Kako se lotiš: Algebra 3

Patrik Žnidaršič

Prevedeno 2. junij 2024

1 Galoisova teorija

1.1 Razširitve polj

Pri določanju stopnje razširitve $F(a_1, \ldots, a_n)$ zapišemo vmesne razširitve, in si pomagamo z naslednjo trditvijo:

Trditev. *Naj bo F polje in $a_1, \ldots, a_n$ algebrajski nad F. Potem velja*

- $|F(a_1, \ldots, a_n) : F| = |F(a_1, \ldots, a_n) : F(a_1, \ldots, a_{n-1})| \cdots |F(a_1) : F|$,
- $|F(a_1, \ldots, a_n) : F| \leq |F(a_1) : F| \cdots |F(a_n) : F|$,
- *če imata $|F(a_1) : F|$ in $|F(a_2) : F|$ največji skupni delitelj enak 1, velja $|F(a_1, a_2) : F| = |F(a_1) : F| \cdot |F(a_2) : F|$.*

Stopnje posameznih razširitev lahko ocenimo (najbolj enostavno, če $a_2 \notin F(a_1)$, je $|F(a_1, a_2) : F(a_1)| \geq 2$), ali pa poiščemo minimalni polinom, katerega stopnja je enaka stopnji razširitve. Za minimalni polinom je dovolj, da je nerazcepen, in da ima ničlo a_2; pogosto pa je že to težko. Če je p praštevilo, je $1 + x + x^2 + \cdots + x^{p-1}$ CIKLOTONIČEN POLINOM, ki je nerazcepen nad $\mathbb{Q}$. Za polinome nad $\mathbb{Q}$ imaš na voljo tudi Eisensteinov kriterij:

Trditev. *Naj bo $p(x) = a_n x^n + \cdots + a_0$ polinom s koeficienti v $\mathbb{Z}$. Če obstaja praštevilo p, ki deli vse koeficiente razen a_n, in p^2 ne deli a_0, potem je p nerazcepen nad $\mathbb{Q}$.*

Izrek. *Naj bo $f \in F[X]$ nekonstanten nerazcepen polinom. Naslednje trditve so ekvivalentne:*

- *f ima večkratno ničlo v razpadnem polju,*
- $\gcd(f, f') \neq 1$,
- *f je polinom v x^q, kjer je q karakteristika polja F,*
- *vse ničle v razpadnem polju so večkratne.*

Trditev. *Naj bo $f(X) \in F[X]$ polinom stopnje n. Potem $|F(p) : F|$ deli $n!$.*

1.2 Normalne in separabilne razširitve

Za polinom $p(X) \in F[X]$ je razpadno polje p najmanjša razširitev E, za katero so vse ničle v E. Določeno je do izomorfizma natančno, označimo ga z $F(p)$. Če imamo izomorfizem polje $\sigma : F \to F'$, ga lahko vedno razširimo do izomorfizma razpadnih polj.

Definicija. Končna razširitev E/F je NORMALNA, če za vsak nerazcepen polinom $p(X) \in F[X]$ bodisi p nima ničle v E, bodisi ima vse ničle v E.

Izrek. *Končna razširitev E/F je normalna natanko tedaj, ko je E razpadno polje nekega polinoma s koeficienti iz F.*

Definicija. Polinom $p(X) \in F[X]$ je SEPARABILEN, če ima same enostavne ničle. Končna razširitve E/F je SEPARABILNA, če je za vsak $a \in E$ minimalni polinom separabilen.

Če je karakteristika polja enaka 0, in je polinom nerazcepen, so vse njegove ničle enostavne. V tem primeru je vsaka končna razširitev separabilna; polju s to lastnostjo pravimo PERFEKTNO. Poleg polj s karakteristiko 0 vemo, da so tudi vsa končna polja perfektna.

Izrek (primitivni element)**.** *Vsaka separabilna razširitev je enostavna (tj. obstaja $a \in E$, da je $E = F(a)$).*

1.3 Galoisove grupe in razširitve

Definicija. GALOISOVA GRUPA razširitve E/F je grupa

$$\mathrm{Gal}(E/F) = \{\sigma \in \mathrm{Aut}\, E \mid \sigma|_F = \mathrm{id}_F\}.$$

Elementom te grupe pravimo F-AVTOMORFIZMI polja E.

Galoisovo grupo polinoma $p(X) \in F[X]$ definiramo kot $\mathrm{Gal}(p) = \mathrm{Gal}(F(p)/F)$. Normalnim separabilnim razširitvam pravimo GALOISOVE RAZŠIRITVE. Če ima F karakteristiko 0, je za polinom $p(X) \in F[X]$ je $F(p)/F$ vedno Galoisova; to je končna razširitev, torej je normalna (ker je $F(p)$ razpadno polje), in separabilna, ker ima polje karakteristiko 0. Pri določanju Galoisove grupe si pomagamo z naslednjo trditvijo:

Trditev. *Naj bo E/F končna Galoisova razširitev. Potem je $|\mathrm{Gal}(E/F)| = |E : F|$. Če je E/F končna separabilna, je $|\mathrm{Gal}(E/F)| \leq |E : F|$.*

Pogledamo torej stopnjo razširitve, da vemo, koliko elementov bo v grupi. Potem te elemente poiščemo. V primeru razpadnega polja pride prav naslednja lema:

Lema. *Če je $a \in E$ ničla polinoma $p(X) \in F[X]$ ter $\sigma \in \mathrm{Gal}(E/F)$, je tudi $\sigma(a)$ ničla $p(X)$.*

Avtomorfizme iščemo tako, da si izberemo, kam bomo slikali ničle. Če jih najdemo dovolj, vemo, da je to to. Potem moramo le določiti, kaj točno je grupa. Najbolj enostavno je preveriti komutativnost in red elementov (torej poiskanih avtomorfizmov). Spomnimo se klasifikacijo končnih Abelovih grup:

Izrek. *Vsaka končna Abelova grupa je vsota cikličnih grup, katerih red je potenca praštevila.*

Rezultat, ki bizarno redko pride prav, je fundamentalni izrek Galoisove teorije:

Izrek. *Naj bo E/F končna Galoisova razširitev.*

- *Predpisa* $L \mapsto \mathrm{Gal}(E/L)$ *in*

$$G \mapsto \{x \in E \mid g \cdot x = x \ \forall g \in G\}$$

  sta paroma inverzni preslikavi med vmesnimi polji $F \subseteq L \subseteq E$ *in podgrupami Galoisove grupe.*

- *Za poljubni vmesni polji* $F \subseteq L \subseteq M \subseteq E$ *velja* $|M : L| = |\mathrm{Gal}(E/L) : \mathrm{Gal}(E/M)|$.

- *Za vmesno polje* $F \subseteq L \subseteq E$ *je* L/F *normalna natanko tedaj, ko je* $\mathrm{Gal}(E/L) \triangleleft \mathrm{Gal}(E/F)$.

1.4 Rešljivost grup

Definicija. Grupa G je REŠLJIVA, če obstaja končno zaporedje podgrup

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_k = G,$$

za katere velja $G_i \triangleleft G_{i+1}$ in G_{i+1}/G_i Abelova.

Naslednje grupe so dokazano rešljive:

- Abelove grupe,
- končne p-grupe,
- D_{2n},
- vsaka grupa reda pq, kjer sta p, q praštevili

Vse podgrupe in kvocienti rešljivih grup so rešljivi. Če sta N in G/N rešljivi za edinko $N \triangleleft G$, je tudi G rešljiva.

2 Moduli

Modul je algebrajska struktura nad kolobarjem R, v kateri dovolimo seštevanje in množenje s skalarjem z leve. Veljajo vse običajne definicije, kar se tiče algebrajskih struktur. Če je $X = \{x_1, \ldots, x_n\}$, je podmodul, generiran z X, enak

$$\langle X \rangle = \{r_1 x_1 + \cdots + r_n x_n \mid r_i \in R\}.$$

Če je modul generiran z enim elementom, pravimo, da je CIKLIČEN. Vsak enostaven modul (tj. tak, ki nima netrivialnih podmodulov) je cikličen.

Množici X, za katero je $M = \langle X \rangle$ in za katero iz enakosti $r_1x_1 + \cdots + r_nx_n = 0$ sledi $r_i = 0$ za vsak i, pravimo BAZA. Če ima modul bazo, je PROST. Velja naslednja karakterizacija:

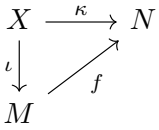
Izrek. *Naj bo M R-modul. Naslednje trditve so ekvivalentne:*

- *M je prost R-modul*
- *Obstaja indeksna množica Λ, da je M kot R-modul izomorfen*

$$M \cong \bigoplus_{\lambda \in \Lambda} R$$

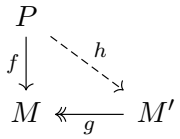
- *Obstaja množica X in preslikava $\iota : X \to M$, da za vsak R-modul N in vsako preslikavo $\kappa : X \to N$ obstaja natanko en homomorfizem $f : M \to N$, za katerega je $f \circ \iota = \kappa$.*

Zadnji točki pravimo UNIVERZALNA LASTNOST. Pripada ji naslednji komutativni diagram:



2.1 Projektivni moduli

Definicija. R-modul P je PROJEKTIVEN, če za vsak homomorfizem R-modulov $f : P \to M$ in vsak epimorfizem R-modulov $g : M' \to M$ obstaja homomorfizem R-modulov $h : P \to M'$, da naslednji diagram komutira:



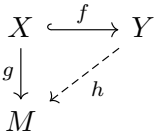
Vsak prost R-modul je projektiven. Dodatno velja naslednja karakterizacija:

Izrek. *Za R-modul P je ekvivalentno:*

- *P je projektiven*
- *za vsak epimorfizem $\varphi : M \to P$ je $M = P \oplus \ker \varphi$*
- *obstaja R-modul M, da je $P \oplus M$ prost R-modul*

Poznamo tudi INJEKCIJSKE MODULE; če je M injekcijski modul, za vsak R-modul Q z $M \leq Q$ obstaja $K \leq Q$, za katerega je $Q = M \oplus K$. Ekvivalentno, če za vsako injektivno

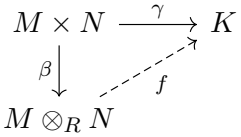
$f : X \to Y$ in vsak $g : X \to M$ obstaja $h : Y \to M$, da spodnji diagram komutira:



2.2 Tenzorski produkt

V tem razdelku je R vedno komutativni kolobar z enico. Definicija tenzorskega produkta je grozno kompliciranа, zato raje uporabljamo univerzalno lastnost, s katero lahko definiramo preslikave iz tenzorskega produkta:

Izrek. *Naj bodo M, N, K R-moduli. Za vsako bilinearno $\gamma : M \times N \to K$ obstaja natanko en homomorfizem R-modulov $f : M \otimes_R N \to K$, da naslednji diagram komutira:*



Kot prostor si tenzorski produkt lahko predstavljamo prostor linearnih kombinacij elementarnih tenzorjev $a \otimes b$, pri čemer imajo elementi lahko več predstavitev. Preslikava $(a, b) \mapsto a \otimes b$ je bilinearna, torej lahko konstante (iz R) nesemo ven iz zapisa, če to želimo. Velja $M \otimes_R N \cong N \otimes_R N$. Poleg tega je tenzorski produkt do izomorfizma natančno asociativen in distributiven z direktno vsoto $\oplus$.

3 Teorija kategorij

KATEGORIJA je sestavljena iz razreda objektov in množic morfizmov med vsakim parom objektov. Morfizme lahko komponiramo, za kompozicijo zahtevamo asociativnost in obstoj enote (za vsak objekt).

Morfizem $A \to B$ je

- IZOMORFIZEM, če obstaja morfizem $g : B \to A$, da je $f \circ g = 1_B$ in $g \circ f = 1_A$.
- PREREZ, če obstaja $g : B \to A$, da je $g \circ f = 1_A$
- RETRAKT, če obstaja $g : B \to A$, da je $f \circ g = 1_B$
- MONOMORFIZEM, če velja pravilo krajšanja iz leve: $f \circ g = f \circ h \implies g = h$
- EPIMORFIZEM, če velja pravilo krajšanja iz desne: $g \circ f = h \circ f \implies g = h$

Za objekt pravimo, da je ZAČETNI, če obstaja natanko en morfizem iz tega objekta na poljuben drug objekt. Podobno je KONČNI OBJEKT tak, na katerega obstaja natanko

en morfizem iz poljubnega drugega objekta. Poljubna začetna ali končna objekta sta izomorfna.

Definicija. Naj bosta C in D kategoriji. FUNKTOR med C in D je predpis F, za katerega velja:

- za vsak objekt A v C imamo natanko določen objekt $F(A)$ v D
- za vsak morfizem $f : A \to B$ imamo natanko določen morfizem $F(f) : F(A) \to F(B)$
- $F(1_A) = 1_{F(A)}$
- $F(f \circ g) = F(f) \circ F(g)$

Definiramo lahko tudi kofunktorje, kjer obrnemo vrstni red v drugi in četrti točki. Kofunktor je funktor med nasprotnima kategorijama C^{op} in D^{op}.

Definicija. Naj bosta F, G funktorja iz C v D. NARAVNA TRANSFORMACIJA med F in G je nabor morfizmov $\mu_A : F(A) \to G(A)$ za objekte A iz C. Zahtevamo, da so ti morfizmi kompatibilni z morfizmi v C: za vsak $f : A \to B$ mora naslednji diagram komutira:

$$\begin{array}{ccc} F(A) & \xrightarrow{F(f)} & F(B) \\ {\scriptstyle \mu_A}\downarrow & & \downarrow{\scriptstyle \mu_B} \\ G(A) & \xrightarrow[G(f)]{} & G(B) \end{array}$$

Pravimo, da sta funktorja F in G NARAVNO IZOMORFNA, če obstaja naravna transformacija $\mu : F \to G$, za katero so vsi morfizmi μ_A izomorfizmi. Za kategoriji C in D pravimo, da sta EKVIVALENTNI, če obstajata funktorja $F : C \to D$ in $G : D \to C$ in naravna izomorfizma $F \circ G \to \mathrm{id}_D$ ter $G \circ F \to \mathrm{id}_C$.

Definicija. Naj bosta A, B objekta kategorije C. PRODUKT objektov A in B je objekt P, skupaj z morfizmoma $p : P \to A$ in $q : P \to B$, da za poljuben objekt X in poljubna morfizma $f : X \to A$ in $g : X \to B$ obstaja natanko en morfizem $h : X \to P$, da diagram komutira:

$$\begin{array}{ccccc} A & \xleftarrow{p} & P & \xrightarrow{q} & B \\ & {\scriptstyle f}\searrow & {\scriptstyle h}\uparrow & \nearrow{\scriptstyle g} & \\ & & X & & \end{array}$$

Podobno definiramo koprodukt, kjer le obrnemo puščice:

$$\begin{array}{ccccc} A & \xrightarrow{p} & P & \xleftarrow{q} & B \\ & \searrow{\scriptstyle f} & \downarrow{\scriptstyle h} & {\scriptstyle g}\swarrow & \\ & & X & & \end{array}$$

Nekatere kategorije premorejo GENERATORJE, torej objekte G, za katere za vsaka različna $f, g : A \to B$ obstaja $h : G \to A$, da je $f \circ h \neq g \circ h$.

Za kategorijo pravimo, da je KONKRETNA, če so objekti množice in morfizmi preslikave. V tem primeru lahko za neprazno množico X definiramo PROSTI OBJEKT nad X kot tak objekt F, skupaj s preslikavo $\iota : X \to F$, da za vsak objekt C in vsako preslikavo $f : X \to C$ obstaja natanko en morfizem $\tilde{f} : F \to C$, da komutira diagram

$$\begin{array}{ccc} X & \xrightarrow{f} & C \\ {\scriptstyle\iota}\downarrow & \nearrow_{\tilde{f}} & \\ F & & \end{array}$$

V konkretni kategoriji za morfizem veljata naslednji verigi implikacij:

$$\begin{aligned} \text{prerez} &\implies \text{injekcija} \implies \text{monomorfizem} \\ \text{retrakt} &\implies \text{surjekcija} \implies \text{epimorfizem} \end{aligned}$$

4 Teorija upodobitev

Definicija. UPODOBITEV R-algebre A nad modulom V je homomorfizem algeber $\rho : A \to \mathrm{End}_R(V)$.

Najbolj relevantna algebra je t.i. grupna algebra RG, prosti R-modul nad G.

Definicija. A-modul V je ENOSTAVEN, če ima le trivialna podmodula. Modul je POLENOSTAVEN, če je končna direktna vsota enostavnih.

Izrek (Maschke)**.** *Naj bo G končna grupa in F polje. Predpostavimo, da karakteristika F ne deli $|G|$. Naj bo $\rho : G \to \mathrm{GL}_F(V)$ upodobitev grupe G, kjer je V končnodimenzionalen modul nad F. Naj bo W G-podmodul V. Potem obstaja G-podmodul X, da je $V = W \oplus X$.*

Kot posledica je vsak končnorazsežen G-modul polenostaven.

Lema (Schur)**.** *Naj bo A F-algebra in S_1, S_2 enostavna A-modula. Če je $S_1 \ncong S_2$, je $\mathrm{Hom}(S_1, S_2) = \{0\}$. Če je $S_1 \cong S_2$, je $\mathrm{End}_A(S_1)$ obseg. Če je F algebraično zaprto polje, je $\mathrm{End}_A(S_1) \cong F$.*

Izrek (Artin-Wedderburn)**.** *Naj bo A končnorazsežna algebra nad poljem F, za katero je vsak končno generiran A-modul polenostaven. Recimo, da je A kot A-modul oblike $A = S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$, kjer so S_i paroma neizomorfni enostavni A-moduli in $S_i^{n_i}$ n_i-kratna direktna vsota. Potem je A kot F-algebra izomorfna direktni vsoti matrik $M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r)$, kjer so $D_i = \mathrm{End}_A(S_i)^{op}$. Če je F algebraično zaprto, je $D_i = F$.*

Izreka imata nekaj posledic. Če karakteristika F ne deli $|G|$, je vsaka upodobitev grupe G povsem razcepna (torej je za vsako upodobitev $G \to \mathrm{GL}_F(V)$ modul V polenostaven FG-modul). Do ekvivalence natančno ima grupa le končno mnogo nerazcepnih upodobitev, $\rho_1, \ldots, \rho_r$; v kolikor je F algebraično zaprto, je $n_1^2 + \cdots + n_r^2 = |G|$.