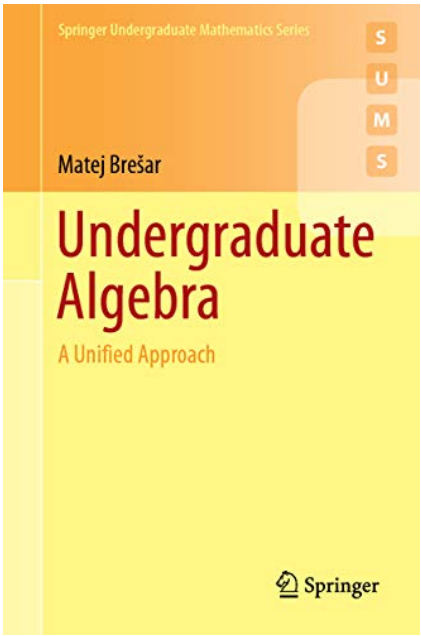
Matej Brešar, Undergraduate algebra – a unified approach, Springer undergraduate mathematics series, Springer, Cham, 2019, 316 strani



Tradicionalno se pri pouku abstraktne algebre najprej obravnavajo grupe, nato kolobarji, moduli in polja. Pri tem se pri vseh strukturah obravnavajo podstrukture, homomorfizmi in (razen pri poljih) kvocientne strukture. Nekateri rezultati, na primer izreki o izomorfizmih, se pri vsaki od struktur ponavljajo. Ker gre za konceptualne rezultate, se tudi dokazi vsebinsko ponavljajo. Predavatelj je tako postavljen pred neprijetno izbiro: izreke vedno dokazati ali pa pri kasnejših rezultatih zgolj navesti, da je dokaz podoben kot pri ustreznem rezultatu za prej obravnavano strukturo. Vsaka od obeh možnosti ima svoje slabe strani. Dokazovanje izrekov, ki so analogni že dokazanim, terja čas, ki ga zato morda zmanjka za kakšno drugo snov, poleg tega pa vsaj pri boljših študentih vzbuja vtis, da se snov preveč ponavlja. V primeru sklicevanja na podobnost dokaza pri že obravnavani strukturi pa se je treba zavedati, da so študenti to strukturo lahko obravnavali več mesecev nazaj in snov zato ni več sveža.

V izogib zgoraj navedenim dilemam profesor Brešar na Fakulteti za matematiko in fiziko Univerze v Ljubljani predmet Algebra 2 predava v drugačnem vrstnem redu. Najprej za vse algebraične strukture hkrati obravnava koncepte, ki so skupni vsem strukturam, v drugem delu predmeta pa natančneje izpostavi rezultate, ki so specifični za posamezne strukture. Za svoje študente je napisal učbenik *Uvod v algebro*, ki je leta 2018 izšel pri DMFA – založništvo. Pričujoča knjiga *Undergraduate algebra – a unified approach* je razširjen prevod slovenskega učbenika. Med drugim so v njej dodane vsebine, ki so zaradi omejenega števila ur pri Algebri 2 na FMF z leti izpadle iz učnega načrta, marsikje v tujini pa so del standardne snovi, ki se obravnava pri abstraktni algebri. Na FMF lahko študent spozna te vsebine pri izbirnem predmetu Algebra 3.

Knjiga Undergraduate algebra – a unified approach je sestavljena iz dveh delov. Prvi del, ki ima naslov The language of algebra, vsebuje štiri poglavja, drugi del z naslovom Algebra in action pa tri. V prvem delu avtor vpelje osnovne algebraične strukture ter razloži koncepte, ki so skupni vsem strukturam, v drugem delu pa natančneje obravnava grupe, kolobarje in razširitve polj. Učbenik je napisan zelo razumljivo in bo v pomoč marsikateremu študentu pri študiju abstraktne algebre, ne glede na to, ali jo predavatelj predava v vrstnem redu, kot je naveden v knjigi, ali na tradicionalen način. Vsi koncepti so ponazorjeni s številnimi primeri, prav tako vsak razdelek vsebuje precej nalog za reševanje.

V prvem poglavju avtor vpelje osnovne algebraične strukture, s poudarkom na grupah, kolobarjih, poljih, vektorskih prostorih in algebrah. Za vse te strukture nato definira podstrukture, opiše, kaj so generatorji posamezne strukture, ter (razen za polja) definira direktne produkte. Že v prvem poglavju je navedenih precej zgledov algebraičnih struktur, pomembnejši primeri pa so natančneje obravnavani v drugem poglavju. Med zgledi komutativnih kolobarjev so obravnavani kolobar celih števil ter kolobar ostankov $\mathbb{Z}_n$ pri deljenju z n, kolobar funkcij ter kolobarji polinomov v eni in več spremenljivkah. Pomembna rezultata v celih številih sta osnovni izrek o deljenju in Evklidov algoritem. Avtor dokaže tudi, da je $\mathbb{Z}_n$ polje natanko takrat, ko je n praštevilo. Od grup so obravnavane simetrična grupa S_n vseh permutacij na n elementih, diedrska grupa ter matrične grupe: splošna in posebna linearna grupa, ortogonalna grupa, unitarna grupa in simplektična grupa. Pri permutacijah sta izpeljana razcepa na produkt disjunktnih ciklov in na produkt transpozicij. Dokazana je enoličnost parnosti števila transpozicij v razcepu, s pomočjo česar je definiran znak permutacije. Avtor tudi pokaže, da sode permutacije tvorijo grupo, ki jo imenujemo alternirajoča grupa. Poglavje o primerih se zaključi s kvaternioni, ki so za študente prvi (in pogosto tudi edini) primer nekomutativnega obsega.

Tretje poglavje je posvečeno homomorfizmom. To so preslikave, ki »ohranjajo operacijo«. Vpeljavo pojma homomorfizma avtor motivira z izomorfizmom vektorskih prostorov, ki ga študenti že poznajo iz linearne algebre, in izomorfizmom končnih grup, ki ga neformalno razloži s preimenovanjem elementov v tabeli množenja. Hkrati vpelje tudi pojem ciklične grupe in reda elementa v grupi. Sledi formalna definicija homomorfizmov vseh obravnavanih algebraičnih struktur. Avtor na enoten način definira sliko in jedro homomorfizma ter pokaže, da je injektivnost homomorfizma ekvivalentna trivialnosti njegovega jedra. V nadaljevanju so obravnavani izreki o vložitvah. Algebraične strukture so pogosto definirane abstraktno, za lažjo

predstavo in računanje z njimi pa je ugodneje, kadar jih prepoznamo kot podobjekte v konkretnih objektih. Da je to vedno mogoče, nam povedo izreki o vložitvah. Vsako končno grupo je mogoče po Cayleyjevem izreku vložiti v permutacijsko grupo, vsaka končnorazsežna algebra nad poljem pa je izomorfna neki matrični algebri. Sledita razdelka o polju ulomkov celega komutativnega kolobarja in o karakteristiki kolobarja.

V četrtem poglavju avtor predstavi kvocientne strukture. Najprej definira odseke po podgrupi in dokaže Lagrangeev izrek, ki pravi, da je moč končne grupe enaka produktu moči podgrupe in indeksu te podgrupe v grupi. Nato bralcu predstavi, da bi na kvocientni množici vseh odsekov radi definirali operacijo na naraven način kot $aN \cdot bN = (ab)N$. Zato definira podgrupo edinko in pokaže, da je v primeru, ko je N podgrupa edinka, navedena operacija dobro definirana in da je kvocientna množica grupa za to operacijo. Enako avtor stori v primeru kolobarjev in algeber, kjer ima vlogo podstrukture, po kateri je mogoče definirati kvocientno strukturo, ideal. Prava moč avtorjevega enotnega pristopa k algebraičnim strukturam se pokaže pri izrekih o izomorfizmih. Prvi izrek o izomorfizmu je formuliran tako za grupe kot za kolobarje, vektorske prostore in algebre. Avtor najprej utemelji, da je jedro homomorfizma $\varphi\colon A \to A'$ podgrupa edinka, ideal oziroma vektorski podprostor, zato je vselej mogoče definirati kvocientno strukturo $A/\ker\varphi$. Nato v primeru grup pokaže, da je kvocientna grupa izomorfna sliki homomorfizma φ, dokaz za druge strukture pa je povsem enak, le notacija se spremeni. Drugi in tretji izrek o izomorfizmu (znana tudi kot izreka Emmy Noether) sta zaradi različnih notacij predstavljena za vsako strukturo posebej, navedena sta ključna koraka dokazov, detajle dokazov pa avtor prepušča bralcu. Poglavje se konča z »notranjima« definicijama direktnega produkta grup in kolobarjev.

Poglavja o grupah, kolobarjih in razširitvah polj v drugem delu knjige so precej razširjena glede na slovenski učbenik Uvod v algebro. Poglavju o kolobarjih je dodana obravnava modulov ter klasifikacija končno generiranih modulov nad glavnimi kolobarji, poglavju o grupah izreki Sylowa in krajša obravnava rešljivih ter enostavnih grup, poglavju o razširitvah polj pa polja s karakteristiko 0, Galoisova teorija, rešljivost polinomskih enačb z radikali ter osnovni izrek algebre. Glede na slovensko knjigo Uvod v algebro bralec v pričujoči knjigi opazi tudi spremenjen vrstni red poglavij o kolobarjih in grupah. Vzrok za zamenjavo poglavij je naslednji: V knjigi Uvod v algebro je v poglavju o grupah predstavljena klasifikacija končnih Abelovih grup. S skoraj povsem enakim dokazom pa je mogoče izpeljati splošnejši rezultat, namreč klasifikacijo končno generiranih torzijskih modulov nad glavnimi ko-

lobarji. Klasifikacija končnih Abelovih grup potem sledi kot poseben primer, če za kolobar vzamemo cela števila. Poleg tega je splošnejši rezultat uporaben tudi na drugih področjih, na primer za izpeljavo Jordanove kanonične forme matrike. Za dokaz splošnejšega izreka pa je seveda treba vpeljati nekatere pojme, povezane s kolobarji in moduli, zato sta poglavji o grupah in kolobarjih zamenjani.

V petem poglavju se avtor torej ukvarja s komutativnimi kolobarji. V kolobarju polinomov v eni spremenljivki nad poljem dokaže osnovni izrek o deljenju in obravnava (ne)razcepnost polinomov. V primeru polinomov nad racionalnimi števili sta pomembna predvsem Gaussova lema in Eisensteinov kriterij. Nato avtor vpelje pojme, povezane z deljivostjo, v poljubnem komutativnem kolobarju, ter obravnava evklidske kolobarje, glavne kolobarje in kolobarje z enolično faktorizacijo. Evklidski kolobar je hkratna posplošitev celih števil in polinomov v eni spremenljivki nad poljem. To je komutativen kolobar brez deliteljev niča, v katerem velja analog Evklidovega algoritma. Glavni kolobar pa je komutativen kolobar brez deliteljev niča, v katerem je vsak ideal glavni, torej generiran z enim elementom. Avtor pokaže, da je vsak evklidski kolobar glavni, vsak glavni kolobar pa ima enolično faktorizacijo, kar pomeni, da je mogoče vsak njegov element napisati kot produkt nerazcepnih elementov na enoličen način. Preostanek petega poglavja obravnava module. Najprej so definirani moduli nad poljubnim kolobarjem, podmoduli, homomorfizmi modulov, kvocienti, direktni produkti in generatorji modulov, nato pa so natančneje obravnavani moduli nad glavnimi kolobarji. Avtor najprej formulira izrek, ki klasificira končne Abelove grupe. Nato razloži, da bo ta izrek sledil iz bolj splošnega izreka o klasifikaciji končno generiranih torzijskih modulov nad glavnimi kolobarji in da direktni dokaz klasifikacije Abelovih grup ni nič krajši. Za bralca, ki ni vešč dela z moduli, tudi razloži, kako naj dokaz izreka o klasifikaciji končno generiranih torzijskih modulov nad glavnimi kolobarji prevede na primer Abelovih grup. Nato je izrek o klasifikaciji končno generiranih torzijskih modulih nad glavnimi kolobarji formuliran in dokazan. Sledi uporaba tega izreka pri izpeljavi Jordanove kanonične forme za linearno preslikavo $T\colon V \to V$, kjer je V končnorazsežen vektorski prostor nad algebraično zaprtim poljem F. Ključni korak je, da na vektorskem prostoru V definiramo strukturo modula nad polinomskim kolobarjem $F[X]$ s predpisom $p(X).v = p(T)(v)$. Modul, ki ga dobimo, je končno generiran in torzijski, za kolobar $F[X]$ pa že vemo, da je glavni, zato lahko uporabimo prej dokazani izrek.

Šesto poglavje natančneje obravnava končne grupe. Avtor izpelje razredno formulo in dokaže Cauchyjev izrek, ki pove, da končna grupa, katere

moč je deljiva s praštevilom p, vsebuje element reda p. Nato definira delovanje grupe, vpelje pojma orbite in stabilizatorja ter dokaže zvezo med njima. S pomočjo delovanj nato dokaže izreke Sylowa o podgrupah moči p^k v dani grupi. Sledita krajša razdelka o rešljivih grupah in o enostavnih grupah. Glavna rezultata, ki bosta pomembna pri razširitvah polj, sta, da je alternirajoča grupa A_5 enostavna, ter da simetrična grupa S_n ni rešljiva za $n \geq 5$.

Sedmo poglavje govori o razširitvi polj. Začne se z opisom problema reševanja polinomskih enačb, ki je zgodovinska motivacija za študij razširitev polj. Nato avtor vpelje algebraične in transcendentne elemente in natančneje obravnava končne razširitve polj. Dokaže tudi, da je mogoče z ravnilom in šestilom konstruirati le tiste točke v ravnini, katerih obe koordinati sta algebraični števili, katerih stopnji sta potenci števila 2. Naslednja tema poglavja so razpadna polja. Za dani polinom s koeficienti iz polja vedno obstaja (morda večje) polje, v katerem ima polinom ničlo. To polje je kvocient polinomskega kolobarja po maksimalnem idealu, generiranem z nerazcepnim deliteljem danega polinoma. Induktivna uporaba tega argumenta pove, da ima vsak polinom s koeficienti iz polja svoje razpadno polje, torej najmanjše polje, nad katerim polinom lahko zapišemo kot produkt linearnih faktorjev. Sledi obravnava končnih polj. Ta so praštevilske karakteristike, zato je njihova moč oblike p^n, kjer je p praštevilo in $n \in \mathbb{N}$. Glavni rezultat o končnih poljih je obrat zadnje trditve, torej da za vsako praštevilo p in vsako naravno število n obstaja do izomorfizma natančno določeno polje s p^n elementi, ki je razpadno polje polinoma $X^{p^n} - X$ nad $\mathbb{Z}_p$. V nadaljevanju so obravnavana polja s karakteristiko 0. Za njih velja izrek o primitivnem elementu, ki pravi, da je vsaka njihova končna razširitev generirana z enim samim elementom. Avtor nato vpelje definicije fiksnega polja, Galoisove razširitve in Galoisove grupe ter dokaže Osnovni izrek Galoisove teorije, ki pravi, da obstaja bijekcija med vmesnimi polji razširitve in podgrupami Galoisove grupe. Iz Galoisove teorije sledi tudi, da je Galoisova grupa polinoma, ki je rešljiv z radikali, vedno rešljiva. Ker simetrična grupa S_n ni rešljiva za $n \geq 5$, sledi Abel-Ruffinijev izrek, ki pravi, da obstajajo polinomi pete stopnje v $\mathbb{Q}[X]$, ki niso rešljivi z radikali, torej taki, katerih ničel ne moremo izraziti s formulami, ki vsebujejo le seštevanje, odštevanje, množenje, deljenje in uporabo poljubnih korenov. Knjiga se zaključi z dokazom osnovnega izreka algebre, ki pravi, da je polje kompleksnih števil algebraično zaprto.

Klemen Šivic