KOMUTATIVNA ALGEBRA – Rešitev 7. domače naloge

(1a) Nalogo lahko rešimo na več načinov. Za vsak obseg K obstaja naravna preslikava $\mathbb{Z} \to K$, ki $1 \in \mathbb{Z}$ pošlje v enico obsega K. Slika binomskega koeficienta v $\mathbb{Z}$ je tako želeni binomski koeficient v K. Alternativni pristopi: induktivna definicija s pomočjo binomske identitete; lahko pa tudi razpišemo imenovalec in števec, ju faktoriziramo in opazimo, da v imenovalcu lahko krajšamo vse faktorje p (če je karakteristika obsega K enaka $p > 0$). Vse tri metode dajo enak rezultat.

(1b) Za polinom $f \in k[X]$ definiramo $\Delta f := f(X+1) - f(X)$ in rekurzivno še $\Delta^k := \Delta(\Delta^{k-1})$. S pomočjo indukcije lahko pokažemo, da je $\Delta^e X^d = \sum_{i=0}^{e} (-1)^{e-i} \binom{e}{i} (X+i)^d$ in hkrati $\Delta^e X^d = d(d-1)\cdots(d-e+1)X^{d-e}+$(členi z nižjimi potencami X–a). Postavimo $e = d-1$ in dobimo

$$\sum_{i=0}^{d-1} (-1)^{d-1-i} \binom{d-1}{i} (X+i)^d = d!X + h,$$

kjer je $h \in \mathbb{Z}$. Postavimo le še $X = 0$ in dobimo

$$\sum_{i=0}^{d-1} (-1)^{d-1-i} \binom{d-1}{i} i^d = h.$$

(1c) Trditev bomo dokazali nekoliko bolj splošno, kot to zahteva naloga. Natančneje: predpostavili bomo le, da je n tuj proti karakteristiki obsega ostankov kolobarja R, ki ima vsaj n elementov. Zato je dokaz nekoliko bolj zapleten, kot če bi dokazovali le trditev iz naloge (ki se preprosteje dokaže z uporabo identitete iz (b)).

Naj bo V celostno zaprtje kolobarja R v obsegu ulomkov K. Potem je V valuacijski podkolobar obsega K. Res, saj za vsak $x \in K$ velja $x^n \in V$ ali $(x^{-1})^n \in V$, torej iz celostne zaprtosti sledi $x \in V$ ali $x^{-1} \in V$. Naj bo $\mathfrak{M}$ maksimalni ideal kolobarja V. Potem je $R \cap \mathfrak{M}$ maksimalen ideal kolobarja R. Zato je $x^n \in R$ za vsak $x \in V$.

Sedaj bomo uporabili identiteto

$$(X+Y)^n - X^n - Y^n = \sum_{i=1}^{n-1} \binom{n}{i} X^{n-i} Y^i.$$

Za X vstavimo $x \in V$, medtem ko za Y zaporedoma vstavimo $n-1$ elementov $c_j \in R$, katerih ostanki v $R/(R \cap \mathfrak{M})$ so neničelni in paroma različni (obstajajo zaradi dodatne predpostavke o obsegu ostankov lokalnega kolobarja R). Dobimo sistem $n-1$ linearnih enačb

$$\sum_{i=1}^{n-1} \binom{n}{i} x^{n-i} c_j^i = d_j,$$

kjer $d_j = (x+c_j)^n - x^n - c_j^n \in R$. (Vandermondova) determinanta tega sistema je

$$\det[c_j^i]_{1 \leqslant i,j \leqslant n-1} = \prod_i c_j \prod_{i<j} (c_i - c_j)$$

in je neničelna v obsegu ostankov kolobarja R. Posledično je ta determinanta enota (obrnljiv element) v R in po Cramerjevem pravilu dobimo

$$\binom{n}{i}x^{n-i} \in R$$

za $1 \leqslant i \leqslant n-1$. Postavimo $i = n-1$ in dobimo $nx \in R$. Ker je n tuj proti karakteristiki obsega ostankov, je n enota v R. Sledi $x \in R$, kar smo želeli dokazati.

(1d) Naj bo K končen obseg, ki ima pravi podobseg k. Če je $\operatorname{card} K$=q, potem velja $K^{q-1} = \{0, 1\} \subseteq k$. Naj bo sedaj $(V, \mathfrak{m})$ poljuben valuacijski kolobar z obsegom ostankov K in naj bo $R := \{x \in V \mid x + \mathfrak{m} \in k\}$ kolobar tistih elementov, katerih ostanki ležijo v k. Potem je $V^n := \{v^n \mid v \in V\} \subseteq R \subsetneq V$.

(2a) Obe trditvi sta analogni. Za zgled dokažimo vložitev obsegov ostankov. Imamo naravni preslikavi $\mathcal{O}_v \hookrightarrow \mathcal{O}_u \twoheadrightarrow k_u$. Pri tem kompozitum očitno slika $\mathfrak{m}_v$ v 0. Torej inducira $\mathcal{O}_v \hookrightarrow \mathcal{O}_u$ naravno preslikavo $k_v \to k_u$, ki je očitno vložitev, saj je homomorfizem med dvema obsegoma.

(2b) Najprej opazimo, da za vsako valuacijo w in a, b z $w(a) \neq w(b)$ velja $w(a + b) = \min\{w(a), w(b)\}$ (tej enakosti pogosto pravimo *trikotniška enakost*). Za $x \in \mathcal{O}_u$ z $\bar{x}$ označimo njegovo sliko v k_u, torej $\bar{x} = x + \mathfrak{m}_u$.

Brez škode za splošnost smemo predpostaviti $v(a_1) \leqslant \cdots \leqslant v(a_f)$. Če sedaj množimo vse a_j z a_1^{-1}, opazimo, da smemo predpostaviti $v(a_1) = 0$ in dokazujemo $w(a_1x_1 + \cdots + a_fx_f) = 0$. Denimo nasprotno. Tedaj zaradi trikotniške neenakosti velja $w(a_1x_1 + \cdots + a_fx_f) > 0$. Torej je $\bar{a}_1\bar{x}_1 + \cdots + \bar{a}_f\bar{x}_f = 0$ in so $\bar{a}_i \in k_v$. Ker pa so bili $\bar{x}_i$ linearno neodvisni nad k_v, sledi $\bar{a}_i = 0$ za vsak i. Torej je $v(a_1) > 0$, kar je v nasprotju z našo predpostavko.

Trdimo, da so x_i linearno neodvisni nad K. Pa denimo nasprotno. Tedaj obstajajo $a_i \in K$, ne vsi enaki 0, za katere velja $a_1x_1 + \cdots + a_fx_f = 0$. Sledi

$$\infty = w(0) = w(a_1x_1 + \cdots + a_fx_f) = \min\{v(a_i)\} < \infty,$$

protislovje.

(2c) Naj bodo x_i kot v (2b) (obstajajo zaradi definicije f) in naj bo $\Gamma_w/\Gamma_v = \{\gamma_1 + \Gamma_v, \ldots, \gamma_e + \Gamma_v\}$. Poiščimo $y_i \in L$ z $w(y_i) = \gamma_i$. Trdimo, da je množica $\{x_iy_j \mid i = 1, \ldots, f,\ j = 1, \ldots, e\}$ linearno neodvisna nad K.

Naj bodo $\lambda_{ij} \in K$ poljubni, a ne vsi enaki 0. Trdimo, da je $\sum_{i,j} \lambda_{ij}x_iy_j \neq 0$. Velja

$$w(\sum_{i,j} \lambda_{ij}x_iy_j) = w\big(\sum_j(\sum_i \lambda_{ij}x_i)y_j\big).$$

Za vsak j velja $w(\sum_i \lambda_{ij}x_i) = \min_i\{v(\lambda_{ij})\} \in \Gamma_v$. Ker pa so y_j imeli vsi različne vrednosti modulo Γ_v, sledi $w(\sum_{i,j} \lambda_{ij}x_iy_j) = \min_{i,j}\{v(\lambda_{ij}) + \gamma_j\} < \infty$, torej $\sum_{i,j} \lambda_{ij}x_iy_j \neq 0$.

(2d) Po točki (c) je Γ_w/Γ_v končna grupa. V posebnem je Γ_w končno generirana Abelova grupa. Torej lahko uporabimo fundamentalni izrek o strukturi le–teh: $\Gamma_w \cong \mathbb{Z}^r \oplus G$, kjer je grupa G končna. Ker je Γ_w urejena in s tem brez torzije, je $G = \{0\}$. Sledi $\Gamma_w \cong \mathbb{Z}^r$. Vse, kar moramo še pokazati, je $r = 1$. Recimo, da je $r \geqslant 2$. Potem obstajata neničelna $\alpha, \beta \in \Gamma_w$ z lastnostjo $\mathbb{Z}\alpha \cap \mathbb{Z}\beta = \{0\}$. Ker je Γ_w/Γ_v končna, obstajata neničelna $r_\alpha, r_\beta \in \mathbb{Z}$, da velja $r_\alpha\alpha, r_\beta\beta \in \Gamma_v$. Sedaj uporabimo $\Gamma_v \cong \mathbb{Z}$. Obstajata $p_\alpha, p_\beta \in \mathbb{Z} \setminus \{0\}$, za katera velja $p_\alpha(r_\alpha\alpha) = p_\beta(r_\beta\beta)$. To pa je v nasprotju s predpostavko. Torej je $\Gamma_w \cong \mathbb{Z}$. (Vendar ne velja nujno $\Gamma_v = \Gamma_w$: glej npr. $\Gamma_v := 2\mathbb{Z} \subsetneq \mathbb{Z} =: \Gamma_w$.)

(3a) Za vsak $\gamma \in \Gamma_v$ definiramo dve ekvivalenčni relaciji na K: $x\bar{\gamma}y :\Longleftrightarrow v(x-y) > \gamma$ in $x\bar{\bar{\gamma}}y :\Longleftrightarrow v(x-y) \geqslant \gamma$. Naj bo C_γ množica vseh $\bar{\gamma}$–ekvivalenčnih razredov v K. Očitno je vsak $\bar{\gamma}$–ekvivalenčni razred X vsebovan v $\bar{\bar{\gamma}}$–ekvivalenčnem razredu $X^\star$. Preprosto je dokazati, da je kardinalnost množice $\bar{\gamma}$–ekvivalenčnih razredov, ki so vsebovani v danem $\bar{\bar{\gamma}}$–ekvivalenčnem razredu, natanko $\operatorname{card} k_v$. Torej obstaja $f_\gamma : C_\gamma \to k_v$, tako da za vsaka $X, Y \in C_\gamma$ iz $f_\gamma(X) = f_\gamma(Y)$ in $X^\star = Y^\star$ sledi $X = Y$.

Vsakemu $x \in K$ priredimo preslikavo $\hat{x} : \Gamma \to k_v$, ki γ pošlje v $f_\gamma(X)$. Tukaj smo z X označili $\bar{\gamma}$–ekvivalenčni razred x–a. Če sta $x, y \in K$ različna, potej sta $\hat{x}$ in $\hat{y}$ tudi različna, saj za $\gamma := v(x-y)$ velja $\hat{x}(\gamma) \neq \hat{y}(\gamma)$. Torej je ˆ vložitev K v $k_v^{\Gamma_v}$. S tem je trditev dokazana.

(3b) Naj bo $\mathfrak{A}$ množica vseh (paroma neizomorfnih) maksimalnih neposrednih razširitev obsega z valuacijo (K, v) (pozor: $\mathfrak{A}$ je res množica po točki (a), saj lahko izračunamo njeno kardinalnost). S preprosto uporabo Zornove leme pokažemo, da v $\mathfrak{A}$ obstajajo maksimalni elementi glede na urejenost

$$(L_1, v_1) \subseteq (L_2, v_2) \quad :\Longleftrightarrow \quad L_1 \subseteq L_2 \ \wedge\ v_2|_{L_1} = v_1.$$

Vsak tak element pa je maksimalna neposredna razširitev.