in K$ (vaihdannaisuus).

(c) On olemassa ykkösalkio $1 \in K$, jolle $1 * a = a$ kaikilla $a \in K$.

(d) Kaikilla $a \in K^* = K \setminus \{0\}$ on olemassa käänteisalkio $a^{-1} \in K^*$, jolle $a * a^{-1} = 1$.

3. Osittelulaki:

(a) $a * (b + c) = a * b + a * c$ kaikilla $a, b, c \in K$.

Määritelmän 8 mukaista joukkoa K kutsutaan kunnaksi

Määritelmän 8 mukaista joukkoa K kutsutaan kunnaksi ja annettuja ehtoja sanotaan kunta-aksiomeiksi.

Määritelmän 8 mukaista joukkoa K kutsutaan kunnaksi ja annettuja ehtoja sanotaan kunta-aksiomeiksi.

Aksiomit 1a–d sanovat, että $(K, +)$ on Abelin ryhmä, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.

Määritelmän 8 mukaista joukkoa K kutsutaan kunnaksi
ja annettuja ehtoja sanotaan kunta-aksiomeiksi.

Aksiomit 1a–d sanovat, että $(K, +)$ on Abelin ryhmä, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.
Voidaankin sanoa, että $(K, +)$ on kunnan K yhteenlaskuryhmä, jonka neutraalialkio on nolla-alkio 0.

Määritelmän 8 mukaista joukkoa K kutsutaan kunnaksi
ja annettuja ehtoja sanotaan kunta-aksiomeiksi.

Aksiomit 1a–d sanovat, että $(K, +)$ on Abelin ryhmä, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.
Voidaankin sanoa, että $(K, +)$ on kunnan K yhteenlaskuryhmä, jonka neutraalialkio on nolla-alkio 0.

Edelleen, aksiomit 2a–d sanovat, että $(K^*, *)$ on Abelin ryhmä, jonka laskutoimitusta $*$ kutsutaan kertolaskuksi.

Määritelmän 8 mukaista joukkoa K kutsutaan kunnaksi
ja annettuja ehtoja sanotaan kunta-aksiomeiksi.

Aksiomit 1a–d sanovat, että $(K, +)$ on Abelin ryhmä, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.
Voidaankin sanoa, että $(K, +)$ on kunnan K yhteenlaskuryhmä, jonka neutraalialkio on nolla-alkio 0.

Edelleen, aksiomit 2a–d sanovat, että $(K^*, *)$ on Abelin ryhmä, jonka laskutoimitusta $*$ kutsutaan kertolaskuksi.
Sanotaan siis, että $(K^*, *)$ on kunnan K kertolaskuryhmä, jonka neutraalialkio on ykkös-alkio 1.

LYHYESTI: Kolmikko $(K, +, \cdot)$, $\#K \geq 2$ on *kunta*, jos:

1. $(K, +)$ on Abelin ryhmä (additiivinen ryhmä),
2. $(K^*, *)$ on Abelin ryhmä (multiplikatiivinen ryhmä), $K^* = K \backslash \{0\}$.
3. $a(b + c) = ab + ac, \ \forall a, b, c \in K$.

Erityisesti, kunta on kommutatiivinen ykkösellinen rengas.
Edelleen kunnassa on aina vähintään kaksi alkiota, nimittäin $0, 1 \in K$, $0 \neq 1$.

Esimerkki 4

Field K is an integral domain.
Proof: Let

$$ab = 0, \tag{4.4}$$

where $a, b \in K$. Antithesis: $a \neq 0$ and $b \neq 0$.
Because K is a field, then $a^{-1} \in K$. Multiplying (4.4) by a^{-1} gives

$$a^{-1}ab = a^{-1} \cdot 0 \quad \Rightarrow \quad b = 0. \tag{4.5}$$

A contradiction. □

Esimerkki 5

The fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$, where $p \in \mathbb{P}$, are integral domains.

Esimerkki 6

Any subring S of a field K is an integral domain.

Esimerkki 7

$\mathbb{Z}$ is an integral domain.

Esimerkki 8

The set

$$\mathbb{Z}[i] = \{a + ib |\ a, b \in \mathbb{Z}\} \tag{4.6}$$

of Gaussian integers is an integral domain and its unit group is

$$\mathbb{Z}[i]^* = \{1, i, -1, -i\}. \tag{4.7}$$

Esimerkki 9

The set

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} |\ a, b \in \mathbb{Z}\} \tag{4.8}$$

is an integral domain and its unit group is

$$\mathbb{Z}[\sqrt{-5}]^* = \{1, -1\}. \tag{4.9}$$

Karakteristika

Määritelmä 9

Kunnan K karakteristika

$$\mathit{char}\ K = \begin{cases} p \Leftrightarrow \exists\ p \in \mathbb{P} :\ \ p1 = 0; \\ 0 \Leftrightarrow \nexists\ n \in \mathbb{Z}^+ :\ \ n1 = 0. \end{cases}$$

Olkoon D kokonaisalue/Let D be an integral domain.

Määritelmä 10

Olkoot $a, b \in D$. Tällöin

$$b|a \quad \Leftrightarrow \quad \exists c \in D: \quad a = bc. \tag{5.1}$$

Kun $b|a$, niin b jakaa (divides) a:n eli b on a:n tekijä (factor).

Merkitään: $b \nmid a$, kun b ei jaa a:ta.

Esimerkki 10

$$0|0, \quad 0 \nmid a \neq 0. \tag{5.2}$$

Merkintä 4

Olkoot $d, b \in D$ ja $s \in \mathbb{N}$, tällöin

$$d^s || b \;\Leftrightarrow\; d^s | b \text{ ja } d^{s+1} \nmid b. \tag{5.3}$$

Lemma 1

Olkoot $a, b, c \in D, a \neq 0$. Tällöin

$$ab = ac \quad \Rightarrow \quad b = c. \tag{5.4}$$

Todistus.

$$ab = ac \quad \Rightarrow \quad a(b-c) = 0,\ a \neq 0, \quad \Rightarrow \quad b - c = 0. \quad \square \tag{5.5}$$

Määritelmä 11

Alkiot $a, b \in D$ ovat liitännäisiä (associates) eli

$$a \sim b \quad \Leftrightarrow \quad \exists \quad u \in D^* : \; b = ua. \tag{5.6}$$

Lemma 2

Relaatio $\sim$ on ekvivalenssirelaatio eli

$$a \sim a; \tag{5.7}$$

$$a \sim b \quad \Leftrightarrow \quad b \sim a; \tag{5.8}$$

$$a \sim b, \quad b \sim c \quad \Rightarrow \quad a \sim c. \tag{5.9}$$

Todistus. 5.8:

$$a \sim b \quad \Leftrightarrow \quad b = ua,\ u \in D^* \quad \Leftrightarrow$$
$$\exists \quad v \in D^* :\ uv = 1,\ b = ua \quad \Leftrightarrow \quad vb = vua = a$$
$$\Leftrightarrow \quad a = vb,\ v \in D^* \quad \Leftrightarrow \quad b \sim a. \quad \square \qquad (5.10)$$

Muut kohdat laskareissa.

Merkintä 5

Alkion $a \in D$ määräämä ekvivalenssiluokka on

$$[a] = \{b \in D |\ b \sim a\}, \qquad (5.11)$$

missä a on luokan $[a]$ edustaja.

Lemma 3

Olkoon D kokonaisalue ja $1, a, b \in D$. Tällöin

$$a \sim b \quad \Rightarrow \quad a|b; \tag{5.12}$$

$$a \sim 1 \quad \Leftrightarrow \quad a|1 \quad \Leftrightarrow \quad a \in D^*; \tag{5.13}$$

$$[1] = D^*; \tag{5.14}$$

$$[a] = aD^*; \tag{5.15}$$

$$a \sim b \quad \Leftrightarrow \quad a|b \quad ja \quad b|a. \tag{5.16}$$

Todistus. 5.13: Oletus $a \in D$.

$$a \sim 1 \quad \Rightarrow \quad 1 = ua,\ u \in D^* \subseteq D \quad \Rightarrow \quad a|1;$$
$$a|1 \quad \Rightarrow \quad \exists\, c \in D:\ 1 = ca \quad \Rightarrow\ c \in D^* \ \Rightarrow\ a \sim 1.$$
$$\rightsquigarrow \qquad a \sim 1 \quad \Leftrightarrow \quad a|1. \qquad \square$$

$$a|1 \quad \Rightarrow \quad \exists\, c \in D:\ 1 = ca \quad \Rightarrow \quad a, c \in D^*;$$
$$a \in D^* \quad \Rightarrow \quad 1 = ua, u \in D \quad \Rightarrow \quad a|1.$$
$$\rightsquigarrow \qquad a|1 \quad \Leftrightarrow \quad a \in D^*. \qquad \square$$

5.14:

$$b \in [1] \quad \Leftrightarrow \quad b \sim 1 \quad \Leftrightarrow \quad b \in D^*. \qquad \square$$

5.15:

$$x \in [a] \quad \Leftrightarrow \quad x \sim a \quad \Leftrightarrow \quad a \sim x$$
$$\Leftrightarrow \quad x = ua,\ u \in D^* \quad \Leftrightarrow \quad x \in aD^*. \qquad \square$$

5.16: Tarkastele ensin tapaus $b = 0$, jolloin myös $a = 0$.

$$a \sim b \quad \Leftrightarrow \quad b \sim a, \quad \Rightarrow \quad a|b \quad \text{ja} \quad b|a;$$
$$a|b \quad \text{ja} \quad b|a \quad \Rightarrow \quad b = ca,\ a = db,\ c, d \in D,$$
$$\Rightarrow \quad b = cdb \quad \Rightarrow \quad cd = 1 \quad \Rightarrow \quad c, d \in D^*,$$
$$\Rightarrow \quad a \sim b \quad \text{ja} \quad b \sim a. \quad \square$$

Huomautus 1

Olkoon $b \in D$. Tällöin

$$b = 1 \cdot b = u(u^{-1}b) \quad \forall\ u \in D^*. \tag{5.17}$$

Siten yksiköt ja alkion liitännäiset ovat aina tekijöinä.

Esimerkki 11

Remember that the unit group of Gaussian integers was

$$\mathbb{Z}[i]^* = \{1, i, -1, -i\}. \tag{5.18}$$

Thus

$$2 - i \sim 1 + 2i \sim -2 + i \sim -1 - 2i \tag{5.19}$$

and the equivalence class

$$[2 - i] = \{2 - i, 1 + 2i, -2 + i, -1 - 2i\} \tag{5.20}$$

of $2 - i$ consists of four elements.

Määritelmä 12

Alkion $b \in D$ triviaalit tekijät/trivial factors q ovat kaikki/are all yksiköt/units ja liittännäiset/associates eli alkiot

$$q \in [1] \quad ja \quad q \in [b]. \tag{5.21}$$

Alkio $j \in D, j \neq 0, j \notin D^*$ on jaoton/irreducible, mikäli sillä on vain triviaaleja tekijöitä eli

$$q|j \quad \Leftrightarrow \quad q \in [1] \quad tai \quad q \in [j]. \tag{5.22}$$

Alkio $p \in D, p \neq 0, p \notin D^*$ on alkualkio/prime, mikäli

$$p|ab \quad \Rightarrow \quad p|a \quad tai \quad p|b \quad \forall a, b \in D. \tag{5.23}$$

Alkio $a \in D, a \notin D^*$ jakaantuu/is reducible, mikäli sillä on aito tekijä $d \in D$ eli

$$\exists\, d \in D: \quad d|a \quad \Rightarrow \quad d \notin [1] \quad ja \quad d \notin [a]. \tag{5.24}$$

Huomautus 2

Nolla-alkio jakaantuu/zero-element is reducible.

Merkintä 6

Asetetaan

$$J_D = \{j \in D | \ j \text{ on jaoton}\} \tag{5.25}$$

ja

$$P_D = \{p \in D | \ p \text{ on alkualkio}\}. \tag{5.26}$$

Lemma 4

Olkoot $a, b \in D$ ja $j, h \in J_D$. Tällöin

$$j = ab \quad \Rightarrow \quad a \sim 1 \quad tai \quad b \sim 1. \tag{5.27}$$

$$j = bh, \quad \Rightarrow \quad b \sim 1. \tag{5.28}$$

Todistus (5.27). Antithesis: $a \not\sim 1$ and $b \not\sim 1$

$$\Rightarrow \quad a, b \notin [1] \quad \Rightarrow \quad a, b \in [j] \tag{5.29}$$

because j is irreducible. Thus

$$a = d_1 j \quad b = d_2 j, \quad d_1, d_2 \in D^* \quad \Rightarrow \tag{5.30}$$

$$j = ab = d_1 d_2 j^2 \quad \Rightarrow \quad 1 = d_1 d_2 j \quad \Rightarrow \quad j \in D^* = [1]. \tag{5.31}$$

A contradiction. □

Määritelmä 13

Olkoot $a, b \in D$ annettu/be given. Tällöin alkio $d \in D$ on alkioiden a ja b suurin yhteinen tekijä (greatest common divisor) eli
$d = syt(a, b) = gcd(a, b) = (a, b)$ mikäli

$$d|a \quad ja \quad d|b; \tag{5.32}$$

$$c|a \quad ja \quad c|b \quad \Rightarrow \quad c|d. \tag{5.33}$$

Jos $(a, b) \sim 1$, niin sanotaan, että a ja b ovat keskenään jaottomia (relatively prime) ja merkitään $(a, b) = 1$ tai $a \perp b$.

Määritelmä 14

Olkoot $a, b \in D$ annettu. Tällöin alkio $f \in D$ on alkioiden a ja b pienin yhteinen jaettava (least common multiple) eli
$f = pyj[a, b] = lcm[a, b] = [a, b]$ mikäli

$$a|f \quad ja \quad b|f; \tag{5.34}$$

$$a|g \quad ja \quad b|g \quad \Rightarrow \quad f|g. \tag{5.35}$$

Esimerkki 12

$$(0, 0) = 0, \quad [0, 0] = 0. \tag{5.36}$$

Lemma 5

Olkoot $a \in D$ ja $j \in J_D$. Tällöin

$$j \not| a \quad \Rightarrow \quad (a, j) = 1. \tag{5.37}$$

Todistus. Antithesis: $(a, j) \neq 1$. Therefore $(a, j) = d \not\sim 1$ and

$$d|a \quad \text{and} \quad d|j, \quad j \in J_D. \tag{5.38}$$

Because j is irreducible, then $d \sim 1$ or $d \sim j$, hence $d \sim j$. Consequently

$$d = vj, \ v \in D^* \quad \text{and} \quad a = cd = cvj \quad \Rightarrow \quad j|a. \tag{5.39}$$

A contradiction. □

Määritelmä 15

Alkion $a \in D$ esitys jaottomien alkioiden tulona on yksikäsitteinen, jos ehdosta/ The representation of the element $a \in D$ by irreducible elements is unique, if from the condition

$$a = j_1 \cdots j_r = h_1 \cdots h_s, \quad j_l, h_k \in J_D \tag{5.40}$$

seuraa/follows

$$r = s \quad ja \quad h_k \sim j_l \quad \forall k = 1, ..., r \quad jollakin\ l = 1, ..., r. \tag{5.41}$$

Määritelmä 16

Kokonaisalue D on UFD eli yksikäsitteisen tekijöihinjaon alue/unique factorization domain, jos jokainen alkio $a \in D, a \neq 0, a \notin D^*$ voidaan esittää yksikäsitteisesti muodossa

$$a = j_1 \cdots j_r, \quad j_i \in J_D. \tag{5.42}$$

Lause 4

Olkoon D kokonaisalue/Let D be an ID. Tällöin/Then

$$P_D \subseteq J_D \tag{5.43}$$

eli alkualkiot ovat jaottomia/primes are irreducible..

Todistus. (5.43): Let $p \in P_D$. If $q|p$, then $p = qd_1$ for some $d_1 \in D$. Then

$$p|qd_1 \quad \Rightarrow \quad p|q \quad \text{or} \quad p|d_1 \tag{5.44}$$

because p is a prime.
If $p|q$, then $q = d_2 p$, $d_2 \in D$ and $q = d_2 q d_1$, where $q \neq 0$ by $p \neq 0$. So $1 = d_1 d_2$ meaning that $d_1, d_2 \in D^*$. Therefore $q \in [p]$.
If $p|d_1$, then (homework...) $q \in [1]$.
Thus $p \in J_D$. □

Lause 5

Olkoon D kokonaisalue. Tällöin

$$D = UFD \quad \Rightarrow \quad J_D \subseteq P_D \tag{5.45}$$

eli UFD:n jaottomat alkiot ovat alkualkiota/irreducibles are primes ja tällöin $J_D = P_D$.

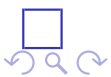
Todistus: Olkoon $j \in J_D$ ja oletetaan, että $j|ab$, missä $a, b \in D$. Koska $D =$UFD, niin a:lla ja b:llä $\exists!$ esitykset

$$a = a_1 \cdots a_m, \quad b = b_1 \cdots b_n, \quad a_i, b_i \in J_D. \tag{5.46}$$

Siten

$$j|a_1 \cdots a_m b_1 \cdots b_n = j \cdot j_2 \cdots j_{m+n}, \tag{5.47}$$

josta seuraa että $j \sim a_i$, jollakin a_i tai $j \sim b_i$, jollakin b_i, koska $D =$UDF.
Täten $j|a$ tai $j|b$.
Siispä $j \in P_D$.



Huomautus 3

Yksikäsitteisessä tekijöihinjaon alueessa esitystä (5.42) sanotaan alkion a alkutekijähajotelmaksi. In UFD the representation (5.42) is called prime factorization.

Määritelmä 17

Olkoon D kokonaisalue ja $a \in D$. Jos jaottomalle alkiolle $j \in J_D$ pätee

$$j^m \| a, \quad m \in \mathbb{Z}_{\geq 0}, \tag{5.48}$$

niin luku m on alkion a tekijän j kertaluku/multiplicity of the factor.

Tietenkin, jos $j \nmid a$, niin $m = 0$.

Lause 6

Olkoon D kokonaisalue. Tällöin

$$J_D \subseteq P_D \quad \Rightarrow \quad D = UFD. \tag{5.49}$$

Todistus: Let

$$a = j_1 \cdots j_r = h_1 \cdots h_s, \quad j_l, h_k \in J_D \tag{5.50}$$

Now irreducibles j_l and h_k are primes. Thus

$$j_1 | h_1 \cdots h_s \quad \Rightarrow \quad j_1 | h_1 \quad \text{or} \quad j_1 | h_2 \cdots h_s \ldots \tag{5.51}$$

and eventually $j_1 | h_{k_1}$ implying $j_1 \sim h_{k_1}$,...,$j_r \sim h_{k_r}$ and $r = s$. □

Division algorithm/Euclidean domain

Olkoon nyt D kokonaisalue, jossa on ns. Eukleideen funktio $E: \ D \to \mathbb{N} \cup \{-\infty\}$ eli pätee
Jakoalgoritmi: Jos $a, b \in D$ on annettu ja $ab \neq 0$, $0 \leq E(b) \leq E(a)$, niin $\exists \ q, r \in D$ s.e.

$$(J.A.) \quad a = qb + r \text{ ja } E(r) < E(b). \tag{5.52}$$

Tälläista aluetta sanotaan Eukleideen alueeksi/This kind of domain is called Euclidean domain/ED. (huomaa, että Eukleideen funktion määritelmä vaihtelee.)

Esimerkki 13

$a) D = \mathbb{Z}, \quad E(k) = |k|.$
$b) D = K[x], \quad E(p(x)) = \deg p(x).$

Jakoalgoritmin nojalla saadaan
Eukleideen algoritmi=E.A.:

$$
\begin{aligned}
& r_0 = a,\ r_1 = b && E(r_1) < E(r_0) \\
& r_0 = q_1 r_1 + r_2 && E(r_2) < E(r_1) \\
& \vdots \\
& r_k = q_{k+1} r_{k+1} + r_{k+2} && E(r_{k+2}) < E(r_{k+1}) \\
& \vdots \\
& r_{n-1} = q_n r_n && \exists\ n \in \mathbb{N}:\ r_n \neq 0,\ r_{n+1} = 0 \\
& r_n = \mathrm{syt}(a, b).
\end{aligned}
$$

Tässä $n =$ Eukleideen algoritmin pituus/length.

Set now/Asetetaan nyt

$$R_k = \begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix}, \; Q_k = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}, \; k \in \mathbb{N}, \tag{5.53}$$

whereupon/jolloin

$$\det Q_k = -1, \quad {Q_k}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix}. \tag{5.54}$$

We see that/Nähdään, että

$$\text{E.A.} \Leftrightarrow R_k = Q_{k+1} R_{k+1}, \; \forall k = 0, \ldots, n-1, \tag{5.55}$$

whereupon holds/jolloin pätee

$$R_0 = Q_1 Q_2 \cdots Q_k R_k. \tag{5.56}$$

Denote/Merkitään

$$S_0 = \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{5.57}$$

ja

$$S_k = \begin{pmatrix} s_k & t_k \\ s_{k+1} & t_{k+1} \end{pmatrix} = {Q_k}^{-1} \cdots {Q_2}^{-1} {Q_1}^{-1}, \tag{5.58}$$

jolloin

$$R_k = S_k R_0. \tag{5.59}$$

Nyt

$$S_{k+1} = Q_{k+1}^{-1} S_k \tag{5.60}$$

eli

$$\begin{pmatrix} s_{k+1} & t_{k+1} \\ s_{k+2} & t_{k+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{k+1} \end{pmatrix} \begin{pmatrix} s_k & t_k \\ s_{k+1} & t_{k+1} \end{pmatrix} =$$

$$\begin{pmatrix} s_{k+1} & t_{k+1} \\ s_k - q_{k+1} s_{k+1} & t_k - q_{k+1} t_{k+1} \end{pmatrix} \tag{5.61}$$

$\Leftrightarrow$ Palautuskaavat eli rekursiot/recurrences:

$$\begin{cases} s_{k+2} = s_k - q_{k+1} s_{k+1}, \ \ k = 0, 1, \ldots \\ t_{k+2} = t_k - q_{k+1} t_{k+1}, \ \ k = 0, 1, \ldots \end{cases} \tag{5.62}$$

From formula/Yhtälöstä (5.59) we get/saadaan

$$r_n = s_n a + t_n b, \tag{5.63}$$

josta edelleen/further saadaan

Lause 7

Olkoon D Eukleideen alue/ED, silloin

$$syt(a, b) = s_n a + t_n b, \tag{5.64}$$

where/missä n on E.A:n pituus/lenght.

Usein riittää seuraava tulos/Usually the following formulation is enough

Lause 8

Let D be an ED. Then there exist $s, t \in D$ *such that*

$$gcd(a, b) = sa + tb. \tag{5.65}$$

Lause 9

Olkoon D Eukleideen alue. Tällöin

$$J_D \subseteq P_D \tag{5.66}$$

eli jaottomat alkiot ovat alkualkioita/In ED irreducibles are primes. Edelleen, Eukleideen alue on UFD.

Todistus. Let $j \in J_D$ and let us assume, that $j|ab$, where $a, d \in D$.
We should show that $j|a$ or $j|b$.
Suppose that $j \not| a$, then $j \perp a$ by Lemma 5. Then by Theorem 8 there exist $s, t \in D$ such that

$$1 = sa + tj \quad \Rightarrow \quad b = sab + tbj \quad \Rightarrow \quad j|b. \quad \square \tag{5.67}$$

Seuraus 1

.

A. $\mathbb{Z}$ on UFD, missä jaottomat alkiot ovat alkualkioita.

B. $K[x]$ on UFD, missä jaottomat alkiot ovat alkualkioita.

Polynomijoukko

Olkoon R ykkösellinen rengas. Tällöin R-kertoimisten polynomien joukolle käytetään merkintää

$$R[x] = \{P(x) \mid P(x) = \sum_{k=0}^{n} p_k x^k;\ p_k \in R,\ n \in \mathbb{N}\}.$$

Polynomia

$$0(x) = 0 + 0 \cdot x + 0 \cdot x^2 + \ldots \tag{6.1}$$

kutsutaan nollapolynomiksi ja polynomia

$$1(x) = 1 + 0 \cdot x + 0 \cdot x^2 + \ldots \tag{6.2}$$

ykköspolynomiksi. Ne ovat erikoistapauksia vakiopolynomista

$$c(x) = c + 0 \cdot x + 0 \cdot x^2 + \ldots, \quad c \in R. \tag{6.3}$$

Laskutoimitukset

Määritelmä 18

Olkoot $P(x) = \sum_{k=0}^{n} p_k x^k, \quad Q(x) = \sum_{k=0}^{n} q_k x^k \in R[x]$, *jolloin asetetaan*

$$P(x) = Q(x) \Leftrightarrow \forall k(p_k = q_k);$$

$$P(x) + Q(x) = \sum_{k \geqslant 0} (p_k + q_k) x^k;$$

$$P(x) \cdot Q(x) = \sum_{k \geqslant 0} r_k x^k,$$

$$r_k = \sum_{i=0}^{k} p_i q_{k-i} = \sum_{i+j=k} p_i q_j, \tag{6.4}$$

joka on Cauchyn kertosääntö.

Polynomial ring/degree

Lause 10

Tällöin $(R[x], +, \cdot)$ *on rengas, missä* $0(x)$ *on yhteenlaskun nolla-alkio ja* $1(x)$ *on kertolaskun ykkösalkio.*

Määritelmä 19

Jos $p_n \neq 0$, *niin polynomin* $P(x) = \sum_{k=0}^{n} p_k x^k$ *aste/degree on*

$$\deg P(x) = n, \tag{6.5}$$

lisäksi asetetaan/set

$$\deg 0(x) = -\infty. \tag{6.6}$$

Astekaava/Degree formula

Huomautus 4

$$\begin{aligned} -\infty + (-\infty) &= -\infty \\ -\infty + k &= -\infty, \quad \forall\ k \in \mathbb{Z}. \end{aligned} \tag{6.7}$$

Lause 11

Degree formula.
Olkoon D kokonaisalue ja $P(x), Q(x) \in D[x]$. Tällöin

$$\deg P(x)Q(x) = \deg P(x) + \deg Q(x). \tag{6.8}$$

Lause 12

.

A. Olkoon $R = D$ kokonaisalue. Tällöin polynomirengas $D[x]$ on kokonaisalue.
B. Olkoon $R = K$ kunta. Tällöin polynomirengas $K[x]$ on kokonaisalue.

Todistus: Olkoon $a(x)b(x) = 0(x)$. Astekaavan nojalla

$$\deg a(x)b(x) = \deg a(x) + \deg b(x) = \deg 0(x) = -\infty. \tag{6.9}$$

Jos olisi $a(x) \neq 0(x)$ ja $b(x) \neq 0(x)$, niin

$$0 \leq \deg a(x) + \deg b(x) = -\infty. \tag{6.10}$$

Ristiriita. □

Lause 13

Olkoon K kunta.
A. Polynomirenkaan $K[x]$ yksikköryhmä on K^* eli

$$K[x]^* = K^*. \tag{6.11}$$

B. Polynomi $j(x) \in K[x] \setminus K$ on jaoton täsmälleen silloin, kun sen ainoat tekijät ovat vakioita k tai polynomeja $k \cdot j(x)$, missä $k \in K \setminus \{0\}$.
C. Edelleen, polynomi $a(x) \in K[x] \setminus \{0(x)\}$ on jaollinen täsmälleen silloin, kun sillä on tekijä $d(x) \in K[x]$, jolle pätee

$$1 \leq \deg d(x) \leq \deg a(x) - 1. \tag{6.12}$$

D. Erityisesti ensimmäisen asteen polynomit ovat jaottomia.

Todistus. A: $a(x) \in K[x]^* \quad \Rightarrow \quad \exists\ b(x) \in K[x]$ such that

$a(x)b(x) = 1 \quad \Rightarrow \quad \deg a(x) = \deg b(x) = 0 \quad \Rightarrow \quad a(x), b(x) \in K^*.$ □

Todistus. B: $j(x) = a(x)b(x) \in J_{K[x]} \quad \Rightarrow$

$$a(x) \in [1] = K[x]^* = K^* \quad \Rightarrow \quad a(x) = k, \quad k \in K^*$$

or

$$a(x) \in [j(x)] = j(x)K^* \quad \Rightarrow \quad a(x) = kj(x), \quad k \in K^*.$$ □

Todistus. C: Let $a(x) \in K[x] \setminus \{0\}$ be reducible. Then there exists $d(x), b(x) \in K[x] \setminus \{0\}$ such that

$$a(x) = d(x)b(x), \quad d(x) \notin [1] \quad \text{and} \quad d(x) \notin [a(x)] \quad \Rightarrow$$

$$d(x) \notin K^* \quad \text{and} \quad d(x) \notin a(x)K^*.$$

If $\deg d(x) = 0$, then $d(x) \in K^*$; a contradiction.
If $\deg d(x) = \deg a(x)$, then by the degree formula $\deg b(x) = 0$ implying $b(x) = k \in K^*$. Thus $a(x) = kd(x)$ and then $d(x) \in [a(x)]$; a contradiction. □
Todistus. D: Homework.

Renkaan $R[x]$ yksikköryhmästä

Let R be commutative ring with a unit. Let us study its unit group $R[x]^*$. Pick $a(x) = a_0 + a_1x + ... + a_Ax^A \in R[x]^*$, then there exists $b(x) = b_0 + b_1x + ... + b_Bx^B \in R[x]^*$ such that

$$1 = a(x)b(x) = (a_0 + a_1x + ... + a_Ax^A)(b_0 + b_1x + ... + b_Bx^B). \quad (6.13)$$

If $a_1 = ... = a_A = 0$, then $a(x) \in R^*$. Otherwise there exists an $A \geq 1$ such that $a_A \neq 0$. Then

On the unit group of the ring $R[x]$

$$
\begin{aligned}
& a_0 b_0 = 1 \\
& a_0 b_1 + a_1 b_0 = 0 \\
& a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \\
& \dots \\
& a_{A-2} b_B + a_{A-1} b_{B-1} + a_A b_{B-2} = 0 \\
& a_{A-1} b_B + a_A b_{B-1} = 0 \\
& a_A b_B = 0
\end{aligned}
\tag{6.14}
$$

Multiply the second last by a_A to get

$$
a_{A-1} a_A b_B + a_A^2 b_{B-1} = 0 \quad \Rightarrow \quad a_A^2 b_{B-1} = 0 \tag{6.15}
$$

On the unit group of the ring $R[x]$

$$\begin{aligned} &\dots \\ &a_{A-2}b_B + a_{A-1}b_{B-1} + a_A b_{B-2} = 0 \\ &a_{A-1}b_B + a_A b_{B-1} = 0 \\ &a_A b_B = 0 \end{aligned} \tag{6.16}$$

Multiply the third last by a_A^2 to get

$$a_{A-2}a_A^2 b_B + a_{A-1}a_A^2 b_{B-1} + a_A^3 b_{B-2} = 0 \quad \Rightarrow \quad a_A^3 b_{B-2} = 0 \tag{6.17}$$

and so on to the situation

$R[x]^*$

$$\begin{aligned} &\dots \\ &a_0 b_B + a_1 b_{B-1} + \dots + a_A b_0 = 0, \quad A \leq B \\ &a_A^A b_1 = 0 \end{aligned} \tag{6.18}$$

or

$$\begin{aligned} &\dots \\ &a_c b_B + a_1 b_{B-1} + \dots + a_A b_0 = 0, \quad A = B + c, c > 0, \\ &a_A^A b_1 = 0. \end{aligned} \tag{6.19}$$

Anyway, multiply now by a_A^A. Then you get

$R[x]^*$

$$a_A^{A+1} b_0 = 0, \tag{6.20}$$

where $b_0 \in R^*$ meaning that $b_0 \neq 0$. Then multiplying by b_0^{-1} we are in the situation $a_A^{A+1} = 0$.
Thus if

$$r^K \neq 0 \quad \forall\ r \in R \setminus \{0\},\ K \geq 2, \tag{6.21}$$

then $a(x) = a_0 \in R^*$.
Otherwise: if there exists such an element $r \in R \setminus \{0\}$ that

$$r^K = 0 \quad \text{for some} \quad K \geq 2, \tag{6.22}$$

then you may find a non-constant unit polynomial $a(x)$ i.e $a(x) \in R[x]^* \setminus R^*$.

$\mathbb{Z}_m[x]^*$

Esimerkki 14

$$\mathbb{Z}_{10}[x]^* = \mathbb{Z}_{10}^*.$$

Esimerkki 15

$$1 + 10x \in \mathbb{Z}_{20}[x]^*.$$

Jakoalgoritmi/Division algorithm

Lause 14

Division algorithm. Olkoon K kunta. Olkoon $a(x), b(x) \in K[x]$, $a(x)b(x) \neq 0(x)$ ja $\deg b(x) \leq \deg a(x)$.
Tällöin $\exists\ q(x), r(x) \in K[x]$ s.e.

$$[J.A.] \quad a(x) = q(x)b(x) + r(x), \quad \deg r(x) < \deg b(x). \tag{6.23}$$

Edelleen, $K[x]$ on Eukleideen alue!

Huomautus 5

Jos D ei ole kunta, niin jakoalgoritmi ei välttämättä päde polynomirenkaassa $D[x]$!!
If D is not a field, then the division algorithm does not work necessarily in the polynomial ring $D[x]$!!

Polynomien $a(x)$ ja $b(x)$ suurin yhteinen tekijä $d(x) = \text{s.y.t.}(a(x), b(x))$ voidaan valita pääpolynomiksi.
Eukleideen algoritmin nojalla saadaan, että on olemassa sellaiset polynomit $s(x), t(x) \in K[x]$, että

$$d(x) = s(x)a(x) + t(x)b(x). \tag{6.24}$$

Määritelmä 20

Polynomin

$$p(x) = \sum_{k=0}^{n} p_k x^k \in K[x]$$

(formaali) derivaatta $Dp(x)$*on polynomi*

$$Dp(x) = \sum_{k=1}^{n} k p_k x^{k-1} \in K[x]. \tag{6.25}$$

Lemma 6

Olkoon K *kunta,* $p(x) \in K[x]$ *ja* $\deg p(x) \geq 1$*. Tällöin*

$$\deg Dp(x) = \deg p(x) - 1, \quad \deg p(x) \geq 1; \tag{6.26}$$

$$p(x) \not| Dp(x). \tag{6.27}$$

Lause 15

Olkoon K kunta ja $a(x), b(x), c(x) \in K[x]$. Tällöin

$$a = b^2 c, \quad b \not\sim 1 \quad \Leftrightarrow \quad d = syt(a, Da) \not\sim 1. \tag{6.28}$$

Todistus.
Olkoon $a = b^2 c$, $b \not\sim 1$. Koska $Da = b(2cDb + bDc)$, niin $b|\text{syt}(a, Da)$ ja siten $\text{syt}(a, Da) \not\sim 1$.
Olkoon $d = \text{syt}(a, Da) \not\sim 1$. Tällöin on olemassa $p \in P_{K[x]}$, $p|d$. Siten $a = ps$ ja $Da = pr$. Toisaalta $Da = (Dp)s + pDs$, joten $pr = (Dp)s + pDs$. Koska $p \nmid Dp$ ja p on alkualkio, niin $p|s$. Niinpä $s = ph$ ja $a = ps = p^2 h$, jollakin h ja $p \not\sim 1$. □

Väite (6.28) on yhtäpitävää seuraavan väitteen kanssa:
Polynomi on neliövapaa täsmälleen silloin kun sillä ei ole yhteisiä tekijöitä derivaattansa kanssa.
Claim (6.28) is equivalent to following claim:
A polynomial is square-free exactly when it does not have common factors with its derivative.

Esimerkki 16

Olkoon $p(x) = x^5 + 2x^3 + x \in \mathbb{Q}[x]$. *Laskemalla saadaan/by calculating*

$$syt(p, Dp) \not\sim 1 \quad \Rightarrow \tag{6.29}$$

polynomilla $p(x)$ *on useampikertainen tekijä/higher order factor/multiple factor renkaassa* $\mathbb{Q}[x]$.

Lause 16

Olkoon K kunta ja $p(x) \in K[x]$, $1 \leq \deg p(x)$. Tällöin

$$p(\alpha) = 0,\ \alpha \in K \Leftrightarrow (x-\alpha) \underset{K[x]}{\mid} p(x). \tag{6.30}$$

Todistus. "$\Diamond \rightarrow$": Olkoon $p(\alpha) = 0,\ \alpha \in K$. Jakoalgoritmin nojalla

$$p(x) = q(x)(x-\alpha) + r(x), \quad \deg r(x) < \deg(x-\alpha) = 1, \tag{6.31}$$

joten $r(x) \in K$ on vakio. Edelleen

$$\begin{aligned} 0 = p(\alpha) = q(\alpha)(\alpha-\alpha) + r(\alpha) = r(\alpha), \\ \Rightarrow \quad r(x) = 0(x) \quad \Rightarrow \quad (x-\alpha) \underset{K[x]}{\mid} p(x). \end{aligned} \tag{6.32}$$

"$\leftarrow \triangle$":

$$(x-\alpha) \underset{K[x]}{\mid} p(x) = (x-\alpha)h(x), \quad \Rightarrow \quad p(\alpha) = 0,\ \alpha \in K. \ \square \tag{6.33}$$

Huomautus 6

Olkoon K on kunta ja $p(x) \in K[x]$, $\deg p(x) = 2$ tai $\deg p(x) = 3$. Jos $p(x)$ jakaantuu/is reducible polynomirenkaassa $K[x]$, niin sillä on 1. asteen tekijä/then it has first degree factor ja Lauseen 16 nojalla $p(\alpha) = 0,\ \alpha \in K$. Jos nollakohtaa ei ole K:ssa/If there is no zero in K, niin $p(x)$ on jaoton/irreducible polynomirenkaassa $K[x]$.

Laajennetaan Määritelmää 3.

Määritelmä 21

Olkoon $K \subseteq L$ kuntia ja $p(x) \in K[x]$. Tällöin

$$Z_L(p) = \{\alpha \in L |\ p(\alpha) = 0\} \tag{6.34}$$

on polynomin $p(x)$ nollajoukko L:ssä.

Määritelmä 22

Olkoon $\alpha \in L$, $K \subseteq L$ kuntia ja $p(x) \in K[x]$. Jos

$$(x-\alpha)^m \underset{L[x]}{\parallel} p(x), \quad m \in \mathbb{N}, \tag{6.35}$$

niin $m = m_L(\alpha, p(x))$ on polynomin $p(x)$ nollakohdan $\alpha \in L$ kertaluku/order of zero/multiplicity of zero. Edelleen

$$n_L(p(x)) = \sum_{p(\alpha_i)=0,\ \alpha_i \in L} m_L(\alpha_i, p(x)). \tag{6.36}$$

nollakohtien lukumäärä/number of zeros joukossa L.

Lause 17

Olkoon K kunta, $\mathrm{char}\, K = 0$, $\alpha \in K$ ja $p(x) \in K[x]$ ja $m \in \mathbb{N}$. Tällöin

$$(x-\alpha)^m \underset{K[x]}{\parallel} p(x) \quad \Leftrightarrow \tag{6.37}$$

$$D^k p(\alpha) = 0 \quad \forall\ k = 0, \ldots, m-1 \quad , D^m p(\alpha) \neq 0. \tag{6.38}$$

Huomautus 7

Lause 17 EI päde esimerkiksi polynomirenkaassa $\mathbb{Z}_p[x]$.

Esimerkki 17

Olkoon $p(x) = (x-1)^3(x+1/2)^5$. *Polynomin* $p(x)$ *nollakohdat ovat* $\alpha_1 = 1$ *ja* $\alpha_2 = -1/2$. *Nollakohtien kertaluvut ovat*

$$m_{\mathbb{Q}}(\alpha_1, p(x)) = 3, \quad m_{\mathbb{Q}}(\alpha_2, p(x)) = 5 \tag{6.39}$$

ja nollakohtien lukumäärä

$$n_{\mathbb{Q}} = 3 + 5 = 8. \tag{6.40}$$

Esimerkki 18

Olkoon $(x^2+1)(x^2-2) \in \mathbb{R}[x]$. *Nyt nollakohtien lukumäärät ovat*

$$n_{\mathbb{Q}} = 0 < 4 = \deg p(x). \tag{6.41}$$

$$n_{\mathbb{R}} = m(-\sqrt{2}) + m(\sqrt{2}) = 2 < 4 = \deg p(x). \tag{6.42}$$

$$n_{\mathbb{C}} = 4 = \deg p(x). \tag{6.43}$$

Lause 18

Olkoon K kunta, $p(x) \in K[x]$ ja $\deg p(x) \geq 1$. Tällöin pätee

$$n_K(p(x)) \leq \deg p(x). \tag{6.44}$$

Todistus:

1. Jos $\nexists$ nolla-kohtaa, niin $m_K(\alpha, p(x)) = 0$, kaikilla $\alpha \in K$. Siten $n_K(p(x)) = 0 < 1 \leq \deg p(x)$.
2. Olkoot $\beta_1, ..., \beta_k$ erillisiä nollakohtia, jolloin

$$m_j := m_K(\beta_j, p(x)) \geq 1 \quad \text{ja} \quad (x - \beta_j)^{m_j} \underset{K[x]}{\parallel} p(x), \quad j = 1, ..., k. \tag{6.45}$$

Siten

$$p(x) = (x - \beta_1)^{m_1} p_2(x), \quad p_2(\beta_1) \neq 0 \quad \Rightarrow \quad p_2(\beta_2) = 0, \tag{6.46}$$

$$p_2(x) = (x - \beta_2)^{m_2} p_3(x), \quad p_3(\beta_2) \neq 0 \quad \Rightarrow \quad p_3(\beta_3) = 0 \quad ... \tag{6.47}$$

... Lopulta

$$p(x) = (x - \beta_1)^{m_1} \cdots (x - \beta_k)^{m_k} p_{k+1}(x), \quad \deg p_{k+1}(x) \geq 0. \qquad (6.48)$$

Astekaavalla saadaan

$$\begin{aligned} \deg p(x) &= m_1 + \ldots + m_k + \deg p_{k+1}(x) \\ &\geq m_1 + \ldots + m_k = n_K(p(x)). \quad \square \end{aligned} \qquad (6.49)$$

Lause 19

ALGEBRAN PERUSLAUSE.
Olkoon $p(x) \in \mathbb{C}[x]$, *deg* $p(x) \geq 1$, *tällöin*

$$n_{\mathbb{C}}(p(x)) = \deg p(x). \tag{6.50}$$

Lause 20

Olkoot $K \subseteq L$ kuntia, $p(x) \in K[x]$ ja $p(x) \in J_{K[x]}$. Tällöin

$$m_L(\alpha, p(x)) \leq 1 \quad \forall \alpha \in L. \tag{6.51}$$

Todistus. Koska $p \in J_{K[x]}$, niin $\deg p(x) \geq 1$ ja siten $p \not| Dp$. Täten Lemman 5 nojalla $p \perp Dp$ ja edelleen Lauseen 8 nojalla

$$\operatorname{syt}_{K[x]}(p, Dp) = 1 = sp + tDp, \quad s, t \in K[x] \subseteq L[x]. \tag{6.52}$$

Jos nyt

$$d \underset{L[x]}{|} p \quad \text{ja} \quad d \underset{L[x]}{|} Dp \tag{6.53}$$

niin yhtälön (6.52) mukaan $d \underset{L[x]}{|} 1$. Siten myös

$$\operatorname{syt}_{L[x]}(p, Dp) = 1. \tag{6.54}$$

Tällöin Lauseen 15 nojalla $\nexists$ neliötekijää renkaassa $L[x]$, joten $\nexists$ sellaista $\alpha \in L$, että

$$(x-\alpha)^2 \underset{L[x]}{\mid} p(x). \tag{6.55}$$

Siten:
Jos $p(\alpha) = 0$, niin $m_L(\alpha, p(x)) = 1$ ja
jos $p(\alpha) \neq 0$, niin $m_L(\alpha, p(x)) = 0$. □

Lause 21

Olkoon K kunta, $p(x), q(x) \in K[x]$, $p(x) \in J_{K[x]}$ sekä $p(\alpha) = q(\alpha) = 0$. Tällöin

$$p(x) \underset{K[x]}{\mid} q(x). \tag{6.56}$$

Todistus. Koska p on jaoton, niin

$$d = \operatorname{syt}_{K[x]}(p, q) = 1 \quad \text{tai} \quad p. \tag{6.57}$$

Jos $d = 1$, niin $1 = s(x)p(x) + t(x)q(x)$ ja edelleen $1 = s(\alpha)p(\alpha) + t(\alpha)q(\alpha) = 0$. Ristiriita.
Niinpä $d = p$ ja siten $p|q$. □

Seuraavassa käytetään jakojäännösluokkia $\overline{a} \in \mathbb{Z}_n$. Huomaa, että kun $p \in \mathbb{P}$, niin $\mathbb{Z}_p$ on kunta.

Määritelmä 23

Olkoon $n \in \mathbb{Z}_{\geq 2}$ *ja* $a(x) = a_0 + a_1 x + \ldots + a_d x^d \in \mathbb{Z}[x]$. *Kuvaus*

$$r_n(a_0 + a_1 x + \ldots + a_d x^d) = \overline{a}_0 + \overline{a}_1 x + \ldots + \overline{a}_d x^d \tag{6.58}$$

$$r_n : \ \mathbb{Z}[x] \to \mathbb{Z}_n[x], \quad r_n(a(x)) = \overline{a}(x),$$

on reduktio $\pmod{n}$.

Lause 22

Reduktio

$$r_n : \ \mathbb{Z}[x] \to \mathbb{Z}_n[x], \quad r_n(a(x)) = \overline{a}(x),$$

on rengasmorfismi.

Määritelmä 24

Vektori $(a_0, ..., a_A) \in \mathbb{Z}^{m+1}$ *ja polynomi*
$a(x) = a_0 + a_1 x + ... + a_A x^A \in \mathbb{Z}[x]$ *ovat primitiivisiä, jos*

$$syt(a_0, ..., a_A) = 1. \tag{6.59}$$

Joskus vaaditaan, että primitiiviselle polynomille pätee lisäksi $a_A \geq 1$.

Lemma 7

Olkoot $a(x) \in \mathbb{Z}[x]$ *ja* $B, C \in \mathbb{Z}$.
A. Jos $a(x)$ *on primitiivinen, niin*

$$B \underset{\mathbb{Z}[x]}{\mid} C \cdot a(x) \quad \Rightarrow \quad B \underset{\mathbb{Z}}{\mid} C. \tag{6.60}$$

B. Jos $D = syt(a_0, \ldots, a_A)$, *niin*

$$a(x) = D \cdot b(x), \quad b(x) \in \mathbb{Z}[x], \tag{6.61}$$

missä polynomi $b(x)$ *on primitiivinen.*
C. Kohtien A. ja B. polynomit voi korvata vastaavilla
vektoreilla/polynomials may be replaced by corresponding vectors.

Lemma 8

Olkoot $b(x)$ ja $c(x)$ primitiivisiä. Tällöin $b(x)c(x)$ on primitiivinen

Todistus. Olkoon

$$a(x) = b(x)c(x) = a_0 + a_1x + ... + a_Ax^A \in \mathbb{Z}[x] \tag{6.62}$$

ja

$$syt(a_0, ..., a_A) = d \geq 2 \quad \Rightarrow \quad \exists \quad p \in \mathbb{P}, \quad p|d. \tag{6.63}$$

Otetaan reduktio $\pmod p$, jolloin

$$\overline{a}(x) = \overline{0}(x) = \overline{b}(x)\overline{c}(x) \quad \in \mathbb{Z}_p[x]. \tag{6.64}$$

Nyt $\mathbb{Z}_p[x]$ on kokonaisalue, joten

$$\overline{b}(x) = \overline{0}(x) \quad \text{tai} \quad \overline{c}(x) = \overline{0}(x). \tag{6.65}$$

Siten

$$p|syt(b_0, ..., b_B) \quad \text{tai} \quad p|syt(c_0, ..., c_C) \tag{6.66}$$

mikä on ristiriita.

Merkintä 7

A. Olkoon $B = \frac{q}{r} \in \mathbb{Q}$, $q \in \mathbb{Z}$, $r \in \mathbb{Z}^+$, $q \perp r$. *Tällöin*

$$den(B) := r \tag{6.67}$$

on rationaaliluvun B *nimittäjä.*
Olkoot $den(B_j) = r_j$, $j = 1, ..., m$, *rationaalilukujen* B_j *nimittäjiä. Tällöin*

$$pyn(B_1, ..., B_m) := pyj(r_1, ..., r_m) \tag{6.68}$$

on lukujen $B_1, ..., B_m$ *pienin yhteinen nimittäjä (least common denominator=lcd).*

Lemma 9

Olkoon
$B(x) = B_0 + B_1 x + \ldots + B_m x^m \in \mathbb{Q}[x]$ *ja*

$$R := pyn(B_0, B_1, \ldots, B_m), \quad Q := syt(RB_0, \ldots, RB_m). \tag{6.69}$$

Tällöin polynomi

$$\frac{R}{Q} B(x) := b_0 + b_1 x + \ldots + b_m x^m \in \mathbb{Z}[x] \tag{6.70}$$

on primitiivinen. Edelleen $R \perp Q$.

Todistus: Koska

$$\frac{R}{Q}B_j = b_j, \quad j = 0, 1, ..., m, \tag{6.71}$$

niin

$$(RB_0, ..., RB_m) = Q \cdot (b_0, b_1, ..., b_m), \tag{6.72}$$

missä $Q = syt(RB_0, ..., RB_m)$. Siten Lemman 7 nojalla $(b_0, b_1, ..., b_m)$ ja edelleen polynomi $b_0 + b_1x + ... + b_mx^m$ ovat primitiivisiä.
Tutkitaan väitettä $R \perp Q$. Olkoon $d = syt(R, Q)$, siten $R = dr$ ja $Q = dq$, $r, q \in \mathbb{Z}^+$. Yhtälöstä (6.71) saadaan

$$Rq_j = Qr_jb_j \quad \Rightarrow \quad rq_j = qr_jb_j, \quad j = 0, 1, ..., m. \tag{6.73}$$

Koska $q_j \perp r_j$, niin $r_j|r$ aina, kun $j = 0, 1, ..., m$. Siten $R = dr|r$, josta $d = 1$. □

Esimerkki 19

$$B(x) = 7 + \frac{21}{5}x + \frac{14}{3}x^2, \quad R = 15, \quad Q = 7. \tag{6.74}$$

Lause 23

Gaussin lemma. Olkoon $a(x) \in \mathbb{Z}[x]$ *primitiivinen ja* $\deg a(x) \geq 2$. *Jos* $a(x)$ *jakaantuu polynomirenkaassa/reducible in the polynomial ring* $\mathbb{Q}[x]$, *niin on olemassa sellaiset primitiiviset polynomit*

$$b(x), c(x) \in \mathbb{Z}[x], \quad \textit{että} \quad a(x) = b(x)c(x). \tag{6.75}$$

Todistus. Oletetaan, että

$$a(x) = B(x)C(x), \quad B(x), C(x) \in \mathbb{Q}[x]. \tag{6.76}$$

Lemman 9 nojalla on olemassa sellaiset $R, Q, T, S \in \mathbb{Z}^+$, että

$$\frac{R}{Q}B(x) := b(x) \in \mathbb{Z}[x],$$

$$\frac{T}{S}C(x) := c(x) \in \mathbb{Z}[x],$$

$$R \perp Q, \quad T \perp S, \tag{6.77}$$

missä $b(x)$ ja $c(x)$ ovat primitiivisiä. Edelleen

$$RTa(x) = QSb(x)c(x). \tag{6.78}$$

Koska $R \perp Q$ ja $a(x)$ on primitiivinen, niin $Q|T = Qt$ ja vastaavasti $S|R = Qr$. Siispä

$$rta(x) = b(x)c(x), \tag{6.79}$$

missä $b(x)c(x)$ on primitiivinen, joten $rt = 1$ ja lopulta $a(x) = b(x)c(x)$.

Gaussin lemman nojalla polynomin $a(x) \in \mathbb{Z}[x]$ jaollisuutta voidaan tarkastella polynomirenkaassa $\mathbb{Z}[x]$. Siten polynomi on jaoton renkaassa $\mathbb{Q}[x]$, jos se on jaoton renkaassa $\mathbb{Z}[x]$. Edelleen saadaan tulos

Lause 24

Olkoon $a(x) \in \mathbb{Z}[x]$. Tällöin saadaan yksikäsitteinen esitys

$$a(x) = Aa_1(x) \cdots a_n(x), \quad A \in \mathbb{Z}, \tag{6.80}$$

missä $a_1(x), ..., a_k(x) \in \mathbb{Z}[x]$ ovat primitiivisiä jaottomia polynomeja.

Lause 25

Olkoot $p \in \mathbb{P}$, $a(x) \in \mathbb{Z}[x]$, $\overline{a}(x) \in \mathbb{Z}_p[x]$ *ja* $A = \deg a(x) = \deg \overline{a}(x)$. *Jos* $\overline{a}(x)$ *on jaoton polynomirenkaassa* $\mathbb{Z}_p[x]$, *niin* $a(x)$ *on jaoton polynomirenkaassa* $\mathbb{Q}[x]$.

Todistus. Vastaoletus eli olkoon

$$a(x) = b(x)c(x), \quad B = \deg b(x) \geq 1, \ C = \deg c(x) \geq 1. \tag{6.81}$$

Otetaan reduktio $\pmod p$, jolloin

$$\overline{a}(x) = \overline{b}(x)\overline{c}(x) \quad \in \mathbb{Z}_p[x]. \tag{6.82}$$

Koska

$$\deg \overline{b}(x) \leq B, \quad \deg \overline{c}(x) \leq C \tag{6.83}$$

ja

$$\deg \overline{b}(x) + \deg \overline{c}(x) = \deg \overline{a}(x) = A, \tag{6.84}$$

niin

$$\deg \overline{b}(x) = B \geq 1, \quad \deg \overline{c}(x) = C \geq 1. \tag{6.85}$$

Siten $\overline{a}(x)$ jakaantuu polynomirenkaassa $\mathbb{Z}_p[x]$.
Ristiriita. □

Lause 26

Eisensteinin kriteeri. Olkoon

$$a(x) = a_0 + a_1 x + \ldots + a_A x^A \in \mathbb{Z}[x], \quad \deg a(x) = A \geq 2.$$

Jos on olemassa sellainen $p \in \mathbb{P}$, *että*

$$p | a_i \quad \forall\ i = 0, 1, \ldots, A-1, \quad p^2 \nmid a_0, \quad p \nmid a_A, \tag{6.86}$$

niin $a(x)$ *on jaoton polynomirenkaassa* $\mathbb{Q}[x]$.

Todistus. Olkoon

$$a(x) = b(x)c(x) \in \mathbb{Z}[x] \tag{6.87}$$

eli

$$a_0 + a_1 x + \ldots + a_A x^A = (b_0 + b_1 x + \ldots + b_B x^B)(c_0 + \ldots + c_C x^C) \tag{6.88}$$

ja

$$B = \deg b(x) \geq 1, \;\; C = \deg c(x) \geq 1, \quad B + C = A. \tag{6.89}$$

Nyt

$$p | a_0 = b_0 c_0, \quad p^2 \nmid a_0 \quad \Rightarrow \quad \text{joko} \quad p | b_0 \quad \text{tai} \quad p | c_0. \tag{6.90}$$

Tarkastellaan tapaus

$$p|b_0 \quad \text{ja} \quad p \not| c_0. \tag{6.91}$$

Koska

$$p|a_1 = b_0c_1 + b_1c_0, \quad \Rightarrow \quad p|b_1 \tag{6.92}$$

...

$$p|a_B = b_0c_B + \ldots + b_Bc_0, \quad \Rightarrow \quad p|b_B. \tag{6.93}$$

Mutta

$$a_A = b_Bc_C, \quad \Rightarrow \quad p|a_A. \tag{6.94}$$

Ristiriita. □

Lause 27

Olkoon

$$a(x) = a_0 + a_1 x + \ldots + a_A x^A \in \mathbb{Z}[x]$$

ja

$$a(r/s) = 0, \quad r, s \in \mathbb{Z}, \quad r \perp s, \tag{6.95}$$

tällöin

$$r | a_0, \quad s | a_A, \tag{6.96}$$

Tämän avulla voidaan etsiä polynomin mahdolliset rationaali-nollakohdat.

Todistus. Yhtälö (6.95) on yhtäpitävää yhtälön

$$s^A a_0 + s^{A-1} r a_1 + \ldots + s r^{A-1} a_{A-1} + r^A a_A = 0 \tag{6.97}$$

kanssa. Koska $r \perp s$, niin välttämättä $r | a_0$ ja $s | a_A$. □

Lause 28

Olkoon K kunta, $p(x) \in K[x]$, $p(x) \in J_{K[x]}$, $\deg p(x) = d$ ja $k \in K$. Tällöin

$$p^*(x) = x^d p(1/x) \in J_{K[x]}, \quad \overrightarrow{p}_k(x) = p(x+k) \in J_{K[x]}. \tag{6.98}$$

Esimerkki 20

Tarkastellaan polynomin

$$a(x) = 4x^3 - 2x^2 + 3x + 5 \in \mathbb{Z}[x] \tag{6.99}$$

tekijöihinjakoa. Jos 3. asteen polynomi jakaantuu, niin sillä on ainakin yksi 1. asteen tekijä, joten

$$a(x) = b(x)c(x), \quad \deg b(x) = 1. \tag{6.100}$$

Valitaan $p = 3$ ja otetaan reduktio $\pmod 3$ eli

$$\overline{a}(x) = \overline{b}(x)\overline{c}(x) \quad \in \mathbb{Z}_3[x], \quad \deg \overline{b}(x) = 1. \tag{6.101}$$

Tällöin

$$\overline{b}(x) \underset{\mathbb{Z}_3[x]}{\mid} \overline{a}(x) = x^3 + x^2 + 2, \quad \deg \overline{b}(x) = 1. \tag{6.102}$$

Lauseen 16 nojalla polynomilla $\overline{a}(x)$ on nollakohta kunnassa $\mathbb{Z}_3$.

Mutta

$$\bar{a}(0) = 2, \quad \bar{a}(1) = 1, \quad \bar{a}(2) = 2. \tag{6.103}$$

Ristiriita. Siten $a(x)$ on jaoton polynomirenkaassa $\mathbb{Z}[x]$ ja edelleen myös renkaassa $\mathbb{Q}[x]$.

Esimerkki 21

Eisensteinin kriteerin, $p = 7$, nojalla

$$a(x) = 7 + 7x - 14x^3 + 2x^5 \in J_{\mathbb{Q}[x]}. \tag{6.104}$$

Käyttämällä lausetta 28 saadaan

$$b(x) = x^5 a(1/x) = 2 - 14x^2 + 7x^4 + 7x^5 \in J_{\mathbb{Q}[x]}; \tag{6.105}$$

$$b(x-1) = 2 - 14(x-1)^2 + 7(x-1)^4 + 7(x-1)^5 \in J_{\mathbb{Q}[x]}; \tag{6.106}$$

Esimerkki 22

Olkoon $p \in \mathbb{P}$. Tällöin

$$a(x) = 1 + x + x^2 + \ldots + x^{p-1} \in J_{\mathbb{Q}[x]}. \tag{6.107}$$

Todistus. Aluksi saadaan

$$a(x) = \frac{x^p - 1}{x - 1}, \tag{6.108}$$

mihin sijoitetaan $x = t + 1$. Tällöin

$$a(x) = a(t+1) = \frac{(t+1)^p - 1}{t} = t^{p-1} + \binom{p}{p-1} t^{t-2} + \ldots + \binom{p}{2} t + \binom{p}{1}. \tag{6.109}$$

Lukuteorian perusteet kurssin nojalla

$$p \left| \binom{p}{k} \right. \quad \forall\ 1 \leq k \leq p-1. \tag{6.110}$$

Nyt Eisensteinen kriteerin ehdot ovat voimassa, joten
$a(t+1)$ on jaoton ja siten myös $a(x)$ on jaoton polynomirenkaassa $\mathbb{Q}[x]$.

Reducibility in $\mathbb{C}[x]$ and $\mathbb{R}[x]$

Let

$$a(x) = a_0 + a_1 x + \ldots + a_A x^A \in \mathbb{C}[x], \quad \deg a(x) \geq 1, \tag{6.111}$$

then

$$a(x) = a_A(x - \alpha_1) \cdots (x - \alpha_A), \quad \alpha_1, \ldots, \alpha_A \in \mathbb{C} \tag{6.112}$$

by the Fundamental Theorem of Algebra. Consider now

$$a(x) = a_0 + a_1 x + \ldots + a_A x^A \in \mathbb{R}[x], \quad \deg a(x) \geq 1. \tag{6.113}$$

Then we have

$$a(z) = 0 \quad \Leftrightarrow \quad a(\overline{z}) = 0 \tag{6.114}$$

because

$$0 = \overline{a(z)} = a_0 + a_1 \overline{z} + \ldots + a_A \overline{z}^A. \tag{6.115}$$

Therefore, non-real complex roots exist in pairs:
$\beta_j \neq \overline{\beta_j}$, $\beta_j \in \{\alpha_1, \ldots, \alpha_A\}$.

Reducibility in $\mathbb{C}[x]$ and $\mathbb{R}[x]$

Consequently

$$a(x) = a_A(x-\alpha_1)\cdots(x-\alpha_h)\cdot(x-\beta_1)(x-\overline{\beta_1})\cdots(x-\beta_k)(x-\overline{\beta_k}),$$
$$\alpha_1,\ldots,\alpha_h \in \mathbb{R}, \quad \beta_1,\ldots,\beta_k \in \mathbb{C}\setminus\mathbb{R}, \quad h+2k=A. \quad (6.116)$$

Write $\beta = a+ib$, where $a, b \in \mathbb{R}$ and compute

$$(x-\beta_1)(x-\overline{\beta_1}) = (x-a-ib)(x-a+ib) = (x-a)^2+b^2 \in \mathbb{R}[x]. \quad (6.117)$$

Hence

$$a(x) = a_A(x-\alpha_1)\cdots(x-\alpha_h)\cdot((x-a_1)^2+b_1^2)\cdots((x-a_k)^2+b_k^2),$$
$$(x-\alpha_1),\ldots,(x-\alpha_h),((x-a_1)^2+b_1^2),\ldots,((x-a_k)^2+b_k^2) \in \mathbb{R}[x].$$

In other words: Any non-constant polynomial with real coefficients, factors in $\mathbb{R}[x]$ into first and second degree polynomials.