Radikal ideala.

Radikal ideala $I \subset A$ je skup $\sqrt{I} = r(I) = \{a \in A \,|\exists n \in N, a^n \in A\}$. To je ideal u A (prvi dokaz: direktni, drugi dokaz: $\sqrt{I} = \varphi^{-1}((\mathrm{nil}\, A/I))$ gde je $\varphi : A \to A/I$ kanonski epimorfizam).

Tvrdjenje. Radikal ideala ima sledeće osobine.

(1) $\sqrt{I} \supset I$;

(2) $\sqrt{\sqrt{I}} = \sqrt{I}$;

(3) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$;

(4) $\sqrt{I} = (1) \Leftrightarrow I = (1)$;

(5) $\sqrt{\sqrt{I} + \sqrt{J}} = \sqrt{I + J}$;

(6) Ako je P prost ideal, tada je za svako $n \in \mathbb{N}$, $\sqrt{P^n} = P$;

(7) Radikal $\sqrt{I}$ je presek svih prostih ideala koji sadrže I (uputstvo za dokaz: uočiti nilradikal faktorprstena A/I).

Ideal I je *radikalan* ako je $I = \sqrt{I}$. Lako se vidi da je I radikalan ako i samo ako je $I = \sqrt{J}$ za neki ideal J. Svaki prost ideal je radikalan, ali obratno ne važi. Primer: u prstenu $\mathbb{Z}$, $\sqrt{(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k})} = (p_1 p_2 \ldots p_k)$, a ovaj ideal je radikalan. On je prost $\Leftrightarrow k = 1$.

Kratka ekskurzija: topološki prostori

Ideja topološkog prostora nastala je prilikom aksiomatizacije pojma blizine koja ne bi koristila pojam rastojanja odnosno metrike.

Definicija. Topološki prostor je skup X zajedno sa familijom svojih podskupova $\mathcal{T} = \{U_i \,| U_i \subset X, i \in I\} \subset \mathcal{P}(X)$ koja zadovoljava sledeće uslove:

(1) $\varnothing \in \mathcal{T}$, $X \in \mathcal{T}$;

(2) $U_j \in \mathcal{T}$ $(j \in J) \Longrightarrow \cup_{j \in J} U_j \in \mathcal{T}$;

(3) U_i, $U_j \in \mathcal{T} \Longrightarrow U_i \cap U_j \in \mathcal{T}$.

Elementi familije $\mathcal{T}$ nazivaju se *otvorenim skupovima* topološkog prostora X.

Uslovi u definiciji označavaju sledeće: prazan skup i ceo prostor su otvoreni, unija proizvoljne familije otvorenih skupova je otvorena i presek konačne familije otvorenih skupova je otvoren.

Skup $V \subset X$ je *zatvoren* ako je njegov komplement $X \backslash V$ otvoren. Prazan skup i ceo prostor su zatvoreni, presek proizvoljne familije zatvorenih skupova je zatvoren i unija konačne familije zatvorenih skupova je zatvorena. Jasno je da se topologija može zadati i zadavanjem familije svih zatvorenih skupova.

Primer. Uobičajeni pojam otvorenog skupa na realnoj pravoj $\mathbb{R}$ kao podskupa $U \subset \mathbb{R}$ čija je svaka tačka $x \in U$ unutrašnja, tj. takva da postoji ceo interval $(x - \varepsilon, x + \varepsilon)$ koji leži u U, pretvara $\mathbb{R}$ u topološki prostor.

Zatvoreni intervali $[a, b]$ su zatvoreni skupovi, jer je njihov komplement $(-\infty, a)\,(b, \infty)$ otvoren kao unija dva otvorena intervala. Naravno, to nisu jedini zatvoreni skupovi - setite se primera Kantorovog skupa.

Pojam se lako prenosi na metrički prostor $\mathbb{R}^n$ za svako n: otvoreni skup u metričkom prostoru $\mathbb{R}^n$ (za svako n) je podskup $U \subset \mathbb{R}^n$ čija je svaka tačka $x \in U$ unutrašnja, tj. takva da postoji cela kugla $K(x, \varepsilon) \subset U$.

Ovu topologiju nazivamo standardnom topologijom $\mathbb{R}^n$. Primetimo da je svaki otvoreni skup u $\mathbb{R}$ odnosno $\mathbb{R}^n$ unija intervala odnosno kugli.

Definicija. Potfamilija $\mathcal{B}$ topologije $\mathcal{T}$ topološkog prostora X naziva se *baza topologije* $\mathcal{T}$ ako je svaki otvoreni skup unija baznih otvorenih skupova.

Otvoreni intervali (a, b) čine bazu standardne topologije u $\mathbb{R}$, a kugle $K(a, \varepsilon)$ - u metričkom prostoru $\mathbb{R}^n$ za proizvoljno n.

Spektar prstena i spektralna topologija

Neka je A prsten (komutativni prsten sa jedinicom).

Definicija. *Spektar* prstena $\operatorname{Spec} A$ je skup svih prostih ideala, a *maksimalni spektar* $\operatorname{Max} A$ (ili $\operatorname{Specm} A$) $\subset \operatorname{Spec} A$ je podskup maksimalnih ideala. Spektar postaje topološki prostor (v. dalje) ako se topologizira familijom zatvorenih skupova oblika $\{V(S)\,|S \subset A\}$ gde je $V(S) = \{P \in \operatorname{Spec} A\,|S \subset P\}$. Naime, lako se vidi da je $V(S_1) \cup V(S_2) = V(S_1 S_2)$, $\cap_{i\in I} V(S_i) = V(\cup_{i\in I} S_i)$, $V(0) = \operatorname{Spec} A$ i $V(1) = \emptyset$. Isto tako, očigledno je $V(S) = V((S))$. Ova topologija naziva se *topologija Zariskog* ili *spektralna topologija*. Umesto $V(\{f\})$ piše se jednostavno $V(f)$. Dakle, $V(f) = \{P \in \operatorname{Spec} A\,|P \ni f\}$.

Tvrdjenje. Skupovi $D(f) := (\operatorname{Spec} A)\backslash V(f)$ čine bazu topologije Zariskog u $\operatorname{Spec} A$ i nazivaju se *glavni otvoreni skupovi*.

Naime, $\operatorname{Spec} A \backslash V(S) = D(S) = D(\underset{f\in S}{\cup}\{f\}) = (\operatorname{Spec} A)\backslash V(\underset{f\in S}{\cup}\{f\}) = (\operatorname{Spec} A)\backslash \underset{f\in S}{\cap} V(f) = \underset{f\in S}{\cup} D(f)$.

Za proizvoljni podskup $X \subset \operatorname{Spec} A$ definišimo ideal $I(X) = \cap\{P\,|P \in X\} \subset A$.

Tvrdjenje. (1) $V(I(X)) = \bar{X}$ (zatvorenje u topologiji Zariskog).

(2) $I(V(S)) = \sqrt{(S)}$ (radikal ideala generisanog sa S).

Dokaz. (1) Očigledno, skup $V(I(X))$ je zatvoren i sadrži X. Neka je $V(S)$ neki drugi zatvoreni skup takav da $X \subset V(S)$. Tada je $P \in X \Rightarrow S \subset P$, pa je $P \in V(I(X)) \Rightarrow P \supset I(X) = \cap\{P\,|P \in X\} \supset S \Rightarrow P \in V(S)$.

(2) $\sqrt{(S)} = \cap\{P\,|P \supset (S)\} = \cap\{P\,|P \in V(S)\} = I(V(S))$.

Posledica: Preslikavanje $V : I \mapsto X$ definiše obostrano jednoznačnu korespondenciju izmedju radikalnih ideala u A i zatvorenih skupova u $\operatorname{Spec} A$, sa inverzom $I = V^{-1}$.

Naravno, ako se ne ograničimo radikalnim idealima, korespondencija nije jednoznačna.

Primeri (1) Koordinatni početak se može zadati kao $V(I)$ za bilo koji ideal $I = (x^n, y^m)$. Pri tome je $\sqrt{I} = (x, y)$ odgovarajući radikalni ideal, koji je i prost pa čak i maksimalan.

(2) Koordinatna osa $x = 0$ se zadaje i drugim idealima, recimo idealom $(x^2, xy) = (x) \cap (x^2, y) = (x) \cap (x, y)^2$, a njegov radikal je $\sqrt{(x^2, xy)} = \sqrt{(x)} \cap \sqrt{(x, y)} = (x) \cap (x, y) = (x)$.

Primeri (1) $\operatorname{Spec} \mathbb{Z} = \{(0), (2), (3), (5), (7), (11), \ldots, (p), \ldots\}$. Pri tome, $\overline{(p)} = (p)$ a $\overline{(0)} = \operatorname{Spec} \mathbb{Z}$. Dakle, u topološkom prostoru $\operatorname{Spec} A$ mogu postojati i nezatvorene tačke, tj. čak ni aksioma separacije T_1 ne mora biti zadovoljena[1].

(2) Neka je $A = \mathbb{Z} + \mathbb{Z}i = \mathbb{Z}[i]$ tzv. *prsten Gausovih brojeva*. Može se pokazati da je ovaj prsten euklidski (algoritam deljenja s ostatkom se bazira na normi $v(a + bi) = a^2 + b^2$) pa je zato i glavnoidealski. Pošto je A domen, ideal (0) je prost. Ako je $(a + bi)$ prost ideal u A, tada je $(a + bi) \cap \mathbb{Z} = (p)$ prost ideal u $\mathbb{Z}$. Prost broj p mora zato biti oblika $(a + bi)(c + di)$ u A, odakle sledi da je $p = (a+bi)(a-bi) = a^2 + b^2$. Očigledno, $2 = (1+i)(1-i)$. Na osnovu teoreme koju je prvi formulisao Ferma, a dokazao Lagranž (dokaz koristi teoriju celobrojnih kvadratnih formi), ako je $p \equiv 1 \bmod 4$, onda je $p = a^2 + b^2$ suma kvadrata dva cela broja: na primer, $5 = 2^2 + 1^2$. Ako je pak $p \equiv 3 \bmod 4$ tada se p ne može predstaviti kao suma kvadrata dva cela broja. Odavde sledi da $\operatorname{Spec} A$ ima ove tačke: ideal (0), ideal $(1 + i)$ (koji je jednak idealu $(1 - i)$, jer je $i \cdot (1 - i) = 1 + i$), za svaki prost broj $p \equiv 3 \bmod 4$ jedan ideal (p), a za svaki prost broj $p \equiv 1 \bmod 4$ dva (različita) ideala $(a + bi)$ i $(a - bi)$. Slika:

Ako je $h : A \to B$ homomorfizam prstena, možemo definisati preslikavanje ${}^a h : \operatorname{Spec} B \to \operatorname{Spec} A$ na sledeći jednostavan način: inverzna slika prostog ideala $Q \subset B$ je prost ideal, pa možemo staviti ${}^a h(Q) = h^{-1}(Q) \in \operatorname{Spec} A$

Tvrdjenje. Preslikavanje ${}^a h$ je neprekidno u topologiji Zariskog. Dodeljivanje ${}^a(-) : Hom_{Ring}(A, B) \to Hom_{Top}(\operatorname{Spec} B, \operatorname{Spec} A)$ je kontravarijantni

[1] Aksioma separacije T_0: za svake dve različite tačke $x, y \in X$ postoji otvorena okolina jedne od njih koja ne sadrži drugu.

Aksioma separacije T_1: za svake dve različite tačke $x, y \in X$ postoje otvorene okoline $U \ni x$, $V \ni y$ takve da $y \notin U$, $x \notin V$.

Aksioma separacije T_2 (Hausdorfova aksioma): za svake dve različite tačke $x, y \in X$ postoje otvorene okoline $U \ni x$, $V \ni y$ takve da je $U \cap V = \emptyset$.

funktor (v. kasnije "Jezik kategorija i funktora").

Dokaz. Preslikavanje ${}^a h$ je neprekidno ako je inverzna slika $({}^a h)^{-1}$ svakog otvorenog skupa otvorena. Pošto inverzna slika prolazi kroz unije, dovoljno je to pokazati za bazne otvorene skupove $D(f) \subset \operatorname{Spec} A$, $f \in A$. Neka je $Q \in \operatorname{Spec} B$, $Q \in ({}^a h)^{-1}(D(f))$. To znači da je ${}^a h(Q) = h^{-1}(Q) = P \in D(f)$ odnosno da $f \in P$ i $h(f) \in Q$, dakle $Q \in D(h(f))$. Dakle, $({}^a h)^{-1}(D(f)) = D(h(f))$ je otvoren, što dokazuje da je ${}^a h$ neprekidno.

Primetimo da on ne mora biti bijektivan na morfizmima. Moguće su obe krajnosti. Recimo, $\operatorname{Hom}_{Ring}(\mathbb{Z}, \mathbb{Z}) = \{id\}$ je jednoelementan skup, a $Hom_{Top}(\operatorname{Spec} \mathbb{Z}, \operatorname{Spec} \mathbb{Z})$ je beskonačan (sve permutacije zatvorenih tačaka (p) su neprekidna preslikavanja). Obrnuto, $Hom_{Ring}(\mathbb{R}, \mathbb{R})$ je beskonačan skup automorfizama polja realnih brojeva, a $\operatorname{Spec} \mathbb{R}$ je jedna tačka i $Hom_{Top}(\operatorname{Spec} \mathbb{R}, \operatorname{Spec} \mathbb{R}) = \{*\}$ je jednoelementan.

Tvrdjenje. (1) $V(I) \approx \operatorname{Spec} A/I$; (2) $D(f) \approx \operatorname{Spec} A_f$.

Tvrdjenje. Topologija Zariskog je kompaktna i T_1, a ne mora biti T_2.

Dokaz. Neka je presek familije zatvorenih skupova prazan: $\bigcap_{i \in I} V(S_i) = V\left(\bigcup_{i \in I} S_i\right) = \emptyset = V(1)$. Odatle je $1 \in \sqrt{\left(\bigcup_{i \in I} S_i\right)}$ i sledi da je $1 = a_1 s_1 + \cdots + a_k s_k$ za neke $s_m \in S_{i_m}$ $(m = 1, \ldots, k)$. Zato je $1 \in (S_{i_1} \cup \cdots \cup S_{i_m})$ i $\emptyset = V(S_{i_1}) \cap \cdots \cap V(S_{i_k})$.

Lokalni prsteni. Proširenje (ekstenzija, going-up) i suženje (kontrakcija, going-down)

Neka je $h : A \to B$ homomorfizam prstena. Inverzna slika ideala $J \subset B$ je ideal $I = h^{-1}(J)$, koji se naziva *kontrakcijom* ideala J i obeležava $I = J^c$. Za ideal J^c kažemo još da se nalazi *pod* idealom J. Direktna slika $h(I)$ ideala $I \subset A$ ne mora biti ideal u B. Ideal $J = (h(I)) = Bh(I)$ generisan tim skupom naziva se *ekstenzijom* ideala I i obeležava $J = I^e$. Kažemo još da se ideal I^e nalazi *nad* idealom I.

Ako homomorfizam h faktorišemo kao kompoziciju projekcije i inkluzije $A \underset{p}{\to} A/\operatorname{Ker} h \cong \operatorname{Im} h \underset{i}{\hookrightarrow} B$, $h = i \circ p$, tada projekcija p uspostavlja obostrano-jednoznačnu korespondenciju izmedju ideala u A koji sadrže $\operatorname{Ker} h$ i ideala u $A/\operatorname{Ker} h$, pa je problem kontrakcije i ekstenzije ideala vezan za ponašanje inkluzije i. Ponašanje ekstenzije i kontrakcije opisano je sledećim tvrdjenjem.

Tvrdjenje. (1) $I^{ec} \supset I$, $J^{ce} \subset J$;

(2) Ekstenzija i kontrakcija su monotona preslikavanja u odnosu na inkluz-

iju;

(3) $I^{ece} = I^e$, $J^{cec} = J^c$;

(4) Neka je $\mathcal{C}$ skup svih kontrahovanih ideala u A tj. $\mathcal{C} = \{J^c \,|\, J \text{ ideal u } B\}$ i $\mathcal{E}$ skup svih ekstendiranih ideala u B tj. $\mathcal{E} = \{I^e \,|\, I \text{ ideal u } A\}$. Tada je $\mathcal{C} = \{I \,|\, I^{ec} = I\}$, $\mathcal{E} = \{J \,|\, J^{ce} = J\}$, i preslikavanja $(-)^e : I \to I^e$, $(-)^c : J \mapsto J^c$ predstavljaju obostrano jednoznačne uzajamno inverzne korespondencije izmedju skupova $\mathcal{C}$ i $\mathcal{E}$.

Dokaz. (1) Ako $a \in I$, tada $h(a) \in h(I) \subset Bh(I)$ pa $a \in h^{-1}(Bh(I)) = I^{ec}$. S druge strane, $h(h^{-1}(J)) \subset J$ pa je i $J^{ce} = Bh(h^{-1}(J)) \subset BJ \subset J$;

(2) je očigledno;

(3) Imamo $I^{ece} = (I^{ec})^e \supset I^e$ i istovremeno $I^{ece} = (I^e)^{ce} \subset I^e$. Isto tako i za drugu jednakost;

(4) Naime, ako je $I^{ec} = I$, tada je $I = (I^e)^c$. S druge strane, ako je $I = J^c$, tada je $I^{ec} = J^{cec} = J^c = I$. Isto tako i za drugu jednakost.

Primedba. Ovde se radi o tzv. *Galoaovoj koneksiji*, koju je Galoa prvi otkrio u njegovoj teoriji rešivosti algebarskih jednačina. Ako su P i Q dva parcijalno uredjena skupa, Galoaova koneksija je par monotonih funkcija $f : P \to Q$ i $g : Q \to P$ takvih da je $gf(p) \leq p$ i $q \leq fg(q)$ za $\forall p \in P$ i $\forall q \in Q$. Tada je $f(p) \leq fgf(p) \leq f(p)$ odakle je $fgf = f$ i analogno $gfg = g$.

Primer. Proučimo ekstenziju i kontrakciju u sledeća dva primera proširenja glavnoidealskog prstena celih brojeva $\mathbb{Z}$.

(1) $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$. Kao što je rečeno, ovaj prsten je glavnoidealski. Ekstenzija ideala $I = (d) = d\mathbb{Z}$ je ideal $I^e = (d) = d\mathbb{Z}[i]$. Šta je kontrakcija ideala $J = (a+bi)$? Imamo $(a+bi)(m+ni) = (am-bn)+(an+bm)i \in \mathbb{Z} \Leftrightarrow an+bm = 0$ pa je $J^c = J \cap \mathbb{Z} = \{am - bn \in \mathbb{Z} \,|\, an + bm = 0\} = \left\{\frac{(a^2+b^2)m}{a} \,|\, m \in \mathbb{Z}\right\} \cap \mathbb{Z}$. Ako je $d = M(a, b)$ najveći zajednički delilac, $a = da_1$, $b = db_1$, tada treba da bude $\frac{d(a_1^2+b_1^2)m}{a_1} \in \mathbb{Z}$. Pri tome su a_1 i $a_1^2 + b_1^2$ uzajamno prosti. Neka je $p = M(d, a_1)$ najveći zajednički delilac, $d = pd_1$, $a_1 = pq$. Tada mora q deliti m tj. $m = qm_1$ te je $J^c = (d_1 (a_1^2 + b_1^2))$ Na primer, $(6 + 4i)^c = (26)$, $(4 + 6i)^c = (13)$. U ovom slučaju $I^{ec} = I$, $\mathcal{C} \rightleftarrows \mathcal{E} = \{(d) \,|\, d \in \mathbb{Z}\}$ i svaki ideal u $\mathbb{Z}$ je kontrahovan, a nije svaki ideal u $\mathbb{Z}[i]$ ekstendovan. Razni ideali u $\mathbb{Z}[i]$ mogu imati istu kontrakciju u $\mathbb{Z}$. Pri ovom proširenju broj ideala se povećao.

(2) $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Ovo je polje, pa su njegovi jedini ideali (0) i (1). Jasno da je $(0)^c = (0)$ i $(1)^c = (1)$, a da je $(d)^e = (1)$ ako je $d \neq 0$ i $(0)^e = (0)$. U ovom slučaju $J^{ce} = J$, $\mathcal{C} \rightleftarrows \mathcal{E} = \{(0), (1)\}$ i svaki ideal u $\mathbb{Q}$ je ekstendovan, a nije svaki ideal u $\mathbb{Z}$ kontrahovan. Razni ideali u $\mathbb{Z}$ mogu imati istu ekstenziju u

$\mathbb{Q}$. Pri ovom proširenju broj ideala se smanjio.

Prsten A je *lokalan* ako ima tačno jedan maksimalni ideal $\mathfrak{M}$. Tada je količnicki prsten $k = A/\mathfrak{M}$ polje, tzv. *polje ostataka* prstena A. Prsten je *polulokalan* ako ima samo konačno mnogo maksimalnih ideala.