**§ 1. Žiedo apibrėžimas**

**Apibrėžimas 1.**

Netuščia aibė , kurioje apibrėžtos dvi algebrinės operacijos „+“ ir „ vadinama žiedu, jei

1. Galioja asociatyvumas sudėties atžvilgiu, tai yra

Visiems :

1. Egzistuoja neutralusis elementas sudėties atžvilgiu vadinamas :
2. Kiekvienam , egzistuoja priešingas elementas , toks, kad
3. Galioja komutatyvumas sudėties atžvilgiu, tai yra

Visiems :

1. Galioja asociatyvumas daugybos atžvilgiu, tai yra

Visiems :

1. Galioja distributyvumo dėsnis, tai yra

Visiems

ir

Apibrėžta algebrinė struktūra žymima .

**Pastaba:** Duotojo apibrėžimo 1-4 sąlygas galime pakeisti sakydami, kad žiedas yra Abelio grupė sudėties atžvilgiu.

Be to, jei žiedas be apibrėžtųjų sąlygų tenkina ir komutatyvumo dėsnį daugybos atžvilgiu, jis vadinamas **komutatyviuoju žiedu**.

Iš pateikto apibrėžimo, aišku, kad žiedas nesudaro grupės daugybos atžvilgiu, nes šioje struktūroje gali neegzistuoti neutralusis elementas daugybos atžvilgiu, kuris vadinamas vienetu (žym. 1). Be to, ne kiekvienas žiedo elementas privalo turėti ir atvirkštinį elementą.

**Apibrėžimas 2.**

Komutatyvus žiedas, kuris turi neutralųjį elementą (vienetą) vadinamas žiedu su vienetu.

**Apibrėžimas 3.**

Komutatyvus žiedas su vienetu, kurio kiekvienas elementas, išskyrus 0 turi atvirkštinį elementą vadinamas kūnu.

**Pvz.: 1.**

Struktūros 1) ; 2) ; 3) ; 4) - yra žiedai. Be to, 2-4 struktūros yra taip pat ir kūnai. Struktūra yra žiedas su vienetu, tačiau nėra kūnas (jame nė vienas elementas neturi atvirkštinio elemento).

**Pvz.: 2.**

Struktūra yra žiedas, tačiau jame nėra vieneto.

**Teiginys.** Visiems žiedo elementams teisinga lygybė

**Įrodymas**

Turime, kad

čia .

**§ 2. Žiedo nulio dalikiai**

**Apibrėžimas 4.**

Komutatyvaus žiedo elementas vadinamas žiedo nulio dalikliu, jei egzistuoja žiedo elementas , kad .

Žiedas, neturintis nulio daliklių vadinamas sveikumo arba integralumo sritimi.

Sveikųjų skaičių žiedas neturi nulio daliklių, tačiau kai kurie žiedai jų gali ir turėti.

Imkime ir apibrėžkime klasę

Šių klasių aibę pažymėkime .

Šioje aibėje tarp klasių apibrėšime sudėties ir daugybos operacijas, tokiu būdu:

+

Tuomet struktūra - žiedas.

Pastebėkime, kad žiedą sudaro skirtinga klasė

Klasė

, todėl ir t.t. šis žiedas turi vienetą.

**Pvz.: 3.** Panagrinėkime du žiedus ir . Žiede nėra nulio daliklių, be to jame kiekvienas elementas turi atvirkštinį

Klasė atvirkštinė klasei , o klasė atvirkštinė pati sau. Taigi, struktūra ne tik žiedas, bet ir kūnas. Tuo tarpu žiede turime, kad

Taigi, klasė atvirkštinė pati sau, o klasė atvirkštinės neturi. Be to ši klasė yra žiedo nulio daliklis.

**Teorema 1.** Žiedas yra kūnas tada ir tik tada, kai yra pirminis skaičius.

**Įrodymas.**

**Būtinumas.**

Tarkime, kad yra kūnas ir nėra pirminis skaičius. Tuomet, . Taigi žiede egzistuoja klasės ir , kad . Taigi, elementai ir yra žiedo nulio dalikliai. Tačiau, jei struktūra yra kūnas, kiekvienas jo elementas turi turėti atvirkštinį elementą, todėl egzistuoja klasės ir , kad

ir

Tuomet,

Prieštara, nes žiede klasės ir skirtingos.

Būtinumas įrodytas.

**Pakankamumas.**

Tarkime, kad yra pirminis skaičius. Imkime bet kokią klasę . Kadangi, nedalija () iš mažosios Ferma teoremos turime, kad

Iš čia matome, kad . Taigi kiekviena klasė turi atvirkštinę klasę.

Teorema įrodyta.

**§ 3. Žiedo idealai**

**Apibrėžimas 5.**

Netuščia aibė vadinama komutatyvaus žiedo idealu, jei

1. Visiems
2. Kiekvienam ir

Tegul, , apibrėžkime aibę

**Teorema 2.** Aibė yra žiedo idealas.

**Įrodymas.**

Jei ir , tai

Taip pat, jei ir , tai . Teorema įrodyta.

Idealas vadinamas idealu generuotu elemento .

**Apibrėžimas 6.**

Idealas generuotas vieno žiedo elemento vadinamas pagrindiniu žiedo idealu.

**Pvz.: 4.** Imkime žiedą. Jo idealas yra generuotas elemento 2 ir yra pagrindinis. Yra įrodoma, kad žiedo visi idealai yra pagrindiniai.

**Teorema 3.** Jei struktūra yra kūnas, tai jo idealai yra tik ir .

**Įrodymas.**

Kadangi, ir

bei

kiekvienam ir turime, kad

tai pagal 5 apibrėžimą gauname, kad yra idealas.

Tarkime, kad yra bet koks nenulinis idealas. Tegul, ir . Turime, kad , todėl . Imkime bet kokį , tada .

Tačiau, pagal idealo apibrėžimą. Taigi, . Teorema įrodyta.

Tarkime, ir - žiedo idealai. Apibrėžkime sumą:

Tuomet, yra taip pat žiedo idealas.

Galime apibrėžti idealų sumą ir iš dėmenų. Tarkime, kad ; ;...; yra žiedo idealai, tuomet suma

yra to paties žiedo idealas.

Tarkime, kad turime žiedo idealus: ; ; ...; generuotus elementų ;;...;. Tuomet, taip pat bus žiedo idealas. Elementai ;;...; vadinami šio idealo sudaromosiomis, o pats idealas generuotu elementų ;;...;.

Apibrėšime ekvivalentumo klasę pagal idealą. Tegul, ir yra žiedo idealas, tuomet aibė

vadinama ekvivalentumo klase pagal idealą .

Apibrėžkime sudėties ir daugybos operacijas tarp šių ekvivalentumo klasių:

ir

Dabar apibrėšime šių klasių faktoraibę

Struktūra yra žiedas. Šis žiedas vadinamas žiedo faktoržiedu pagal idealą .

**Pvz.: 5.** Imkime žiedą ir jo pagrindinį idealą , tuomet

**Pvz.: 6.** Apibrėžkime aibę

Ši aibė bus žiedas . Šis žiedas vadinamas **Gauso sveikųjų skaičių žiedu.**

Nagrinėkime šio žiedo pagrindinį idealą

Rasime Gauso sveikųjų skaičių žiedo faktoržiedą pagal šį idealą.

Imkime skaičių . Kadangi,

ir

Tai reiškia, kad

Tai gauname, kad

Tokiu būdu, bet koks elementas priklauso vienai iš dviejų klasių arba .

Klasės nesikerta ir neturi bendrų elementų, todėl

.