Algebra 2

Hugo Trebše (hugo.trebse@gmail.com)

19. oktober 2024

> Algebra is the offer made by the devil to the mathematician. The devil says: »I will give you this powerful machine, it will answer any question you like. All you need to do is give me your soul: give up geometry and you will have this marvelous machine.«
>
> *Michael Atiyah*

Kazalo

1 Grupe

Definicija 1.1

Grupa je par $(G, \cdot)$, kjer je operacija $\cdot$ asociativna, zanjo v G obstaja nevtralni element ter ima vsak element inverz.

Naloga 1.2

Permutaciji imata *enako zgradbo disjunktnih ciklov*, če sta permutaciji produkta disjunktnih ciklov enakih dolžin. Pokaži, da če imata permutaciji σ, σ' enako zgradbo disjunktnih ciklov, potem sta si konjugirani - obstaja $\pi \in S_n$, da je $\sigma' = \pi\sigma\pi^{-1}$.

Oris dokaza. Lahko, po tem ko opazimo, da če je $\sigma = d_1 \dots d_k$ in $\sigma' = d'_1 \dots d'_k$, potem je $\pi^{-1}\sigma\pi = (\pi^{-1}d_1\pi)(\pi^{-1}d_2\pi)\dots(\pi^{-1}d_k\pi)$. Problem je tako reduciran na dokaz, da obstaja π, da je $d'_j = \pi^{-1}d_j\pi$, ne pridemo do problemov, saj so cikli disjunktni. □

Centralizator elementa ($C_G(x)$) je podgrupa, ki vsebuje vse elemente, ki konjugirajo z danim elementom.

Trditev 1.3

Če je $H, K \leq G$, potem HK ni nujno podgrupa G. Če pa velja $HK = KH$, pa je HK podgupa G.

Oris dokaza. Protiprimer je H, K generirani s transpozicijama v S_3. Dokaz je očiten. □

Trditev 1.4

Če je $H \leq G$ in $a \in G$, potem je aHa^{-1} podgrupa G.

Definicija 1.5

- *Center* grupe G je podgrupa $Z(G) = \{u \in G \mid au = ua \, \forall a \in G\}$.
- $aH = \{ah | h \in H\}$ je levi odsek $a \in G$ po $H \leq G$.
- Kardinalnost vseh (različnih) odsekov G po $H \leq G$ je indeks H, kar označujemo z $[G : H]$

Trditev 1.6

- Odseka sta bodisi enaka, bodisi disjunktna. $aH = bH \implies ab^{-1} \in H$

Izrek 1.7: Lagrange

Naj bo $H \leq G$, kjer je G končna grupa. Potem je $|G| = |H| \cdot [G : H]$.

Oris dokaza. Grupo G razdelimo na disjunktne odseke. Vsak odsek ima H elementov. □

1.1 Kvocientne grupe

Definicija 1.8

N je **podgrupa edinka** grupe G, če velja $N \leq G$ ter

$$gNg^{-1} \subseteq N \quad \forall g \in G.$$

Netrivialna grupa brez pravih edink (različnih od same sebe) je *enostavna* grupa.

Trditev 1.9

Ekvivalenten pogoj, da je N podgrupa edinka grupe G je enakost

$$gNg^{-1} = N \text{ za vse } g \in G.$$

Podobne enakosti ter vsebovanosti lahko dosežemo z levim ter desnim 'množenjem' z g^{-1} oz. g.

Trditev 1.10: Operacije z edinkami

- $H \leq G$ ter $N \trianglelefteq G \implies HN = NH \leq G$.
- $M, N \trianglelefteq G \implies MN = NM \trianglelefteq G$ ter $M \cap N \trianglelefteq G$.

Lema 1.11: Kanonični epimorfizem

Naj bo N podgrupa edinka grupe G. Preslikava $\pi : G \to G/N$, za katero velja $\pi(a) = aN$, je epimorfizem grup.

Jedro te preslikave je edinka. Odkrijemo, da velja tudi obrat - vsaka edinka je jedro nekega epimorfizma.

Izrek 1.12: Cauchyjev izrek

Naj bo G končna grupa. Če praštevilo p deli $|G|$, potem G vsebuje element reda p.

1.2 Direktni ter notranji produkti

Definicija 1.13

Naj so $G_1, \ldots, G_n$ grupe. Potem je $G = G_1 \times \cdots \times G_n$ prav tako grupa za očitno operacijo na n-tericah. Grupi G pravimo *direktni produkt* grup $G_1, \ldots, G_n$.

Opazimo, da je $\tilde{G}_j = \langle (1_1, \ldots, g_j, \ldots, 1_n) \mid g_j \in G_j \rangle$ podgrupa edinka v G, ter da celo velja $G = \prod_{i=1}^{n} \tilde{G}_i$, kar motivira naslednjo definiicjo.
Če so $N_1, \ldots, N_s \lhd G$ ter velja:

- $G = \prod_{i=1}^{s} N_i$
- $N_i \cap (N_1 \ldots N_{i-1} N_{i+1} \ldots Ns) = 1$,

potem je G *notranji direktni produkt* $N_1, \ldots, N_s$.

Trditev 1.14

G je notranji direktni produkt svojih edink $N_1, \ldots, N_s$ natanko tedaj, ko lahko vsak element x grupe G zapišemo na enoličen način kot produkt elementov $n_i \in N_i$.

Dokaz trditve je popolnoma klasičen.

Lema 1.15

Če je $|G| = mn$, kjer sta m in n tuji si naravni števili, potem za podgrupi

$$H = \{x \in G \mid mx = 0\} \quad \text{in} \quad K = \{x \in G \mid nx = 0\}$$

velja $G = H \oplus K$ ter $|H| = m$ in $|K| = n$.

Oris dokaza. H in K sta očitno podgrupi. Seveda je $nx \in H$ in $mx \in K$ za vse $x \in G$. Po Bezoutovi lemi obstajata števili $u, v \in \mathbb{Z}$, da je $x = u(nx) + v(mx)$, kar dokaže $G = H + K$. Da je $H \cap K = \{0\}$ je prav tako očitno, kar dokazuje direktnost vsote. Z enostavno uporabo Cauchyjevega izreka dokažemo tudi ustrezne kardinalnosti H in K. □

Izrek 1.16: Osnovni izrek o končnih Abelovih grupah

Vsaka končna Abelova grupa G je direktna vsota cikličnih p grup.
Natančneje je

$$G \cong G_1 \oplus \cdots \oplus G_n,$$

kjer je n enolično določen ter je p praštevilo in

$$G_i \cong \mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_l}},$$

ter so $\{k_i\}$ enolično določeni za vsak G_i.

Naloga 1.17

Pokaži, da je podgrupa edinka generirana z množico X enaka podgrupi generirani z množico $\{gxg^{-1} \mid g \in G, x \in X\}$. Kot posledico pokaži, da je vsak element iz G enak produktu elementov konjugiranem nekem fiksnem elementu $x \neq 1$.

Definicija 1.18

- $K \leq G$ je *karakteristična podgrupa*, če je $\varphi(K) \subseteq K \, \forall \, \varphi \in \mathrm{Aut}(G)$. Vse karakteristične podgrupe so normalne, saj je za slednje zadosti enakost za $\varphi \in \mathrm{Inn}(G)$.
- Grupa je *torzijska*, če ima vsaka njena podgrupa končen red, ter *torzijsko prosta*, če je edini element s končnim redom enota.

1.3 Delovanje grup

Izrek 1.19: Cayleyjev izrek

Naj bo G grupa in S_n simetrična grupa reda n. Za vsak $a \in G$ lahko definiramo preslikavo $\ell_a(x) = ax$, za katero hitro preverimo, da je avtomorfizem G. Trdimo, da je preslikava $\varphi : G \to \mathrm{Sim}(G)$, definirana kot $\varphi(a) = \ell_a$ injektivna, kar z lahkoto dokažemo.
Sledi, da lahko vsako grupo G vložimo v neko simetrično grupo (gotovo v simetrično grupo $S_{|G|}$).

Definicija 1.20

Grupa G *deluje na množici* X, če obstaja preslikava iz $G \times X$ v X, ki paru (a, x) priredi element $a \cdot x$, da velja:

- $(ab) \cdot x = a \cdot (b \cdot x)$
- $1 \cdot x = x$

Primeri delovanja so trivialno delovanje, levo množenje ter konjugiranje - $a \cdot x = axa^{-1}$.

Definicija 1.21

Naj grupa G deluje na množici X.

- *Orbita* elementa $x \in X$ je množica $G \cdot x = \{a \cdot x \mid a \in G\}$,
- *Stabilizator* elementa x pa množica $G_x = \{g \in G \mid g \cdot x = x\}$.

Definicija 1.22

Naj bo $x \in G$. Potem je množica $C(x) = \{g \in g \mid xg = gx\}$ centralizator elementa x.

Lema 1.23

Naj grupa G deluje na množici X.

- S predpisom $x \sim y \iff y = a \cdot x$ za nek $a \in G$ je definirana ekvivalenčna relacija na množici X. Za vsak $x \in X$ je orbita $G \cdot x$ enaka ekvivalenčnem razredu, ki vsebuje x.
- Vsak stabilizator G_x je podgrupa G.

Izrek 1.24: O orbiti in stabilizatorju

Naj grupa G deluje na množici X. Potem za vsak $x \in X$ velja

$$|G \cdot x| = [G : G_x].$$

Če je G končna, je torej $|G| = |G \cdot x| \cdot |G_x|$

Izrek 1.25: Particija orbit

Naj grupa G deluje na končni množici X in naj Z označuje množico vseh elementov $x \in X$, za katere velja $a \cdot x = x$ za vse $a \in G$. Če je $X \neq Z$ (delovanje je netrivialno), potem obstajajo $x_1, \ldots, x_m \in X \setminus Z$, da je

$$|X| = |Z| + \sum_{j=1}^{m} |G \cdot x| = |Z| + \sum_{j=1}^{m} [G : G_{x_j}]$$

Posledica izreka je:

Trditev 1.26

Naj končna p-grupa G deluje na končni množici X in naj Z označuje množico elementov $x \in X$, da je $a \cdot x = x$ za vse $a \in G$. Potem p deli $|X| - |Z|$.

Če za delovanje izberemo konjugiranja dobimo naslednjo formulo:

Izrek 1.27: Razredna formula

Naj bo G končna grupa, ki ni Abelova. Potem obstajajo $x_1, \ldots, x_n \in G \setminus Z(G)$, da je

$$|G| = |Z(G)| + \sum_{j=1}^{m} [G : C(x_j)].$$

Če za G izberemo netrivialno p-grupo pridemo do zaključka: **Vsaka netrivialna p grupa ima netrivialen center**. Ponovno dobimo naslednjo posledico:

Trditev 1.28

Če za grupo G velja, da je $|G| = p^2$ za $p \in \mathbb{P}$, potem je G Abelova.

Oris dokaza. $Z(G)$ je netrivialna, zato reda p ali p^2. Če je reda p^2 smo končali, drugače pa je $G = Z(G) \oplus G/Z(G)$. Ker je $|G/Z(G)| = p$ je ciklična, kar hitro preverimo, da je nemogoče. □

Izrek 1.29: Dvomljivo Burnsideova lema

Naj G deluje na X. Potem je število orbit delovanja enako količini

$$\frac{1}{|G|} \sum_{g \in G} |\text{FixPt } g| ,$$

kjer je FixPt g število elementov $x \in X$, za katere je $g \cdot x = x$.

Izrek 1.30: Cauchyjev izrek

Naj bo G končna grupa in $p \mid |G|$. Potem G vsebuje element reda p.

Oris dokaza. Definirajmo

$$X = \{(a_1, \ldots, a_p) \mid a_i \in G \text{ in } a_1 \ldots a_p = 1\}.$$

Grupa $\mathbb{Z}_p$ s predpisom $k \cdot (a_1, \ldots, a_p) = (a_{k+1}, \ldots, a_p, a_1, \ldots, a_k)$ deluje na množici X. Po izreku 1.25 ugotovimo, da $p \mid |Z|$, saj je $|X| = |G|^{p-1}$. Hitro dokažemo, da je $(a_1, \ldots, a_p) \in Z$ natanko tedaj, ko je $a_1 = a_2 = \cdots = a_p$. Ker je $(1, \ldots, 1)$ v Z ter $p \mid |Z|$, slednji vsebuje nek element različen od enote, posledično je $(a, \ldots, a) \in Z$, kar implicira $a^p = 1$. □

1.3.1 Izreki Sylowa

Definicija 1.31

- $H \leq G$. Potem je naslednja množica *normalizator* H:

$$N(H) = \{a \in G \mid aHa^{-1} = H\}$$

- $H \leq G$, kjer je G končna grupa, je *p-podgrupa Sylowa*, če je

$$|H| = p^k \quad \text{ter} \quad p^{k+1} \nmid |G|$$

Seveda je $N(H) = G$ natanko tedaj, ko je H edinka. Venomer pa je $N(H) \leq G$ in $H \lhd N(H)$.

Izrek 1.32: Izreki Sylowa

Naj $p \in \mathbb{P}$ deli red končne grupe G.

- Če $p^\ell \mid |G|$, potem G vsebuje p-podgrupo reda p^ℓ.
- Vsaka p-podgrupa G je vsebovana v neki p-podgrupi Sylowa.
- Vsaki p-podgrupi Sylowa G sta konjugirani.
- Število p-podgrup Sylowa G deli $|G|$ ter je oblike $pm + 1$ za $m \geq 0$.

Število p-podgrup Sylowa označujemo z n_p.

2 Kolobarji ter njihove nadgradnje

Definicija 2.1

$(K, +, \cdot)$ je *kolobar*, če velja, da je $(K, +)$ Abelova grupa, $(K, \cdot)$ monoid ter veljata leva in desna distributivnost.

Od homomorfizma zahtevamo, da je aditiven, multiplikativen ter slika enoto v enoto.

Kot dododatek povemo: Če je e idempotent, oz. je $e^2 = e$, potem je tudi $(1 - e)$ idempotent.

Definicija 2.2

- Če je $(K, \cdot)$ Abelova je kolobar *komutativen*.
- Komutativen kolobar brez deliteljev niča je *cel* kolobar.
- Neničelen kolobar v katerem je vsak neničelen element obrnljiv je *obseg*.
- Komutativen obseg je *polje*.

Definicija 2.3

$(A, +, \cdot, \circ)$ je *algebra* nad poljem $\mathbb{F}$, če je $(A, +, \circ)$ kolobar ter $(A, +, \cdot)$ vektorski prostor nad $\mathbb{F}$.

Od homomorfizma zahtevamo, da je za $(A, +, \circ)$ homomorfizem kolobarjev (aditiven, ohranja komponiranje ter slika enoto komoniranja v enoto komponiranja), ter da je homogen v skalarjih $\mathbb{F}$.

Z željo podobnega objekta kot je normalna podgrupa, ki bi omogočal kvociente, definiramo naslednji objekt.

Definicija 2.4: Ideal

Naj bo I podgrupa kolobarja K za seštevanje. Če za vse $a \in K$ in $u \in I$ velja $au \in I$ ter $ua \in I$, potem imenujemo I *ideal* kolobarja K.

Ponovno ugotovimo, da obstaja dualnost med jedri homomorfizmov kolobarjev ter ideali

Trditev 2.5: Operacije z ideali

- Vsota, produkt in presek idealov I in J so prav tako ideali:

$$I + J = \{u + v \,|u \in I, v \in J\}$$

$$IJ = \langle uv \,|u \in I, v \in J\rangle.$$

- Velja inkluzija

$$IJ \subseteq I \cap J \subseteq I \subseteq I + J$$

Podane trditve veljajo za enostranske in za dvostranske ideale. Prav tako obstaja kanonični epimorfizem iz kolobarja v kvocient kolobarja po nekem idealu, ter velja, da je ideal jedro tega epimorfizma. Kot pri grupah velja, da je aditivna podgrupa $(K, +)$ ideal natanko tedaj, ko je jedro nekega homomorfizma.

Ideal algebre definiramo analogno, dodatno zahtevamo le zaprtje za množenje s skalarji. Za ideale algeber veljajo analogne trditve o operacijah ter definirajo kanonični epimorfizem.

Izrek 2.6: Izrek o izomorfizmu

Naj bo $\varphi : A \to A'$ homomorfizem (grup, kolobarjev ali algeber). Potem je

$$A/\ker\varphi \cong \mathrm{im}\varphi$$

Definicija 2.7

Ideal $I \lhd K$ je maksimalen, če ne obstaja noben ideal J, da je $I \subset J \subset K$.

Ideal I je maksimalen ideal komutativnega kolobarja K natanko tedaj, ko je K/I polje.

Izrek 2.8: Izrek o ohranjanju idealov

Naj bo $I \lhd K$. Preslikava $\varphi : A \to A/I$ je bijekcija, ki ohranja podmnožice, med množico podkolobarjev A kolobarja K, ki vsebujejo I, ter množico podkolobarjev K/I. Dodatno je A ideal K natanko tedaj, ko je A/I ideal K/I

3 Moduli

Na podoben način kot smo splošno grupo vložili v neko simetrično grupo lahko tudi poljuben kolobar oz. algebro vložimo v kolobar endomorfizmov aditivne grupe oz. algebro endomorfizmov vektorskega prostora. Slednje pomeni, da lahko vsako končno-razsežno algebro vložimo v matrično algebro $M_n(\mathbb{F})$ za nek $n \in \mathbb{N}$.

Posledica tega dejstva je naslednje:

Naloga 3.1

Ali končno-razsežna algebra lahko vsebuje elementa s, t, za katera velja

$$st - ts = 1.$$

Oris dokaza. Ne, saj vložimo v matrično algebro ter uporabimo znano lastnost sledi. □

Zgrnji primer je relevanten, saj je pojem modula ekvivalenten pojmu homomorfizma iz kolobarja K v kolobar endomorfizmov aditivne grupe M, kar lahko preverimo po definicjii. Drugače, pa si lahko module predstavljamo tudi kot posplošitve vektorskih prostorov.

Definicija 3.2

Naj bo $(K, +, \cdot)$ kolobar in M množica. Potem je M K-modul, če je $(M, +)$ Abelova grupa in obstaja prelikava $K \times M \to M$, ki slika $(k, m) \mapsto km$, ki je homogena, zanjo veljata obe distributivnosti, ter velja $1_K \cdot m = m$.
$N \subseteq M$ je *podmodul* modula M, če je za isti operaciji sam modul, oz. je aditivna podgrupa M ter sočasno zaprta za modulsko množenje.

Vsota ter presek podmodul je prav tako modul. Če neničelni modul nima pravega podmodula, mu pravimo enostavni modul.

Uvedemo tudi pojem homomorfizma modulov (nad istim kolobarjem), ki je aditivna ter multiplikativna preslikava, ki fiksira elemente kolobarja: $\varphi(u + v) = \varphi(u) + \varphi(v)$ ter $\varphi(au) = a\varphi(u)$. Kot po navadi sta jedro ter slika homomorfizma modulov podmodula.

Definicija 3.3: Kolobar endomorfizmov

Množica endomorfizmov $\mathrm{End}_K(M)$ K-modula M postane kolobar, če definiramo seštevanje endomorfizmov na očiten način ter množenje endomorfizmov kot komponiranje.

Lema 3.4: Schur

Če je M enostaven K-modul je kolobar $\mathrm{End}_K(M)$ obseg

Oris dokaza. Naj bo $\varphi \in \mathrm{End}_(M)$ neničelen. Potem je $\ker(\varphi)$ pravi, $\mathrm{im}(\varphi)$ pa netrivialni podmodul enostavnega modula M. Sledi $\ker(\varphi) = \{0\}$ ter $\mathrm{im}(\varphi) = M$, sledi da je φ

avtomorfizem, posledično obrnljiv. □

Kot je zdaj že navada lahko definiramo kvocientni modul K-modula M po svojem podmodulu N z enakima operacijama seštevanja in modulskega množenja odsekov.

Kot bi pričakovali od razširitve pojma vektorskega prostora lahko definiramo tudi linearno neodvisnost ter bazo modula. Moduli pa žal ne podedujejo vseh lastnosti vektorskih prostorov, kot ilustrira naslednji primer.

Primer 3.5

Če je G končna aditivna grupa, potem za $|G| = n$ velja $nu = 0 \ \forall u \in G$. Sledi, da nobena neprazna podmnožica $\mathbb{Z}$-modula G ni linearno neodvisna.

Definicija 3.6

Modul, ki ima bazo, se imenuje *prost* modul.

Prostemu $\mathbb{Z}$-modulu M pravimo *prosta Abelova grupa*.

Tudi prosti moduli se substantivno razlikujejo od vektorskih prostorov; podmodul prostega modula na primer ni nujno prost ($\mathbb{Z}_4$ je kot modul nad samim sabo prost, a $2\mathbb{Z}_4$ ni prost kot modul nad $\mathbb{Z}_4$), ter velikost baze ni nujno enolično določena. Nam pa je v olajšanje dejstvo, da so linearne preslikave (homomorfizmi) med moduli enolično določeni z slikami baznih »vektorjev«.

V pričakovanju tenzorskega produkta omenimo naslednji trditvi:

Trditev 3.7

- Za vsako množico $\mathcal{B}$ ter kolobar K obstaja prost modul nad K z bazo $\mathcal{B}$.
- Naj bo M prost K-modul z bazo $\mathcal{B}$ ter N poljuben K-modul. Vsako preslikavo: $f : \mathcal{B} \to N$ lahko na enoličen način razširimo do homomorfizma modulov.

Presenetljivo je morda dejstvo, da prva trditev velja tudi v primeru, ko je $\mathcal{B}$ neskončna - tedaj zahtevamo, da so vse razen končno mnogo komponent elementa modula ničelne.

Modul nad obsegom D imenujemo *vektorski prostor*. Za module nad obsegi potem veljajo pričakovane lastnosti. Zaradi simetrije se brez škode za splošnost omejimo na leve vektorske prostore.

Izrek 3.8

Vsaka linearno neodvisna množica T v vektorskem prostoru V nad obsegom D je vsebovana v neki bazi prostora V.

Oris dokaza. $\mathcal{S}$ naj bo množica vseh linearno neodvisnih množic v V, ki vsebujejo T, ter jo delno uredimo z inkluzijo. Hiter premislek poda, da je množica, ki jo dobimo z

unijo katerekoli verige, linearno neodvisna, kar pomeni, da vsaka veriga vsebuje zgornjo mejo - posledično ima vsaka veriga maksimalni element, po Zornovi lemi. Ta maksimalni element $\mathcal{B}$ je baza, saj je $\mathcal{B} = \mathcal{B} \cup \{v\}$ za vsak vektor $v \in V$, saj je $\mathcal{B}$ zgornja meja verige. Sledi, da je v linearna kombinacija vektorjev iz $\mathcal{B}$, kar dokaže želeno. □

Zvita posledica izreka je, da ima vsak vektorski prostor nad obsegom bazo, saj lahko vzamemo $T = \{\}$. Sledi:

Trditev 3.9

Vsak modul nad obsegom je prost.

Enoličnost velikosti baze lahko pokažemo z analognim postopkom kot nad poljem - izmenjavanjem vektorjev.

3.1 Tenzorski produkt

Obravnavali bomo tenzorski produkt modulov nad komutativnim kolobarjem K.

4 Komutativni kolobarji

Naj bo $\mathbb{F}$ polje in $\mathbb{F}[X]$ kolobar polinomov nad F. Z analizo stopnje produkta polinomov ugotovimo, da je kolobar $\mathbb{F}[X]$ komutativen ter brez deliteljev niča, posledično cel. Vsi njegovi obrnljivi elementi pa so neničelni konstantni polinomi.

Trditev 4.1: Osnovni izrek o deljenju polinomov

Za vsak par polinomov $f(X), g(X) \in \mathbb{F}[X]$, pri čemer je $g(X) \neq 0$ obstajata enolično določena polinoma $q(X), r(X) \in \mathbb{F}[X]$, da velja:

$$f(X) = q(X)g(X) + r(X),$$

in je $r(X) = 0$ ali $\deg(r) < \deg(g)$

Trditev 4.2: Faktorski izrek

Vsak polinom f nad poljem $\mathbb{F}$ ima največ $\deg(f)$ ničel.

Definicija 4.3

- Polinom je *nerazcepen*, če je nekonstanten ter ni produkt nobenih dveh nekonstantnih polinomov.
- Polinom v $\mathbb{Z}[X]$ je *primitiven*, če so si njegovi koeficienti tuji.

Lema 4.4: Gauss

Produkt primitivnih polinomov je primitiven. Prav tako je celoštevilski polinom nerazcepen nad $\mathbb{Z}[X]$ natanko tedaj, ko je nerazcepen nad $\mathbb{Q}[X]$.

Izrek 4.5: Eisensteinov kriterij

Naj bo $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$ v $\mathbb{Z}[X]$. Če obstaja tako praštevilo p, da velja:

† $p \mid a_i$ za vse $i \in \{0, 1, \ldots, n-1\}$.

† $p^2 \nmid a_0$ ter $p \nmid a_n$,

potem je f nerazcepen nad $\mathbb{Z}[X]$.

Naloga 4.6

Pokaži, da je polinom $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1$ nerazcepen nad $\mathbb{Z}[X]$.

Oris dokaza. $\Phi_p(X) = \frac{X^p-1}{X-1} \implies \Phi_p(X+1) = \frac{1}{X}\left((X+1)^p - 1\right).$ □

Trditev 4.7

Naj bo $f(X) = a_n X^n + \cdots + a_0$ polinom nad $\mathbb{Q}$ ter praštevilo p ne deli a_n. Če je polinom $f(X) = (a_n + p\mathbb{Z})X^n + \cdots + (a_o + p\mathbb{Z})$ nerazcepen nad $\mathbb{Z}_p$, potem je nerazcepen tudi nad $\mathbb{Q}$.

4.1 Ideali

Ideal je *glavni*, če je generiran z enim elementom, ter *končno generiran*, če ga generira končno mnogo elementov. Elementi $a_1, \ldots, a_n$ generirajo ideal $\langle a_1, \ldots, a_n \rangle$, za katerega velja

$$\langle a_1, \ldots, a_n \rangle = \langle a_1 \rangle + \cdots + \langle a_n \rangle.$$

Kolobar je *glavni*, če so vsi ideali nad njim glavni.

Definicija 4.8

Cel kolobar K imenujemo *Evklidski kolobar*, če obstaja preslikava $\delta : K \to \mathbb{N}_0$ z nasldnjima lastnostima:

- Za vsak par elementov $a, b \in K$ obstaja par elementov $q, r \in K$, da je $a = qb + r$ in je $r = 0$ ali $\delta(r) < \delta(b)$.
- $\delta(a) < \delta(ab)$ za vse $a, b \in K \setminus \{0\}$.

Primeri evklidskih kolobarjev so $\mathbb{Z}, \mathbb{F}[X], \mathbb{Z}[i]$, ki imajo norme $|\cdot|, \deg(\cdot)$ ter $\delta(a + bi) = a^2 + b^2$.

Znano dejstvo iz kolobarja celih števil, znano pod imenom *»Bezoutova lema«*, v resnici velja v vseh glavnih kolobarjih. Namreč: $a, b \in K \setminus \{0\}$ imata največji skupni delitelj d, ki je oblike $d = ua + vb$ za neka $u, v \in K$

Trditev 4.9

Naj bo p neničelen element glavnega kolobarja K. Naslednje trditve so potlej ekvivalentne:

- p je nerazcepen.
- Ideal $\langle p \rangle$ je glavni.
- $K/\langle p \rangle$ je polje.

Definicija 4.10

Komutativen kolobar K se imenuje *noetherski*, če se vsaka naraščajoča veriga idealov kolobarja K

$$I_1 \subseteq I_2 \subseteq \ldots$$

ustavi, sepravi obstaja $n \in \mathbb{N}$, da je $I_n = I_{n+1} = \ldots$.

Trditev 4.11

Vsak komutativen kolobar, v katerem je vsak ideal končno generiran je noetherski.

Izrek 4.12: Hilbertov izrek o bazi

Če je K komutativen Noetherski kolobar, potem je tudi kolobar $K[X]$ noetherski.

Definicija 4.13

Naj bo K komutativen kolobar. Elementu $p \in K$ pravimo *praelement*, če ni ničelen in ni obrnljiv, ter iz

$$p \mid ab \implies p \mid a \text{ ali } p \mid b.$$

Evklidova lema iz $\mathbb{Z}$ motivira naslednjo trditev

Trditev 4.14

V vsakem celem kolobarju je vsak praelement nerazcepen, v glavnem kolobarju pa praelementi in nerazcepni elementi sovpadajo.

Definicija 4.15

Cel kolobar K imenujemo *kolobar z enoličnо faktorizacijo*, če za vsak $a \in K$, ki je neničelen in neobrnljiv, velja, da ga lahko zapišemo kot produkt nerazcepnih elementov, ter da je ta zapis enoličen do vrstnega reda ter asociiranosti natančno.

Trditev 4.16

- Za cel kolobar K velja naslednja veriga implikacij:

  $$K \text{ je evklidski} \implies K \text{ je glavni} \implies K \text{ je kolobar z enolično faktorizacijo}$$

- V kolobarju z enolično faktorizacijo praelementi ter nerazcepni elementi sovpadajo.

5 Razširitve polj

Izrek 5.1

Naj bo $\mathbb{F}$ polje ter p nerazcepen polinom nad $\mathbb{F}$. Potem obstaja razširitev polja $\mathbb{F}$, ki jo imenujmo $\mathbb{G}$, v kateri ima p ničlo.

Dokaz. Naj bo $\mathbb{G} = \mathbb{F}[x]/\langle p(x)\rangle$. Ker je p nerazcepen nad F je ideal $\langle p\rangle$ maksimalen, posledično je $\mathbb{G}$ polje. $\mathbb{G}$ vsebuje F, saj je restrikcija kanoničnega epimorfizma na $\mathbb{F}$ izomorfna $\mathbb{F}$. Naj bo $\overline{x}$ slika x pod kanoničnim epimorfizmom v $\mathbb{G}$. Velja:

$$p(\overline{x}) = \overline{p(x)} = p(x) = 0,$$

kar pomeni, da je odsek $x \bmod \langle p(x)\rangle$ ničla p v $\mathbb{G}$. □

Trditev 5.2

Naj bo $\theta = x \mod p(x)$ ničla p v $\mathbb{F}[x]/\langle p(x)\rangle$. Potem so elementi $1, \theta, \ldots, \theta^{n-1}$ baza $\mathbb{F}[x]/\langle p(x)\rangle$ kot vektorski prostor nad $\mathbb{F}$, kjer je n stopnja razširitve ter polinoma p.

Izrek 5.3

Naj so $F \subseteq K \subseteq L$ polja ter $[L : K], [K : F]$ končna. Potem je:

$$[L : F] = [L : K][K : F]$$

Dosti preprosto pridemo tudi do ugotovitve, da je razširitev polj končna natanko tedaj, ko jo generira končno mnogo algebraičnih elementov.

Literatura

[1] prof. dr. Matej Brešar. *Uvod v Algebro*. 2018.