Mana personīgā lapa – šeit.

Adrese komentāriem: Karlis.Podnieks@lu.lv

Abstraktā algebra:

Lauki, gredzeni un grupas

Kārlis Podnieks, LU profesors

Lekcijas

Literatūra

[1] E-kursa materiāli (autors: asoc.prof. Juris Smotrovs).

[2] **A. G. Kurošs.** Vispārīgās algebras kurss. Nauka, Maskava, 1971 (vai cita gada izdevums). Pieejama tiešsaistē šeit (krievu valodā).

[3] WolframAlpha Wikipedia – aprēķiniem tiešsaistē.

Abstraktā algebra – lauki

To noskaņu, kas noved pie abstraktās algebras, labi varēja just visu mūsu algebras studēšanas laiku (atcerēsimies "zaļos" secinājumus):

a) **Visa** mūsu attīstītā teorija pilnībā darbojas tikai **komplekso skaitļu pasaulē**. Šajā pasaulē var ar Gausa metodi risināt jebkuras lineāru vienādojumu sistēmas, rēķināt determinantus, iegūt *nxn* matricas A inverso matricu A^{-1}, dalīt polinomus ar atlikumu, atrast polinomu LKD, var uzbūvēt polinomu ar iepriekš uzdotām vērtībām. Bet papildus tam, te (komplekso skaitļu pasaulē) **katram polinomam eksistē saknes un katru polinomu var sadalīt lineāros reizinātajos.**

b) Liela daļa no mūsu teorijas der arī **reālo skaitļu pasaulē**. Neizejot no šīs pasaules, var ar Gausa metodi risināt jebkuras lineāru vienādojumu sistēmas ar reāliem koeficientiem, rēķināt determinantus, iegūt *nxn* matricas A inverso matricu A^{-1}, dalīt polinomus ar atlikumu, atrast polinomu LKD, var uzbūvēt polinomu ar iepriekš uzdotām reālām vērtībām. Bet te **ne katram polinomam ar reāliem koeficientiem eksistē reālas saknes** un ne katru polinomu var sadalīt lineāros reizinātajos (atceramies $x^2+1=(x+i)(x-i)$). Tiesa, izvilkt saknes no pozitīviem reāliem skaitļiem šajā pasaulē mēs tomēr varam (piemēram, $\sqrt{2}$).

c) Vēl mazāka, bet tomēr ievērojama daļa mūsu teorijas der arī **racionālo skaitļu pasaulē**. Neizejot no šīs pasaules, var ar Gausa metodi risināt jebkuras lineāru

vienādojumu sistēmas ar racionāliem koeficientiem, rēķināt determinantus, iegūt *nxn* matricas A inverso matricu A^{-1}, dalīt polinomus ar atlikumu, atrast polinomu LKD, var uzbūvēt polinomu ar iepriekš uzdotām racionālām vērtībām. Bet te **ne vienmēr var izvilkt saknes** pat no pozitīviem skaitļiem (atceramies, ka $\sqrt{2}$ nav racionāls skaitlis),

d) Vēl mazāka mūsu teorijas daļa derēs **veselo skaitļu pasaulē**. **Tas tāpēc, ka ne vienmēr ir iespējama veselo skaitļu dalīšana bez atlikuma.** Lineāru vienādojumu sistēmu (ar veseliem koeficientiem) atrisinājumi parasti būs daļskaitļi (t.i. "ne šīs pasaules" skaitļi), ne vienmēr varēs iegūt *nxn* matricas A inverso matricu A^{-1} (tajā bieži parādīsies daļskaitļi). Polinomu dalīšanas, LKD un Lagranža algoritmu rezultātos iegūstamo polinomu koeficienti arī parasti būs daļskaitļi. Bet rēķināt determinantus te tomēr varam (ar definīcijas formulām, kur neizmanto dalīšanu, ne ar Gausa metodi, kur dalīšana jāizmanto).

Tā esam aplūkojuši 4 dažādas **skaitļu sistēmas ("pasaules")**.

Kādas tad ir tās minimālās **skaitļu sistēmas** īpašības, lai uz tās pamata varētu risināt lineāru vienādojumu sistēmas, veidot "labu" matricu algebru un "labu" polinomu algebru?

"Laba" polinomu algebra – tāda, kurā polinomus vismaz var dalīt ar atlikumu, diviem polinomiem var aprēķināt LKD, var uzbūvēt polinomu ar iepriekš uzdotām vērtībām. "Laba" matricu algebra – tāda, kur nesingulārai *nxn* matricai var aprēķināt inverso matricu.

Ja paskatāmies atpakaļ ("zaļie secinājumi"), tad redzam, ka "labajās" algebrās ir būtiski izmantotas šādas skaitļu sistēmas īpašības:

a) Sistēmā ir asociatīva un komutatīva skaitļu saskaitīšanas operācija, ir skaitlis 0 un vienmēr var izpildīt atņemšanu.

b) Sistēmā ir asociatīva un komutatīva skaitļu reizināšanas operācija, ir skaitlis 1, un **vienmēr var izpildīt dalīšanu** (izņemot dalīšanu ar 0).

c) Reizināšana ir distributīva pret saskaitīšanu: a(b+c)=ab+ac.

Šādas skaitļu sistēmas matemātiķi sauc par

laukiem. T.i. “labas algebras” var būvēt tikai skaitļu laukiem.

Lauku piemēri:

Komplekso skaitļu lauks C. Komplekso polinomu “algebra” (gredzens) C[x]. Komplekso *nxn* matricu “algebra” (gredzens) $M_n[C]$.

Reālo skaitļu lauks R. Reālo polinomu gredzens R[x]. Reālo *nxn* matricu gredzens $M_n[R]$.

Racionālo skaitļu lauks Q. Racionālo polinomu gredzens Q[x]. Racionālo *nxn* matricu gredzens $M_n[Q]$.

Tie ir 3 dažādi lauki.

Veselie skaitļi (kopa Z) lauku neveido, jo tiem ne vienmēr var izpildīt dalīšanu ar nenulles skaitli. Kopa Z pati ir tikai gredzens!

Abstraktā algebra – gredzeni

Šajā kursā esam apguvuši divas algebriskas struktūras, kas sastāv nevis no skaitļiem, bet no sarežģītākiem objektiem – matricām un polinomiem.

Arī šiem objektiem mums ir definētas saskaitīšanas un reizināšanas operācijas. Bet tām piemīt ne visas īpašības, kas minētas **lauka** definīcijā.

Tāpat kā veselo skaitļu gadījumā:

a) polinomu dalīšana bez atlikuma ļoti bieži nav iespējama;

b) matricu dalīšana nav iespējama arī tad, ja dalītājs nav nulles matrica, bet tās determinants ir nulle.

c) Un matricām ir vēl viena īpatnība – matricu reizināšana **nav komutatīva**: bieži vien, $AB \neq BA$.

Tātad

veselie skaitļi,

polinomi (kompleksie, reālie, racionālie),

nxn matricas (kompleksās, reālās, racionālās),

kaut arī tur ir saskaitīšanas, atņemšanas un reizināšanas operācijas, tomēr neveido laukus, tās ir līdzīgas laukiem, bet tomēr savādākas ("vājākas") objektu sistēmas. Šādas sistēmas sauc par **gredzeniem**.

Katrs lauks ir arī gredzens, bet ne otrādi, t.i. prasības gredzenam ir "mīkstākas" nekā laukam – gredzenā dalīšanai ar "nenulli" **ne vienmēr** ir jābūt izpildāmai, un reizināšanai **nav obligāti** jābūt komutatīvai.

Uzrakstīsim tagad stingri formālu gredzenu definīciju, kā tas ir pieņemts abstraktajā algebrā:

[Grāmatās var sastapt arī savādākas gredzena definīcijas, bet tās visas ir ekvivalentas zemāk dotajai.]

Gredzenu veido kāda **objektu kopa** G un divas divvietīgas **operācijas** šajā kopā: + un *, kas vienmēr ir izpildāmas (t.i. ja a, b pieder G, tad a+b un a*b eksistē un pieder G), un kam piemīt 7 īpašības, ko sauc arī par **gredzena aksiomām** (sk. tālāk).

[Ja tā ir vieglāk, "objektu kopas G" vietā domājiet par veselajiem skaitļiem.]

Piemēri.

Komplekso polinomu gredzens C[x].

G=visi polinomi ar kompleksiem koeficientiem, kuru vienīgais mainīgais ir x, piemēram, $x^3-3x^2+(2+3i)x-7$. Ir definētas polinomu saskaitīšanas un reizināšanas operācijas.

Komplekso 2x2 matricu gredzens $M_2[C]$.

G= visas 2x2 matricas ar kompleksiem elementiem, piemēram, $\begin{pmatrix} 1+i & 1-i \\ 2+3i & 5-3i \end{pmatrix}$.

Ir definētas matricu saskaitīšanas un reizināšanas operācijas (pēdējā nav komutatīva).

T0. Ja $x=y$, tad jebkuram a:

$$a+x=a+y\,;\; x+a=y+a\,;$$
$$a*x=a*y\,;\; x*a=y*a\,.$$

Gredzena aksiomas:

1. Saskaitīšana ir *asociatīva*:

$$\mathbf{(a+b)+c=a+(b+c)}.$$

2. Saskaitīšana ir *komutatīva*:

$$\mathbf{a+b=b+a}.$$

3. Kopā G eksistē *nulles elements* 0: visiem a, $\mathbf{0+a=a}$.

T1. Jebkurā gredzenā nulles elements ir tikai viens (tāpēc tiešām varam to apzīmēt ar 0).

Pierādījums (to esam 3 reizes redzējuši jau agrāk: matricām, kompleksajiem skaitļiem, polinomiem, bet tagad vispārinām: izmantojam tikai divas aksiomas). Izmantosim tikai 2. un 3. aksiomu.

Saskaņā ar 3.aksiomu, vismaz viena nulle gredzenā eksistē.

Pieņemsim, ka mums gredzenā ir divas nulles O_1, O_2 : tad visiem a izpildās $O_1+a=a$; $O_2+a=a$.

Aplūkosim izteiksmi: O_1+O_2 . Pirmkārt, $O_1+O_2=O_2$. Otrkārt, saskaņā ar 2.aksiomu, $O_1+O_2=O_2+O_1$. Bet $O_2+O_1=O_1$. Tātad $O_1=O_2$. Q.E.D.

4.aksioma. Katram a eksistē *pretējais elements*

b: **a+b=0**.

T2. Jebkurā gredzenā katram a pretējais elements ir tikai viens (tāpēc varam to apzīmēt ar $-a$).

Pierādījums (jau 3 reizes redzēts...). Izmantosim tikai aksiomas 1, 2, 3, 4 un teorēmu T1. Vismaz viens pretējais elements eksistē (4.aksioma). Pieņemsim, ka elementam a ir divi pretējie:

$a+a_1=0\,;a+a_2=0$ un aplūkosim izteiksmi

$$(a+a_1)+a_2=0+a_2=a_2;$$

$$(a+a_1)+a_2=a+(a_1+a_2)=a+(a_2+a_1)=(a+a_2)+a_1=0+a_1=a_1.$$

Tātad $a_1=a_2$. Q.E.D.

T2'. Jebkurā gredzenā: $-(-a)=a$.

Pierādījums. Izmantosim aksiomas 1-4 un T2: $a+(-a)=0$. Tātad a ir $-a$ vienīgais pretējais, tāpēc $-(-a)=a$. Q.E.D.

Tagad varam pierādīt vēl vairākas teorēmas, kas der **jebkuram gredzenam**.

T3. Jebkurā gredzenā, katriem a, b vienādojumam $x+b=a$ ir viens un tikai viens atrisinājums $x=a+(-b)$.

Pierādījums. Izmantosim aksiomas 1-4 u T1-2. Pārbaudīsim, ka $x=a+(-b)$ der par atrisinājumu. Pēc tam aplūkosim vienādojumu: $x+b=a$, pieskaitīsim abām pusēm $-b$:

Tagad mums ir arī **atņemšanas operācija**: $a+(-b)$

mēs turpmāk apzīmēsim ar $a-b$.

Tā kā x+b=a tad un tikai tad, ja x=$a-b$:

T3'. Jebkurā gredzenā atņemšanas operācija ir saskaitīšanas **apgrieztā** operācija: $(a-b)+b=a$.

T3'' (par saīsināšanu vienādības abās pusēs.). Jebkurā gredzenā, **ja x+a=y+a, tad x=y.**

Pierādījums. x+a+(−a)=y+a+(−a)=x+0=y+0=x=y.

T4. Jebkurā gredzenā, $a-a=0$.

Pierādījums. Izmantosim T3: $a-a$ ir definēts kā $a+(-a)$, bet (T2) $-a$ ir a vienīgais pretējais elements,tātad a+(−a)=0. Q.E.D.

T4'. Jebkurā gredzenā, ja $a \neq 0$, tad $a+a \neq a$.

Pierādījums. Ja a+a=a, tad a+a+(-a)=a+(-a). Kreisā puse ir a, bet labā – 0. Tātad a=0. Q.E.D.

Tālāk seko reizināšanas aksiomas:

5.aksioma. Reizināšana ir *asociatīva*: **(a*b)*c=a*(b*c)**.

Bet reizināšanai ***nav obligāti jābūt komutatīvai*!** Tādas aksiomas nav!

6.aksioma. Kopā G eksistē *elements-vienīnieks* 1: visiem a, **1*a=a*1=a**.

Kāpēc tagad bija jāraksta 1*a=a*1=a nevis tikai 1*a=a? Tāpēc, ka (gredzenā) **reizināšana var nebūt komutatīva**, un tad ar 1*a=a nepietiek.

T5. Jebkurā gredzenā elements-vienīnieks ir tikai viens (tāpēc varam to apzīmēt ar 1).

Pierādījums (jau redzēts 3 reizes...). Izmantosim tikai aksiomu 6, kas garantē, ka vienīnieks eksistē. Ja mums ir divi vienīnieki:

$1_1 * a = a; a * 1_2 = a$, tad $1_1 * 1_2 = 1_2 = 1_1$. Q.E.D.

7.aksioma. Distributīvie likumi (divi!):

a*(b+c)=(a*b)+(a*c);

(b+c)*a=(b*a)+(c*a).

Kāpēc divi? Tāpēc, ka (gredzenā) reizināšana var nebūt komutatīva.

Brīdinājums! Gredzena aksiomas **negarantē**,

a) ka no $a \neq 0$, a*x=a*y (vai x*a=y*a), seko x=y;

b) ka no a*b=0 seko a=0 vai b=0.

Lai pierādītu teorēmas, kas der **jebkuram gredzenam**, ir jāiemācās pierādīt teorēmas, izmantojot tikai gredzenu aksiomas 1-7 un ar tām jau iepriekš pierādītās teorēmas **un neko citu**!

T6. Jebkurā gredzenā jebkuram *a*: *0*a=a*0=0*.

Pierādījums. Aplūkosim izteiksmes $(a+0)*a; a*(a+0)$ un izmantosim 7.aksiomu (abus distributīvos likumus):

T6'. Jebkurā gredzenā,

a*(b−c)=a*b−a*c; (b−c)*a=b*a−c*a.

Pierādiet paši: $b-c=x$; ***tas ir*** $: x+c=b$; $a*(x+c)=a*b$;
A **7**$: a*x+a*c=a*b$; ***tas ir*** $a*x=a*b-a*c$.

Triviālais gredzens sastāv no viena elementa {0}, kam 0+0=0, 0*0=0. Visas 7 gredzena aksiomas te izpildās. [**Pārbaudīsim!**] Šajā gredzenā 0=1.

T7. Ja gredzenā ir vismaz divi dažādi elementi, tad 0≠1.

Pierādījums. No pretējā: ja gredzenā ir kāds x≠0, bet 0=1, tad x*0=x*1. Bet x*0=0 (T6) un x*1=x (T5), tātad x=0. Pretruna.

Gredzenā netiek prasīts, lai **dalīšana** būtu vienmēr izpildāma, t.i. vienādojumi a*x=b, x*a=b **ne vienmēr** būs atrisināmi.

T8. Nenulles elementa **dalīšana ar nulli nav iespējama** nevienā netriviālā gredzenā.

Pierādījums. 0*x=x*0=0, tātad ja b≠0, tad vienādojumiem 0*x=b, x*0=b nav atrisinājumu. Q.E.D.

Vēsture – sk. šādus Wikipedia rakstus: Ring (mathematics). Gredzenus pirmais ieveda Richard Dedekind 1871.gadā (termins: *Order-Modul*), David Hilbert, 1892.gadā (termins: *Ring*).

Sk. Wikipedia arī Ring theory (tur – arī par atšķirībām dažādās gredzenu definīcijās), Noncommutative ring (Kurošs savā grāmatā tādus nemaz nepieļauj), Commutative ring.

Secinājumi.

a) **Veselie skaitļi** veido **komutatīvu gredzenu** Z, bet neveido lauku (sk. tālāk).

b) Jebkuram laukam K, **polinomi** ar

koeficientiem no K veido **komutatīvu gredzenu** K[x], bet neveido lauku (sk. tālāk).

c) Jebkuram laukam K un naturālam skaitlim $n \geq 2$, n x n **matricas** ar elementiem no K veido **nekomutatīvu gredzenu** $M_n[K]$, bet neveido lauku (sk. tālāk).

T9. Jebkurā gredzenā:

$$(-a)*b=a*(-b)=-(a*b);$$
$$(-a)*(-b)=a*b.$$

Pierādījums. Aplūkosim izteiksmes: (−a)*b+a*b; a*(−b)+a*b un izmantosim distributīvos likumus. Un beidzot, kā pierādīt (−a)*(−b)=a*b? Aplūkosim izteiksmi (−a)*(−b)+(−a)*b=(−a)*0=0. Tātad −a*b ir (−a)*(−b) pretējais un (−a)*(−b)=a*b. Pabeidziet paši. Q.E.D.

Gredzenā G, n saskaitāmo summu

$$a+a+\ldots+a$$

saīsināti varam apzīmēt ar na (n – naturāls skaitlis), piemēram, $2a=a+a$, $3a=a+a+a$. **Bet tie nav gredzena reizinājumi!** (Jo naturālie skaitļi parasti nav gredzena G elementi.)

T10. Jebkurā gredzenā: n(−a) = −(na).

Pierādījums. Aplūkosim izteiksmi: n(−a)+na. Pabeidziet paši.

Tātad varam vienoties ka $(-n)a$ nozīmē $-(na)$, un tāpēc na mums tagad ir definēts *jebkuram veselam* skaitlim n. Tāpat, vienosimies, ka 0a=0 (sarkanā nulle gredzenam nepieder!)

T10'. Jebkurā gredzenā G, visiem $a \in G$ un visiem veseliem skaitļiem m, n:

$$ma + na = (m+n)a;$$

$$m(na)=(mn)a.$$

[Pierādiet paši – nekas vairāk kā gredzena aksiomas te nav vajadzīgs.]

Operācijas m+n, mn šeit ir iezīmētas sarkanas, jo tās nav gredzena operācijas. Tās ir operācijas ar veseliem skaitļiem.

Reizinājumu a*a*...*a varam apzīmēt ar a^n (n ir naturāls skaitlis), piemēram, a^2, a^3,...

T11. $(-a)^n=a^n$ pāra skaitlim n, un

$(-a)^n= -a^n$ nepāra skaitlim n.

[Pierādiet paši – nekas vairāk kā gredzena aksiomas te nav vajadzīgs. Izmantojiet T9.]

T11'. Jebkurā gredzenā:

$$a^m * a^n = a^{m+n};\ (a^m)^n=a^{mn}.$$

[Pierādiet paši.]

Operācijas m+n, mn šeit iezīmētas sarkanas, jo tās nav gredzena operācijas. Tās ir operācijas ar veseliem nenegatīviem skaitļiem.

Apgrieztie (inversie) elementi

Gredzena elementam a mēs varam nodefinēt *apgriezto* elementu (jeb inverso elementu) kā vienādojumu xa=ax=1 atrisinājumu.

Atcerēsimies inversās matricas: $A\,A^{-1}=A^{-1}=E_n$.

Gredzenos apgrieztais elements nereti eksistē ne visiem elementiem.

Atcerēsimies inversās matricas: ja $det(A)\neq 0$, tad A^{-1} neeksistē.

Tas pats polinomiem: 1/P eksistē tikai null-tās pakāpes polinomiem.

Un veselajiem skaitļiem: x^{-1} ir vesels skaitlis tikai ja x=1 vai x=– 1.

T12. Ja gredzena elementam *a* eksistē apgrieztais elements, tad tāds ir viens vienīgs (un tāpēc mēs varam to apzīmēt ar a^{-1}).

Pierādījums. Rīkojamies tieši tā, kā to darījām ar matricām: aplūkojam izteiksmi $(a_1 a)a_2 = a_1(a\,a_2)$. Pabeidziet paši.

Piemērs: *n*x*n* matricu gredzens $M_n[K]$, kur n>1 un K – jebkurš lauks (piemēram, komplekso skaitļu lauks). Matricai A inversā matrica eksistē (un tad ir vienīgā) tad un tikai tad, ja det(A) nav nulle.

Tāpat kā matricām, jebkurā (potenciāli nekomutatīvā) gredzenā varam ievest **divas dalīšanas** – kreiso un labējo:

a*x=b; $x = a^{-1} * b$ un

x*a=b; $x = b * a^{-1}$ (ja a^{-1} eksistē).

T12'. Ja a^{-1} un b^{-1} eksistē, tad eksistē arī $(a*b)^{-1}$ un $(a*b)^{-1} = b^{-1}a^{-1}$.

Pierādījums. Atceramies, kā to darījām matricām.

T12''. Ja a^{-1} eksistē, tad no $a*x = a*y$ vai $x*a = y*a$ seko $x = y$.

Pierādiet paši.

T12'''. Vienādība $(a+b)^2 = a^2 + 2a*b + b^2$ vai $(a-b)*(a+b) = a^2 - b^2$ izpildās tad un tikai tad, ja $a*b = b*a$. Tātad visiem *a, b* tās izpildās tikai **komutatīvā** gredzenā.

Pierādiet paši.

Nulles dalītāji

Esam pieraduši pie šādas skaitļu īpašības:

Ja a*b=0, tad a=0 vai b=0.

Bet **no gredzena definīcijas šāda īpašība neseko**. Tāpēc gredzenā G divus *nenulles* elementus a, b, kam a*b=0, sauc par **nulles dalītājiem**.

T13. Nulles dalītājam neeksistē apgrieztais elements.

Pierādījums. Vienādību $a*b=0$ pareizinām ar *a* inverso: $a^{-1}*a*b=1*b=b=0$. Vai arī $a*b*b^{-1}=a*1=a=0$. Q.E.D.

Piemēri.

Veselo skaitļu gredzenā Z **nav nulles dalītāju**: no mn=0 seko, ka m=0 vai n=0.

Jebkuram laukam K polinomu gredzenā P[K] **nav nulles dalītāju**. [Divu nenulles polinomu reizinājums ir nenulles polinoms.]

Teorēma. Ja $n\geq 2$, tad jebkuram laukam K, *n*x*n* matricu gredzenā $M_n[K]$ **eksistē nulles dalītāji.**

Pierādījums. Piemēram, pie n=2 (laukā K, 0≠1, sk. tālāk):

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} .$$

Gadījumu, kad n>2, pierādiet paši.

Uzdevums (i-iespēja). Gredzenā $M_2[R]$ atrodiet **visus** nulles dalītājus.

Vēlreiz par laukiem

Vēsture – sk. Wikipedia rakstus Field (mathematics).

Richard Dedekind 1871.gadā (termins *Körper*, vācieši un franči laukus tā sauc joprojām), Eliakim Hastings Moore, 1893.gadā (termins *field*).

Sk. arī Wikipedia Field theory (mathematics).

[Grāmatās var sastapt arī savādākas lauka definīcijas, bet tās visas ir ekvivalentas zemāk dotajai.]

Formālo (un precizēto!) **lauka definīciju** iegūsim, ja gredzena definīcijai pievienosim vēl trīs aksiomas:

8.aksioma. Reizināšana ir *komutatīva*: **a*b=b*a**.

9.aksioma. $0 \neq 1$.

10.aksioma. Katram nenulles elementam *a* eksistē *apgrieztais elements b*: **a*b=1**.

Turpmāk, reizināšanas apzīmēšanai zvaigznīti vairs nerakstīsim.

Triviālais gredzens sastāvēja no viena elementa {0}, tajā 0=1.

Triviālais lauks sastāv no diviem elementiem {0, 1}, kam 0+0=**1+1**=0, 0+1=1+0=1, 0*0=0*1=1*0=0, 1*1=1. Visas lauka īpašības te izpildās. [Pārbaudiet paši.]

[1+1=0 te ir vienīgā iespēja, jo T4' saka, ka $1+1 \neq 1$, tātad 1+1=0.]

Vēlāk šo lauku nosauksim par Z_2 (veselo skaitļu saskaitīšana un reizināšana pēc moduļa 2).

T14. Jebkurā laukā katram nenulles elementam *a* apgrieztais elements ir viens un tikai viens (tātad varam apzīmēt to ar a^{-1}).

Pierādījums. *Vienīgums* seko no gredzena aksiomām (T12). *Eksistence* – no 10.aksiomas.

T15. Jebkurā laukā, katriem *a*, b, ja $b \neq 0$, tad vienādojumam $xb=a$ ir viens un tikai viens

atrisinājums $x=ab^{-1}$.

Tāpēc tagad mums ir arī (viena!) **dalīšanas operācija** ab^{-1} , ko varam apzīmēt ar $\frac{a}{b}$.

T16. Jebkurā laukā, dalīšanas operācija ir reizināšanas **apgrieztā** operācija: ja a≠0, tad $\frac{a}{b}b=a$.

Pierādījums. $\frac{a}{b}b=a\,b^{-1}b=a\,1=a$.

T16'. Jebkurā laukā, katram a≠0: $\frac{a}{a}=1$.

Pierādījums. $\frac{a}{a}=a\,a^{-1}=1$.

T16''. $(ab)^{-1}=a^{-1}b^{-1}$.

Pierādījums. $(ab)a^{-1}b^{-1}=(ab)b^{-1}a^{-1}=a(b\,b^{-1})a^{-1}=aa^{-1}=1$.

T17. Jebkurā laukā: ja ab=0, tad a=0 vai b=0, t.i. **laukos nav iespējami nulles dalītāji**.

Pierādiet paši.

T18. Jebkurā laukā vienādību var saīsināt ar kopīgu nenulles reizinātāju: ja ac=bc un c≠0, tad a=b.

Seko no T12'.

Negatīvās pakāpes: ja n>0 un a≠0, tad a^{-n} definējam kā $\frac{1}{a^n}$. Tagad mums a^m ir definēts jebkuram veselam skaitlim *m*.

Operācijas ar daļām – jebkurā laukā ar tām var rīkoties kā pierasts no skolas laikiem:

T18'. $\frac{ab}{c}=\frac{a}{c}b=a\frac{b}{c}$.

Pierādījums. $\frac{ab}{c}=(ab)c^{-1};\frac{a}{c}b=(ac^{-1})b;a\frac{b}{c}=a(bc^{-1})$. Reizināšanas komutativitātes dēl visu trīs izteiksmju vērtības ir vienādas.

T19: $\frac{a}{b}\frac{c}{d}=\frac{ac}{bd};\frac{ac}{bc}=\frac{a}{b}$.

Pierādiet paši.

T20: $\frac{a}{b}=\frac{c}{d}$ tad un tikai tad, ja b un d nav 0, un ad=bc.

Pierādiet paši: reiziniet vai daliet ar *bd*.

T21: $\frac{a}{c}+\frac{b}{c}=\frac{a+b}{c};\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$.

Pierādiet paši: $\frac{a}{c}=ac^{-1}$, utt.

Piemēri

Veselie skaitļi lauku neveido – tos ne vienmēr var dalīt bez atlikuma.

$$Z = \{..., -2, -1, 0, 1, 2, ...\}$$

Bet **Z ir komutatīvs gredzens**! [Tikai jāpārbauda

aksiomu 1-7 izpildīšanās.]

Racionālo skaitļu lauks:

$$Q = \{..., -3/2, -2, -2/3, -1, -1/2, 0, 1/4, 5/6, ...\}.$$

[Tikai jāpārbauda aksiomu 1-10 izpildīšanās.]

Te vienmēr var dalīt bez atlikuma (nevar dalīt tikai ar 0), bet – **ne vienmēr var izvilkt saknes** (piemēram, $\sqrt{2}$ nav racionāls skaitlis).

Reālo skaitļu lauks R:

[Tikai jāpārbauda aksiomu 1-10 izpildīšanās.]

Te jau var vilkt saknes no pozitīviem skaitļiem, konverģentām virknēm eksistē robežas, bet tomēr **ne katru algebrisku vienādojumu var atrisināt** (piemēram, $x^2+1=0$).

Komplekso skaitļu lauks C:

[Tikai jāpārbauda aksiomu 1-10 izpildīšanās. Īstenībā mēs to diezgan rūpīgi savulaik jau izdarījām – atceramies "matemātiķa skatu".]

Te jau var atrisināt jebkuru algebrisku vienādojumu.

Ko esam ieguvuši?

1) Ja esam konstatējuši, ka ja mūsu objektu sistēmā ir saskaitīšanas un reizināšanas operācijas, kurās izpildās **gredzena** aksiomas 1-7, tad šai sistēmā izpildās arī teorēmas T1-T13.

2) Ja esam konstatējuši, ka ja mūsu objektu sistēmā ir saskaitīšanas un reizināšanas

operācijas, kurās izpildās **lauka** aksiomas 1-10, tad šai sistēmā izpildās arī teorēmas T1-T21.

Tātad, ja mēs sākumā būtu pārliecinājušies ka kompleksiem polinomiem un kompleksām nxn matricām izpildās gredzena aksiomas, tad **T1-T13 mums polinomiem un matricām vairs nebūtu speciāli jāpierāda.** Jo tās jau ir pierādītas – visiem gredzeniem!

Galīgie gredzeni un lauki Z_n

Līdz šim visi mūsu piemēri bija **bezgalīgi** gredzeni un lauki. Bija tikai divi izņēmumi – triviālais gredzens {g} un triviālais lauks {0, 1}.

Uzbūvēsim gredzenu Z_4, tad būs skaidrs, ko nozīmē Z_n.

Dalot jebkuru veselu skaitli ar 4, atlikumā iegūsim 0, 1, 2 vai 3. Šie atlikumi tad arī būs gredzena elementi: $Z_4 = \{0, 1, 2, 3\}$.

Kā te definēsim saskaitīšanu a+b un reizināšanu a*b? Cik iznāks 2+3 un 2*3?

2+3=5, dalām ar 4, atlikums 1, tātad šajā gredzenā 2+3=1.

2*3=6, dalām ar 4, atlikums 2, tātad šajā gredzenā 2*3=2.

utt.

Tādā veidā varam sastādīt saskaitīšanas un reizrēķina tabulas Z_4:

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0

2	2	3	0	1
3	3	0	1	2

*	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Z_4 **veido gredzenu.** [Varat pārliecināties paši, tas ir paliels darbiņš, bet nav sarežģīts.]

Z_4 **neveido lauku.** Piemēram, elementam 2 nav inversā elementa, jo vienādība 2*x=1 nav iespējama (2*x pēc tabulas vienmēr ir 0 vai 2).

Z_4 ir viens **nulles dalītājs**: 2*2=0, citu nav (sk. reizrēķina tabulu: nenulles x, y reizinājums xy=0, tad un tikai tad, ja x=y=2).

Inversais elements a^{-1} eksistē tikai 1 un 3:

$$1*1=1;1^{-1}=1;$$
$$3*3=1;3^{-1}=3$$

(sk. reizrēķina tabulu)

Bet $0^{-1};2^{-1}$ neeksistē.

Vispārīgais gadījums:

Z_n sastāv no atlikumiem, kas rodas, dalot ar n, t.i. $Z_n=\{0,1,2,\ldots,n-1\}$, attiecīgi nodefinējot

saskaitīšanu un reizināšanu (x+y un x*y atrodam, izpildot parasto saskaitīšanu un reizināšanu, pēc tam rezultātu dalot ar *n* un ņemot atlikumu).

Teorēma. Jebkuram n>0, Z_n veido **gredzenu** no *n* elementiem. Bet Z_n veido **lauku** tad un tikai tad, ja *n* ir **pirmskaitlis**.

Pierādījums: (i-iespēja) nav grūts, bet ir jāzina nedaudz no skaitļu teorijas.

Tātad, piemēram, Z_2, Z_3, Z_5, Z_{19} ir lauki, bet Z_4, Z_6, Z_{16} – tikai gredzeni.

Uzdevums. Laukā Z_7, izdalīsim 4 ar 5, t.i. aprēķināsim $\frac{4}{5}$.

Rezultāts nebūs 0,8! Jo $Z_7=\{0,1,2,3,4,5,6\}$ un mums ir jāatrisina vienādojums 5x=4. Izmēģinām x=0,1,2,3,4,5,6.

Sanāk: 5x=0,5,3,1,6,4,2. Tātad 5*5=4, tāpēc laukā $Z_7: \frac{4}{5}=5$.

Par **galīgo lauku** vispārīgo teoriju un polinomu algebras īpatnībām šajos laukos sk. Wikipedia rakstus: Finite fields, Finite field arithmetic.

Uzdevums (i-iespēja). Pierādiet, ka ja **galīgā komutatīvā** gredzenā nav nulles dalītāju, tad tas ir lauks. Vai šo teorēmu var pierādīt arī bezgalīgiem gredzeniem?

Grupas

Grupas ir algebriskas sistēmas, kas matemātikā parādās arī

savādākās situācijās nekā lauki un gredzeni. To galvenais avots ir **pārveidojumu** (transformāciju) **sistēmas**, nevis skaitļu sistēmas. Kaut arī – skaitļu sistēmās var ieraudzīt diezgan daudzas grupas (sk. tālāk).

Labākais transformāciju grupu pirmais piemērs būtu Permutāciju grupas (Wikipedia). Bet par to būtu ilgi jāstāsta.

Arī citi transformāciju grupu piemēri ir diezgan sarežģīti izstāstāmi.

Bet kopējā shēma te ir šāda:

Ir dota kāda objektu kopa K.

1) **Transformācijas** ir funkcijas $f: K \to K$, kas katru objektu $x \in K$ pārveido par citu objektu $f(x) \in K$.

2) Transformācijas var kombinēt. Izpildīsim divas transformācijas $f: K \to K$ $g: K \to K$ pēc kārtas: vispirms no $x \in K$ iegūsim $g(x) \in K$ un pēc tam no *g(x)* iegūsim $f(g(x)) \in K$. Tādā veidā ir iegūta cita transformācija, kas $x \in K$ pārveido par $f(g(x)) \in K$. To sauc par *f* un *g* **kompozīciju** un apzīmē ar $f \circ g: K \to K$.

3) Aplūkosim tikai **apgriežamas** transformācijas, ko var izpildīt arī pretējā virzienā, no $f(x) \in K$ iegūstot $x \in K$.

Precīzāk to var pateikt šādi:

3a) Ar $e: K \to K$ apzīmēsim **identisko** transformāciju, kam $e(x) = x$ visiem x.

3b) Katrai apgriežamai transformācijai $f: K \to K$ eksistē inversā transformācija $f^{-1}: K \to K$, kam $f \circ f^{-1} = f^{-1} \circ f = e$.

Bet mūsu pieredze ar gredzeniem un laukiem jau ir pietiekama, lai mēs varētu sākt uzreiz ar formālu grupas definīciju arī bez piemēriem.

[Grāmatās var sastapt arī nedaudz savādākas grupas definīcijas, bet tās visas ir ekvivalentas zemāk dotajai.]

Vēsturi sk. Wikipedia rakstā Group (mathematics).
Evariste Galois (1811-1832), gandrīz romāns par viņa dzīvi: Leopold Infeld. *Whom the Gods Love: The Story of Evariste Galois* (ir tulkots latviešu valodā (“Dievu mīlulis”) un krievu valodā).

Formālā **grupas definīcija:**

Grupa ir kāda objektu kopa G un viena divvietīga operācija * šai kopā (parasti to sauc par reizināšanu), kas vienmēr ir izpildāma (t.i. ja *a, b* pieder G, tad *a*b* (jeb vienkārši *ab*) eksistē, ir vienīgs, un pieder G), un kam piemīt šādas īpašības:

1.aksioma. Operācija ir *asociatīva*: **(ab)c=a(bc)**.

Grupas operācijai **nav** obligāti būt *komutatīvai.* **Nekomutatīvas grupas un komutatīvas (jeb Ābela) grupas.** Sk. Wikipedia Abelian group.

2.aksioma. Eksistē *elements-vienīnieks* 1: visiem *a*, **1a=a1=a**.

Līdzīgi kā gredzeniem, varam pierādīt, ka elements-vienīnieks ir tikai viens (tāpēc varam to apzīmēt ar **1**). Kāpēc bija jāraksta 1a=a1=a nevis tikai 1a=a? Tāpēc, ka grupas operācija var nebūt komutatīva, un tad ar 1a=a nepietiek.

3.aksioma. Katram *a* eksistē *apgrieztais elements b*: **ab=ba=1**.

Līdzīgi kā gredzeniem, varam pierādīt, ka katram *a* apgrieztais elements ir tikai viens (tāpēc varam apzīmēt to ar $\boldsymbol{a^{-1}}$).

Grupu piemēri

Triviālā grupa {g}: gg=g. Visas grupas īpašības izpildās. Tā ir komutatīva grupa.

Veselie skaitļi ar saskaitīšanu veido grupu: xy vietā ir x+y, 1 vietā 0, x^{-1} vietā −x. Visas grupas īpašības izpildās:

$$(x+y)+z=x+(y+z);$$
$$0+x=x+0=x;$$
$$x+(-x)=(-x)+x=0.$$

Tā ir komutatīva grupa.

Veselie skaitļi ar reizināšanu – tā nav grupa (jo tikai +1 un –1 eksistē apgrieztais elements).

Toties kopa **{+1, –1}** ar reizināšanu veido grupu. Visas grupas īpašības izpildās

Racionālie skaitļi ar reizināšanu – tā nav grupa (nullei nav apgrieztā elementa).

Racionālie skaitļi bez 0 ar reizināšanu veido grupu. Visas grupas īpašības izpildās. Tā ir komutatīva grupa.

Racionālie pozitīvie skaitļi ar reizināšanu veido grupu. Visas grupas īpašības izpildās. Tā ir komutatīva grupa.

***n x n* matricas jebkurā laukā K ar reizināšanu** – tā nav grupa (nav apgrieztā elementa singulārajām matricām, t.i. tām, kuru determinants ir 0).

Nesingulārās *n x n* matricas laukā K ar reizināšanu. Visas grupas īpašības izpildās. Ja n>1, tad tā ir **nekomutatīva** grupa.

Jebkurš lauks K bez savas nulles ar reizināšanu. Visas grupas īpašības izpildās. Komutatīva grupa.

Vieninieka n-tās pakāpes saknes ar reizināšanu. Visas grupas īpašības izpildās. Galīga komutatīva grupa ar *n* elementiem.

Gredzens Z_n ar saskaitīšanu. Visas grupas īpašības izpildās.

Galīga komutatīva grupa ar *n* elementiem.

Ja n – pirmskaitlis, **lauks Z_n bez savas nulles ar reizināšanu.**

Visas grupas īpašības izpildās. Komutatīva grupa.

Grupas elementārdaļiņu fizikā

Sk. https://en.wikipedia.org/wiki/Special_unitary_group;

https://en.wikipedia.org/wiki/Unitary_matrix