Ekvivalenčne relacije in kvocientne množice

Ekvivalenčne relacije

> **Definicija:** Relacija $R \subseteq A \times A$ je **ekvivalenčna relacija**, če je refleksivna, tranzitivna in simetrična. Kadar velja $x \, R \, y$, pravimo, da sta x in y **ekvivalentna** (glede na R).

Opomba: Kdor reče "ekvivalentna relacija", je noob. Kdor reče, da sta "x in y ekvivalenčna", je rookie.

Ekvivalenčne relacije se običajno označuje s simboli, ki so podobni znaku za enakost: $\equiv$, $\sim$, $\simeq$, $\cong$.

Primeri:

1. Relacija "vzporednost" med premicami v ravnini.
2. Relacija "skladnost" med trikotniki v ravnini.
3. Relacija "podobnost" med trikotniki v ravnini.
4. Relacija "isti ostanek pri deljenju s 7" na množici $\mathbb{N}$.
5. Prazna relacija $\emptyset \subseteq A \times A$ je ekvivalenčna le v primeru, da je $A = \emptyset$.
6. Polna relacija $A \times A$ je ekvivalenčna.
7. Diagonala (oz. enakost) je ekvivalenčna relacija.

Ekvivalenčna relacija porojena s preslikavo

Posebej pomemben je primer ekvivalenčne relacije **porojene (ali inducirane) s preslikavo**: naj bo $f : A \to B$ preslikava in definirajmo relacijo $\sim_f \subseteq A \times A$ s predpisom

$$x \sim_f y \Leftrightarrow f(x) = f(y)$$

Tedaj je $\sim_f$ ekvivalenčna relacija:

- refleksivnost: $x \sim_f x$ velja, ker velja $f(x) = f(x)$,
- tranzitivnost: če je $x \sim_f y$ in $y \sim_f z$, potem je $f(x) = f(y)$ in $f(y) = f(z)$, torej $f(x) = f(z)$ in $x \sim_f z$,
- simetričnost: če je $x \sim_f y$, potem je $f(x) = f(y)$, torej $f(y) = f(x)$ in $y \sim_f x$.

Ali je vsaka ekvivalenčna relacija porojena z neko preslikavo?

Primer: premici sta vzporedni natanko tedaj, ko imata enaka smerna vektorja. Če je torej P množica vseh premic, R^2 množica vektorjev v ravnini, in $s : P \to R^2$ preslikava, ki premici P priredi njen enotski smerni vektor, ki leži v zgornji polravnini ali na pozitivnem delu osi x, tedaj velja

$$p \parallel q \Leftrightarrow s(p) = s(q)$$

Torej je vzporednost porojena s preslikavo s.

Ekvivalenčni razredi in kvocientne množice

Definicija: Naj bo $E \subseteq A \times A$ ekvivalenčna relacija. **Ekvivalenčni razred** elementa $x \in A$ je množica $[x]_A := \{ y \in A \mid x \, E \, y \}$. Z besedami: ekvivalenčni razred x je množica vseh elementov, ki so mu ekvivalentni.

Opomba: Kdor reče "ekvivalentni razred", je newbie.

Definicija: Naj bo $E \subseteq A \times A$ ekvivalenčna relacija. **Kvocientna množica** ali **kvocient** A/E je množica vseh ekvivalenčnih razredov:

$$A/E := \{ \xi \subseteq P(A) \mid \exists x \in A . \xi = [x]\_A \}.$$

Z izpeljanimi množicami lahko to zapišemo bolj razumljivo:

$$A/E = \{ [x]\_E \mid x \in A \}.$$

Kanonična kvocientna preslikava $q\_E : A \to A/E$ je preslikava, ki vsakemu elementu priredi njegov ekvivalenčni razred: $q\_E(x) := [x]\_A$.

Kvocientni množici včasih pravimo tudi *faktorska množica*.

Izrek: Vsaka ekvivalenčna relacija je porojena z neko preslikavo.

Dokaz. Naj bo E ekvivalenčna relacija na A. Najprej ugotovimo naslednje: za vse $x, y \in A$ velja

$$x E y \Leftrightarrow [x]\_E = [y]\_E$$

Dokaz $\Rightarrow$: če je $x E y$ potem je $[x]\_E \subseteq [y]\_E$, ker iz $z E x$ in $x E y$ sledi $z E y$. Podobno dokažemo $[y]\_E \subseteq [x]\_E$.

Dokaz $\Leftarrow$: če je $[x]\_E = [y]\_E$ potem je $y \in [y]\_E = [x]\_E$, torej po definiciji $[x]\_E$ dobimo $x E y$.

Sedaj izrek sledi zlahka: $q\_E(x) = q\_E(y) \Leftrightarrow [x]\_E = [y]\_E \Leftrightarrow x E y$ □

Razdelitev množice

Definicija: Razdelitev ali **particija** množice A je množica nepraznih, paroma disjunktnih množic, ki tvorijo pokritje A (kar pomeni, da je A enaka njihovi uniji). Se pravi, to je množica $S \subseteq P(A)$, za katero velja:

1. Elementi razdelitve so neprazni: $\forall B \in S . B \neq \emptyset$
2. Vsaka dva elementa razdelitve sta bodisi enaka bodisi disjunktna: $\forall B, C \in S . B = C \lor B \cap C = \emptyset$
3. Elementi razdelitve tvorijo pokritje A: $A = \cup S$.

Primer:

- Navpične premice tvorijo razdelitev ravnine.
- Množici sodih in lihih števil tvorita razdelitev naravnih števil.
- Množica $\{\{1,2\}, \{3,5\}, \{4,6,7\}\}$ tvori razdelitev $\{1,2,3,4,5,6,7\}$.
- Množica $\{\{1,2,3,4,5,6,7\}\}$ tvori razdelitev $\{1,2,3,4,5,6,7\}$.

Izrek: Naj bo $E \subseteq A \times A$ ekvivalenčna relacija. Njeni ekvivalenčni razredi tvorijo razdelitev množice A.

Dokaz.

1. Naj bo $\xi \in P(A)$ ekvivalenčni razred za E. Tedaj obstaja $x \in A$, da je $\xi = [x]\_A$, torej je $x \in \xi$ in zato $\xi \neq \emptyset$.

2. Naj bosta $\zeta, \xi \in P(A)$. Dokazali bomo $\zeta \cap \xi \neq \emptyset \Rightarrow \zeta = \xi$. Če je $x \in \zeta \cap \xi$, potem velja $\zeta \subseteq \xi$ ker: naj bo $y \in \zeta$, tedaj je $y E x$ in ker je $x \in \xi$ velja $y \in \xi$. Simetrično dokažemo `$\xi \subseteq \zeta$.

3. Očitno je unija vseh ekvivalenčnih razredov podmnožica A, saj je vsak ekvivalenčni razred

podmnožica A. Zagotovo pa je vsak $x \in A$ v kakem ekvivalenčnem razredu, namreč $x \in [x]_A$. □

Torej vsaka ekvivalenčna relacija na A določa razdelitev množice A, namreč na ekvivalenčne razrede. Velja pa tudi obrat: vsaka razdelitev $S \subseteq P(A)$ določa ekvivalenčno relacijo na A, namreč $\simeq_S$ definiran s predpisom

$$x \simeq_S y \Leftrightarrow \exists\, B \in S\,.\, x \in B \land y \in B$$

Z besedami: x in y sta ekvivalentna, kadar sta v istem elementu razdelitve. Prazvzaprav smo ugotovili, da imamo izomorfizem množic:

$$\{ E \subseteq A \times A \mid E \text{ je ekvivalenčna relacija} \} \cong \{ S \subseteq P(A) \mid S \text{ je razdelitev } A \}$$

V eno smer izomorfizem ekvivalenčni relaciji E priredi njeno razdelitev, v drugo pa razdelitvi priredimo ekvivalenčno relacijo, kakor smo to opisali zgoraj. (Premislite, da sta ti preslikavi inverza.)

Prerezi kvocientne preslikave in aksiom izbire

Ekvivalenčni razred je natanko določen že z enim od svojih elementov, zato pogosto želimo namesto ekvivalenčnih razredov navesti le njihove predstavnike.

Definicija: Naj bo E ekvivalenčna relacija na A. Množico $C \subseteq A$, ki vsak ekvivalenčni razred relacije E seka natanko enkrat, imenujemo **izbor predstavnikov (ekvivalenčnih razredov) za relacijo E**.

Izbor predstavnikov $C \subseteq A$ za E določa preslikavo $c : A/E \to A$, ki priredi ekvivalenčnemu razredu ξ tisti $x \in \xi$, ki je element C:

$$c : A/E \to A$$
$$c : \xi \mapsto (\iota\, x \in \xi\,.\, x \in C)$$

Preslikava $c : A/E \to A$ je *prerez* kvocientne preslikave $q_E : A \to A/E$.

Trditev: Če je $s : A/E \to A$ prerez kvocientne preslikave $q_E : A \to A/E$, potem je njegova slika $s_*(A/E) = \{ c(\xi) \mid \xi \in A/E \}$ izbor predstavnikov za E.

Dokaz: Vaja. □

Ker izbor predstavnikov in prerez kvocientne preslikave določata drug drugega, včasih tudi prerez imenujemo “izbor predstavnikov”.

Primer: Definirajmo ~ na množici celih števil Z s predpisom

$$a \sim b \Leftrightarrow 7 \mid a - b$$

Torej sta števili a in b ekvivalentni, če dasta enak ostanek pri deljenju s 7, na primer $13 \sim 20$ in $\neg (13 \sim 15)$.

Ekvivalenčni razred števila a dobimo tako, da a prištejemo vse večkratnike števila 7:

$$[a]_\sim = \{ a + 7 \cdot k \mid k \in \mathbb{Z} \}$$

Na primer,

$$\begin{aligned} [13]_\sim &= \{ 7 \cdot k + 13 \mid k \in \mathbb{Z} \} \\ &= \{ \ldots, -22, -15, -8, -1, 6, 13, 20, 27, 34, 41, \ldots \} \end{aligned}$$

Koliko pa je ekvivalenčnih razredov? Toliko, kot je ostankov pri deljenju s 7, torej 7. Izbor predstavnikov za ~ je torej množica $\{0, 1, 2, 3, 4, 5, 6\}$, saj je vsako celo število ekvivalentno natanko enemu od teh števil mo modulu 7.

Ni pa to edini izbor! Tudi $\{0, 1, 2, 3, 4, 5, 6, 13\}$ je izbor, prav tako pa $\{-7, -6, -5, -4, -3, -2, -1\}$.

(Konec primera.)

Ali ima vsaka ekvivalenčna relacija izbor predstavnikov? Da to vprašanje ni tako enostavno, kot se zdi na prvi pogled, doma premislite o nalslednji nalogi.

Naloga: Na množici realnih števil $\mathbb{R}$ definiramo relacijo E s predpisom

$$x \mathrel{E} y \iff x - y \in \mathbb{Q}$$

Se pravi, da sta števili ekvivalentni, če je njuna razlika racionalno število. Podajte kak izbor predstavnikov za E.

Izrek: Naslednje izjave so ekvivalentne:

1. Vsaka surjektivna preslikava ima desni inverz (prerez).
2. Vsaka ekvivalenčna relacija ima izbor predstavnikov.
3. Vsaka družina nepraznih množic ima funkcijo izbire.
4. Produkt družine nepraznih množic je neprazen.

Dokaz.

$(1 \Rightarrow 2)$: Naj bo $E \subseteq A \times A$ ekvivalenčna relacija na A. Tedaj je $q\_E : A \to A/E$ surjektivna, zato ima po predpostavki (1) prerez, ki določa izbor predstavnikov.

$(2 \Rightarrow 3)$: Naj bo $A : I \to \mathsf{Set}$ družina nepraznih množic. Naj bo ~ ekvivalenčna relacija na koproduktu $K := \coprod\_\{i \in I\}\ A\_i$, porojena s prvo projekcijo $pr_1 : S \to I$, t.j.,

$$in_i(x) \sim in_j(y) \iff i = j$$

Po predpostavki (2) obstaja izbor predstavnikov za ~, se pravi taka množica $C \subseteq K$, da za vsak $u \in K$ obstaja natanko en $v \in C$, da je $pr_1(u) = pr_1(v)$. Definirajmo $f : I \to \bigcup A$ s predpisom

$$f(i) := \text{tisti } x \in A\_i, \text{ za katerega je } in_i(x) \in C$$

Očitno je f funkcija izbire za družino A, če je le dobro definirana:

- f je enolična, saj iz $in_i(x) \in C$ in $in_i(y) \in C$ sledi $in_i(x) = in_j(y)$.
- f je celovita: ker je A_i neprazna, obstaja $z \in A\_i$, torej obstaja $v \in C$, da je $i = pr_1(in_i(z)) = pr_1(v)$, in je potemtakem $pr_2(v) \in A\_i$ element, za katerega velja $in_i(pr_2(v)) \in C$.

$(3 \Rightarrow 4)$: Elementi produkta so funkcije izbire, zato je produkt res neprazen, če obstaja kaka funkcija izbire.

$(4 \Rightarrow 1)$: Naj bo $f : X \to Y$ surjektivna. Definirajmo družino $A : Y \to \mathsf{Set}$ s predpisom $A\_y = f\text{^*}(\{y\})$. Ker je f surjektivna, je A družina nepraznih množic. Po predpostavki (4) je produkt te družine neprazen, torej vsebuje neko funkcijo izbire $c : Y \to \bigcup A\_y$, se pravi, da je $f(c(y)) = y$ za vsak $y \in Y$. Opazimo še, da je $\bigcup A = Y$, torej je c prerez f. □

Izbor prestavnikov je torej ekvivalenten še nekaterim drugim trditvam. Pa te veljajo? Za to potrebujemo aksiom.

Aksiom izbire: Vsaka družina nepraznih množic ima funkcijo izbire.

Se pravi, če je $A : I \to \mathrm{Set}$ taka družina množica, da za vsak $i \in I$ velja $A_i \neq \emptyset$, tedaj obstaja $f : I \to \bigcup A$, za katerega je $f(i) \in A_i$ za vse $i \in I$.

O aksiomu izbire bomo še govorili.

Univerzalna lastnost kvocientne množice

Naj bo E ekvivalenčna relacija na A in B množica. Pogosto želimo definirati preslikavo

$$f : A/E \to B$$

s pomočjo preslikave $A \to B$. Kdaj lahko to naredimo?

Izrek: Naj bo E ekvivalenčna relacija na A in $g : A \to B$ preslikava, ki je *skladna* z E, kar pomeni da g slika ekvivalentne elemente v enake, se pravi $\forall x, y \in A .\ x\ E\ y \Rightarrow g(x) = g(y)$. Tedaj obstaja natanko ena preslikava $f : A/E \to B$, da je $f([x]_E) = g(x)$ za vse $x \in A$, ali drugače povedano, $f \circ q_E = g$.

Dokaz.

Dokažimo najprej, da imamo največ eno tako preslikavo. Denimo da za $f_1 : A/E \to B$ in $f_2 : A/E \to B$ velja $f_1 \circ q_E = f_2 \circ q_E$. Ker je q_E surjektivna, je epi in jo smemo krajšati na desni, od koder res sledi $f_1 = f_2$.

Sedaj dokažimo, da f obstaja. V ta namen naj bo $\varphi \subseteq A/E \times B$ relacija

$$\varphi(\xi, y) \Leftrightarrow \exists x \in A .\ x \in \xi \land g(x) = y$$

Trdimo, da je φ funkcijska relacija:

- enoličnost: če je $\varphi(\xi, y_1)$ in $\varphi(\xi, y_2)$, potem obstajata $x_1, x_2 \in \xi$, da je $g(x_1) = y_1$ in $g(x_2) = y_2$. Ker pa velja $x_1\ E\ x_2$ in je g skladna z E, sledi $y_1 = g(x1) = g(x_2) = y_2$.

- celovitost: naj bo $\xi \in A/E$. Tedaj obstaja $x \in \xi$. Očitno velja $g(\xi, g(x))$.

Naj bo $f : A/E \to B$ preslikava, ki je določena s funkcijsko relacijo φ. Za $x \in A$ velja $\varphi([x]_E, f([x]_E))$, od tod pa iz definicije φ sledi tudi $g(x) = f([x]_E)$. □

Kanonična razčlenitev preslikave

Naj bo $f : A \to B$ preslikava. Naj bo $\sim_f$ ekvivalenčna relacija na A, ki jo porodi f, in $q_f : A \to A/E$ kanonična kvocientna preslikava (morali bi jo pisati $q_{\sim_f}$, kar je nečitljivo). Naj bo $i : f_*(A) \to B$ kanonična inkluzija slike f v kodomeno. Preslikava $f : A \to f_*(A)$ je skladna s $\sim_f$, zato obstaja (natanko ena) preslikava $b_f : A/f \to f_*(A)$, da velja $b_f([x]_\sim) = f(x)$. Trdimo:

1. $f = i_f \circ b_f \circ q_f$
2. q_f je surjektivna, b_f je bijektivna in i_f je injektivna.

Računajmo: $f(x) = b_f([x]_\sim) = i_f(b_f([x]_\sim)) = i_f(b_f(q_f(x)))$, za vse $x \in A$, od koder sledi prva trditev.

Vemo že, da je kanonična kvocientna preslikava surjektivna in kanonična inkluzija injektivna. Ostane nam še bijektivnost preslikave b_f:

- b_f je injektivna: naj bosta $\xi, \zeta \in A/(\sim\_f)$ in denimo, da velja $b\_f(\xi) = b\_f(\zeta)$. Obstajata $x, y \in A$, da je $\xi = [x]\_\sim$ in $\zeta = [y]\_\sim$. Velja

  $$f(x) = i\_f(b\_f(q\_f(x))) = i\_f(b\_f(\xi)) = i\_f(b\_f(\zeta)) = i\_f(b\_f(q\_f(y))) = f(y)$$

  torej je $x \sim\_f y$ in zato $\xi = [x]\_\sim = [y]\_\sim = \zeta$.

- b_f je surjektivna: naj bo $u \in f\_*(A)$. Tedaj obstaja $x \in A$, da je $u = f(x)$. Vzemimo $\xi = [x]\_E$ in preverimo: $b\_f(\xi) = b\_f([x]\_\sim) = f(x) = u$. □