Jaká je logická výstavba matematiky?

5. Logická dedukce

In: Miroslav Katětov (author): Jaká je logická výstavba matematiky?. (Czech). Praha: Jednota československých mathematiků a fysiků, 1946. pp. 45–59.

Persistent URL: http://dml.cz/dmlcz/403137

Nyní přistoupíme k otázkám, týkajícím se celkové stavby důkazů. Není ovšem možné probrat všechny druhy důkazů a všechny obraty, které se v nich mohou vyskytovat. Uvedeme však některé základní typy důkazů, které jsou důležité pro matematiku.

Důkazy se liší především podle druhu dokazovaného výroku, totiž podle toho, jde-li o výrok individuální, na příklad „$[\frac{1}{2}(-1+i\sqrt{3})]^3 = 1$", obecný, na příklad „libovolný trojúhelník má součet úhlů 180°", nebo existenční, na příklad „existuje funkce, která je všude spojitá, ale nemá nikde derivaci". Matematické věty mají zpravidla povahu obecných nebo existenčních výroků. Individuální věty vystupují v matematice většinou buď jako speciální případ obecné věty nebo jako jakási zkratka za obecný nebo existenční výrok. Tak výrok „číslo π je algebraické" je ekvivalentní s existenčním výrokem „existuje polynom, který má racionální koeficienty a jehož kořenem je číslo π".*) Při důkaze takové individuální věty jde pak vlastně o důkaz ekvivalentní obecné nebo existenční věty.

5·1. Individuální věty. Pokud jde o vlastní individuální věty, patří jejich důkazy mezi logicky nejjednodušší. Většinou spočívá celý důkaz v substitučním úsudku, jímž odvodíme individuální větu z věty obecné — tak na příklad větu „$3^2 - 1 = (3+1)(3-1)$" z věty „pro libovolné x je $x^2 - 1 = (x+1)(x-1)$". Speciálním případem individuálních vět jsou i n d i v i d u á l n í i d e n t i t y (slovem identita míníme zde výrok tvaru „... je totožné s ..."), t. j. identity, které

*) Lze dokázat, že tento výrok je nesprávný. Číslo π algebraické n e n í.

neobsahují neurčité, na příklad $[\frac{1}{2}(-1+i\sqrt{3})]^3 = 1$. Důkazy takových identit se zpravidla skládají z identifikačních úsudků podle schematu „$A = B$, $B = C$; tedy $A = C$" a úsudků substitučních, t. j. dosazování do obecných identit. Jako příklad si může čtenář sám provést a rozebrat důkaz zmíněné identity. — Zcela obdobné jsou ostatně důkazy o b e c n ý c h i d e n t i t, na příklad „$\cos 2x = \cos^2 x - \sin^2 x$". Rozdíl je pouze v tom, že místo individuálních máme obecné výroky, takže identifikační úsudky mají zde tvar „pro každé x je $A(x) = B(x)$ a $B(x) = C(x)$; tedy pro každé x je $A(x) = C(x)$".

Obecný výrok lze dokazovat buď přímo nebo nepřímo; zvláštním typem přímého obecného důkazu je důkaz úplnou indukcí. Probereme tedy tři typy obecného důkazu: 1. přímý obecný důkaz, 2. obecný důkaz úplnou indukcí, 3. nepřímý obecný důkaz.

5·2. Přímý obecný důkaz. Začneme jednoduchým příkladem prvního typu důkazu. Dokazujeme větu „když (celé) číslo x není dělitelné 3, pak $x^2 - 1$ je dělitelné 3". Důkaz probíhá takto: „Nechť x není dělitelné 3; potom buď $x - 1$ nebo $x + 1$ je dělitelné 3; tedy $x^2 - 1$ je dělitelné 3". Jiným příkladem může být zmíněný důkaz identity $\cos 2x = \cos^2 x - \sin^2 x$ nebo většina důkazů elementární geometrie.

Charakteristické pro tento typ obecného důkazu je to, že provádíme důkaz tak, jako by šlo o příklad důkazu individuálního výroku. Zvlášť zřetelné je to u důkazů z elementární geometrie. Tam vedeme zpravidla důkaz následujícím způsobem: Představujeme si zcela určitý individuální případ, znázorněný výkresem (tak při důkazu nějaké obecné věty o trojúhelníku si představujeme trojúhelník s určitými vlastnostmi, na příklad ostroúhlý) a provádíme důkaz pro tento případ, avšak tak, aby měl obecnou platnost. Takovému po-

stupu se někdy říká **paradigmatický.** Po formální logické stránce je tento typ důkazu charakterisován tím, že generální důkaz je vlastně s c h e m a t e m; vhodným dosazením lze z něho dostat důkaz každého individuálního výroku, který je obsažen v dokazované obecné větě.

Tento typ důkazu, totiž **paradigmatický obecný důkaz,** lze považovat za základní druh obecného důkazu. Pro matematiku má však snad ještě větší význam obecný důkaz úplnou indukcí. Budeme se jím zabývat podrobněji.

5·3. Důkaz úplnou indukcí. Začneme jednoduchým příkladem. Dokazujeme větu: pro každé celé kladné n je číslo $n^5 - n$ dělitelné 5. Dokážeme nejdříve toto: když $m^5 - m$ je dělitelné 5, pak též $(m+1)^5 - (m+1)$ je dělitelné 5. Skutečně, číslo $(m+1)^5 - (m+1) = (m^5 + 5m^4 + 10m^3 + 10m^2 + 5m + 1) - (m+1) = 5m^4 + 10m^3 + 10m^2 + 5m + m^5 - m$ je dělitelné 5, kdykoli číslo $m^5 - m$ je dělitelné 5. Protože číslo $1^5 - 1 = 0$ je dělitelné 5, plyne z toho již naše věta.

Rozebereme nyní a schematisujeme tento důkaz. Za výrokový vzorec „$n^5 - n$ je dělitelné 5" zavedeme pro stručnost zkratku „n je P" a smluvíme se, že písmeno n bude v tomto odstavci nadále označovat p o u z e p ř i r o z e n á, t. j. c e l á k l a d n á č í s l a (řečeno logicky korektně: za neurčitou n smíme dosazovat pouze přirozená čísla). — Důkaz, který jsme uvedli, spočívá zřejmě v tom, že dokážeme výroky „pro každé n platí: když n je P, pak také $n+1$ je P" a „1 je P" a z nich pak ihned odvodíme — a v tomto úsudku právě spočívá jádro důkazu — výrok „každé n je P". Takový důkaz nazýváme právě d ů k a z e m ú p l n o u i n d u k c í. Jeho jádro — ú s u d e k p o d l e p r i n c i p u ú p l n é i n d u k c e má toto schema:

pro každé n platí: když n je P, pak $n+1$ je P } premisy
1 je P . . . . . }
tedy každé n je P . . . . . závěr

Zopakujeme si teď ještě jednou, v čem spočívá důkaz úplnou indukcí. Máme dokázat výrok „pro každé (přirozené) n platí $P(n)$" (zde je „$P(n)$" zkratka za jakýsi určitý výrokový vzorec). Neprovedeme to však bezprostředně, nýbrž dokážeme nejdříve výroky (**A**) „$P(1)$" a (**B**) „když $P(n)$, pak $P(n+1)$". Můžeme nyní odvodit z **A** a **B** řetězem implikačních a substitučních úsudků libovolný jednotlivý výrok $P(a)$ (s určitým celým kladným a), a sice takto:

$P(1)$
když $P(1)$, pak $P(2)$ substitučním úsudkem z **B**
tedy $P(2)$ . . . . . implikačním úsudkem
když $P(2)$, pak $P(3)$ substitučním úsudkem z **B**
tedy $P(3)$ . . . . . implikační úsudek
atd.

Můžeme jíti takto libovolně daleko, nedospějeme však tímto způsobem nikdy k obecné větě „pro každé n platí $P(n)$". To znamená, že princip úplné indukce se nedá redukovat na jiné obvyklé druhy úsudků, nýbrž v jistém smyslu shrnuje neomezený řetěz implikačních a substitučních úsudků.

Zde musíme vsunout jednu spíše terminologickou poznámku. Úplná indukce, o níž nyní mluvíme, nemá kromě názvu nic společného s indukcí, s níž se setkáváme v přírodních vědách.*) Abychom ukázali jejich rozdíl, stačí říci, že při „přírodovědecké" indukci vycházíme z řady jednotlivých individuálních výroků

*) To se zdá samozřejmé, avšak bohužel také některé učebnice logiky zaměňují tyto dva naprosto rozdílné pojmy.

(z jednotlivých pozorování) a dospíváme k obecné větě (hypothese), která však nemá povahu logického důsledku těchto výroků. Při matematické úplné indukci naproti tomu vycházíme ze dvou výroků: jednoho individuálního a jednoho obecného („když n je P, pak také $n+1$ je P) a docházíme k obecné větě, která je l o g i c k ý m d ů s l e d k e m daných dvou výroků.

Vraťme se k našemu thematu. Proč jsme neuvedli úsudek podle principu úplné indukce současně se základními úsudky — implikačním, substitučním atd.? Proto, že zmíněné základní úsudky mají zcela obecný ráz a vyskytují se v jakémkoli oboru úvah. Naproti tomu úplná indukce je specifická pro matematiku — přesněji řečeno, pro přirozená čísla, která jsou základem matematiky.

Další otázka je tato: Lze princip úplné indukce dokázati, t. j. lze úsudek podle tohoto principu nahradit řetězem jiných úsudků? Jak jsme již řekli, nikoli, — pokud ovšem nezavedeme nějaký axiom rovnocenný s tímto principem. Princip úplné indukce vyjadřuje totiž určitou základní specifickou vlastnost přirozených čísel, takže se nedá rozložit v řetěz úsudků obecné povahy. Zavedeme-li však vhodný axiom, rovnocenný s tímto principem, na příklad „když (1) 1 má vlastnost P, (2) má-li n vlastnost P, pak ji má též $n+1$, potom každé n má vlastnost P", pak ovšem vystačíme za použití tohoto axiomu s implikačním a substitučním úsudkem. Je však jasné, že zde jde jen o ryze formální a v podstatě bezvýznamný rozdíl mezi zavedením nového axiomu a nového úsudkového schematu.

Princip úplné indukce můžeme také obejít a nahradit nepřímým důkazem. Ukáže se ovšem, že při tom zase používáme jisté zásady (axiomu), která je rovnocenná s principem úplné indukce.

Máme z výroků (**A**) „1 je P", (**B**) „když n je P, pak též $n+1$ je P" odvodit výrok (**C**) „každé n je P" (n je

při tom ovšem podle naší úmluvy přirozené číslo). Provedeme to, jak jsme řekli, nepřímým způsobem: z **A**, **B** a negace **C** odvodíme spor. Negaci **C** můžeme nahradit ekvivalentním výrokem „některé n není P". Z toho pak plyne: existuje n e j m e n š í n, které není P. Potom však buď toto nejmenší n se rovná 1, nebo číslo $n-1$ má vlastnost P. První možnost je však ve sporu s výrokem **A**, a druhá zase vede ke sporu s výrokem **B**. Tím je podle zásady nepřímého důkazu dokázán výrok **C**. Rozebereme-li tuto úvahu podrobně, pak vidíme, že spočívá na dvou principech (axiomech), které jsou oba dohromady rovnocenné s principem úplné indukce. Jsou to tyto axiomy: 1. Když některé přirozené číslo n má vlastnost P, pak existuje n e j m e n š í přirozené číslo, které má tuto vlastnost. 2. Když není $n = 1$, pak existuje m tak, že $n = m+1$ (t. j. že n bezprostředně následuje po m). Axiomatickou výstavbu theorie přirozených čísel můžeme založit také na těchto axiomech, které rovněž úplně charakterisují způsob, jakým jsou uspořádána přirozená čísla.

5·4. Nepřímý obecný důkaz. Při nepřímém důkazu obecné věty vycházíme z její negace, odvodíme z ní spor a na základě toho pak usoudíme, že věta je správná. Uveďme p ř í k l a d. Máme dokázat, že číslo $\sqrt{2}$ není racionální. Tento individuální výrok je podle definice racionálního čísla ekvivalentní s výrokem „neexistují celá čísla m, n taková, aby $\frac{m}{n} = \sqrt{2}$", jenž je zase ekvivalentní s obecným výrokem „pro žádná celá čísla m a n neplatí $m^2 = 2n^2$ a současně $n \neq 0$". Chceme nyní dokázat tento výrok. Nepřímý důkaz provádíme takto: Předpokládáme naopak, že existují celá čísla m a n taková, že $n \neq 0$ a $m^2 = 2n^2$. Z toho se ihned odvodí, že existují celá čísla m, n taková, že $n \neq 0$, $m^2 = 2n^2$ a čísla m a n jsou navzájem nesou-

dělná. Avšak pro libovolná celá m, n platí: když $m^2 = 2n^2$, pak číslo m i číslo n je dělitelné 2, tedy čísla m a n nejsou nesoudělná (to je zřejmé, neboť m^2 a tedy též m je sudé, takže m^2 je dělitelné 4, tedy n^2 je sudé atd.). Tím jsme skutečně dospěli ke sporu, tedy podle zásady nepřímého důkazu je naše věta dokázána.

Schematisujeme nyní tento příklad. Jde v podstatě o důkaz výroku tvaru „žádné x nemá vlastnost V", kde x značí dvojice celých čísel m, n a V značí jejich vlastnost „n je různé od nuly a $m^2 = 2n^2$". Z negace tohoto výroku vyplývá tautologickou úpravou výrok „existuje x, které má vlastnost V". Z něho odvodíme výrok „existuje x, které má vlastnosti V a V_1" (kde V_1 značí vlastnost dvojice m, n: „m a n jsou nesoudělná čísla"). Tento výrok je však ve sporu s větou „žádné x, které má vlastnost V, nemá vlastnost V_1".

Nebudeme nyní rozebírat tento důkaz krok za krokem, nýbrž pouze vytkneme některé okolnosti, typické pro celkovou stavbu podobných důkazů. Abychom provedli nepřímý důkaz, t. j. vyvrátili výrok „některé x má vlastnost V", musíme zpravidla vyhledat nějakou vlastnost W, kterou má každé x a která je v rozporu s vlastností V. Někdy však musíme (jako v našem příkladě) postupovat jinak, totiž nejprve odvodit z výroku „některé x má vlastnost V" důsledek tvaru „některé x má vlastnosti V a V_1" (jde pak vlastně o existenční důkaz, který vystupuje jako část nepřímého obecného důkazu) a pak ukázat, že vlastnosti V a V_1 jsou neslučitelné. — Zde vidíme, jak jsou navzájem spojeny různé typy důkazů a jak složité jsou s logického hlediska matematické důkazy, i když se zdají velmi jednoduché.

5·5. Existenční důkazy. Rozeznáváme tři druhy existenčních důkazů: konstruktivní důkaz, vlastní existenční důkaz a nepřímý existenční důkaz. Kromě toho

zaujímá zvláštní postavení tak zvaný existenční důkaz úplnou indukcí, který je sice názorně dosti jednoduchý, ale po logické stránce značně komplikovaný.

Konstruktivní existenční důkaz spočívá v tom, že přímo **udáme** (sestrojíme) prvek, který má vlastnost, o níž nám jde. Tak na příklad provedeme důkaz věty „existuje číslo, které není racionální" tak, že dokážeme „číslo $\sqrt{2}$ není racionální".*) Obecně dokážeme větu „některé x je P" tak, že udáme (sestrojíme, konstruujeme) prvek a takový, že výrok „a je P" je pravdivý. Tento druh existenčního důkazu je považován za nejdokonalejší, a to jednak proto, že zřejmě dává více, než pouhý důkaz existence, jednak proto, že je současně důkazem existence v užším smyslu, totiž existence ve smyslu sestrojitelnosti (viz str. 26).

Dalším druhem existenčního důkazu je existenční důkaz v užším slova smyslu; odvozujeme existenční výrok z jiných existenčních vět, aniž bychom skutečně udali prvek, který má žádanou vlastnost. Tak můžeme na příklad odvodit existenční větu z jiné obecnější existenční věty; triviální příklad: odvodíme větu „existuje číslo, které není racionální" z věty „existuje číslo, které není algebraické". Existenční věty, které jsou při takovém důkazu premisami, mohou mít různou povahu: mohou to být existenční věty, které byly dokázány dříve, mohou to být také základní věty — definice, tautologické věty, axiomy. Seznámíme se později s jednou takovou velmi obecnou základní existenční větou, která má zásadní důležitost pro vyšší partie matematiky, totiž s axiomem výběru.

Konečně lze vést existenční důkaz také nepřímo, totiž tak, že odvodíme nesprávný výrok z negace exi-

*) Tento důkaz jsme provedli jako příklad v předešlém odstavci. Důkaz individuální věty „číslo $\sqrt{2}$ není racionální" je ovšem sám v podstatě nepřímým obecným důkazem. Zde vidíme zase předivo různých typů důkazů.

stenčního výroku, který chceme dokázat. Tak na příklad můžeme dokazovat výrok „existuje číslo, které není algebraické" také tak, že odvodíme spor z jeho negace, tedy z výroku „každé číslo je algebraické".

5·6. **Existenční důkaz úplnou indukcí.** Nechť máme sestrojit posloupnost čísel $a_1, a_2, a_3, \ldots$ takovou, aby (1) $a_1 = 1$; (2) $a_{n+1} = a_1 + \ldots + a_n$ pro libovolné přirozené n. Můžeme ovšem v tomto případě takovou posloupnost ihned udat: je to posloupnost 1, 1, 2, 4, 8, ...; nás však zde zajímá s logického hlediska postup, při němž konstruujeme posloupnost člen po členu, neboť v složitějších případech můžeme použít pouze tohoto postupu.

Položíme $a_1 = 1$, dále položíme $a_2 = a_1 = 1$, $a_3 = a_1 + a_2 = 2$, atd. Když jsme již stanovili čísla $a_1, a_2, \ldots, a_n$, položíme podle podmínky (2) $a_{n+1} = a_1 + \ldots + a_n$. Když takto neomezeně pokračujeme dále, sestrojíme celou posloupnost. — Tak vyhlíží tento postup, když jej popíšeme „názorným" způsobem. Nyní jej musíme rozebrat a podepřít logicky korektním způsobem. Především je jasné, že jde v podstatě o d ů k a z e x i s t e n c e posloupnosti s určitou vlastností. Podstatná je dále okolnost, že jde vždy o vlastnost určitého k o n e č n é h o ú s e k u posloupnosti (v našem případě o splnění vztahu $a_{n+1} = a_1 + \ldots + a_n$, resp. $a_1 = 1$) a že k úseku $a_1, \ldots, a_n$, který má tuto vlastnost, můžeme vždy připojit takový prvek a_{n+1}, že také úsek $a_1, a_2, \ldots, a_{n+1}$ má požadovanou vlastnost. Jsou-li tyto podmínky splněny, můžeme vždy konstruovat posloupnost, jejíž každý úsek má požadovanou vlastnost. — To, co jsme teď řekli, vyslovíme precisní formou jako p r i n c i p e x i s t e n č n í h o d ů k a z u (konstrukce) ú p l n o u i n d u k c í.

Nechť (1) pro každé (celé kladné) n platí: má-li konečná posloupnost o n členech $a_1, \ldots, a_n$

vlastnost V, pak existuje p r á v ě j e d e n prvek a_{n+1} takový, že také konečná posloupnost o $n+1$ členech $a_1, \ldots, a_n, a_{n+1}$ má vlastnost V; (2) existuje právě jeden prvek a_1 takový, že jednočlenná posloupnost a_1 má vlastnost V.

Potom existuje právě jedna nekonečná posloupnost $a_1, a_2, a_3, \ldots$, taková, že každý její úsek $a_1, \ldots, a_n$ má vlastnost V.

Na tomto principu je založena t. zv. konstrukce posloupnosti úplnou indukcí, jejíž příklad jsme uvedli. Nejde při tom o nový princip, který by stál vedle principu úplné indukce, nýbrž o jeho d ů s l e d e k, tedy o v ě t u theorie přirozených čísel. K tomu se však ještě vrátíme.

Místo principu, který jsme právě uvedli, se někdy užívá velmi podobného, avšak ve skutečnosti značně širšího principu, který již n e n í d ů s l e d k e m p r i n c i p u ú p l n é i n d u k c e, nýbrž spočívá též na axiomu výběru (viz odst. 6·4). Tento rozšířený princip můžeme vyslovit takto:

Nechť (1) pro každé (celé kladné) n platí: má-li konečná posloupnost o n členech $a_1, \ldots, a_n$ vlastnost V, pak existuje prvek a_{n+1} takový, že také konečná posloupnost o $n+1$ členech $a_1, \ldots, a_{n+1}$ má vlastnost V; (2) existuje prvek a_1 takový, že jednočlenná posloupnost a_1 má vlastnost V.

Potom existuje nekonečná posloupnost $a_1, a_2, a_3, \ldots$, taková, že každý její úsek $a_1, \ldots, a_n$ má vlastnost V.

V tomto rozšířeném principu nepožadujeme již existenci právě jednoho prvku a_{n+1} k úseku $a_1, \ldots, a_n$ ani existenci právě jednoho prvku a_1, takže nedospíváme k jednoznačně určené posloupnosti $a_1, a_2, a_3, \ldots$

V matematice (hlavně ovšem ve vyšších partiích) se běžně používá obou těchto principů. O skutečnou t. zv. logickou konstrukci (viz odst. 5·8) jde ovšem pouze při použití vlastního (užšího) principu existenčního důkazu úplnou indukcí.

Abychom ho mohli použít, musíme ovšem udat zcela určitý předpis pro konstrukci u r č i t é posloupnosti s požadovanou vlastností V (což znamená, že musíme najít nějakou vlastnost W, z níž vyplývá vlastnost V a na níž lze použít zmíněného užšího principu).

Vrátíme se nyní k odvození principu konstrukce úplnou indukcí; omezíme se však na pouhou skizzu odvození a nebudeme dbát některých logických fines.

Buď $P(n)$ zkratka za výrokový vzorec „existuje právě jedna posloupnost o n členech, jejíž každý úsek má vlastnost V". Předpoklad (2) principu konstrukce úplnou indukcí znamená pak, že platí $P(1)$; z předpokladu (1) tohoto principu vyplývá: když platí $P(n)$, pak platí též $P(n+1)$. Z toho pak plyne podle principu úplné indukce, že $P(n)$ platí pro každé (rozumí se, celé kladné) n, t. j. že pro každé n existuje právě jedna posloupnost o n členech, jejíž každý úsek má vlastnost V. Nyní dokážeme toto: máme-li dvě takové posloupnosti, jednu o m, druhou o n členech, pak jedna z nich je úsekem druhé. To je názorně samozřejmé, neboť jedna vzniká z druhé připojením nových prvků, k logicky korektnímu důkazu potřebujeme však znovu princip úplné indukce. Víme teď, že na n-tém místě ve všech těchto posloupnostech (pokud ovšem mají aspoň n členů) stojí tentýž prvek. Můžeme tedy říci: tento prvek nechť stojí na n-tém místě v nekonečné posloupnosti, kterou máme konstruovat. Tím je tato posloupnost „konstruována" (t. j. je dokázáno, že existuje taková posloupnost a to jen jedna).

5·7. Jádro důkazu. Položme si nyní otázku, v čem spočívá „jádro" („vtip", „pointa") matematických dů-

kazů. Co tím míníme, je jasné; kdo studoval poněkud složitější matematické důkazy, ten ví, že v nich bývá jeden nebo několik obratů, na nichž spočívá celý důkaz, jež jsou k němu „klíčem"; jakmile je známe, máme již celý důkaz v rukou.

Všimněme si nyní jako příkladu důkazu věty „počet prvočísel je nekonečný", s nímž jsme se již setkali. Důkaz probíhá takto: „Předpokládejme naopak, že počet prvočísel je konečný. Budiž pak P součin všech prvočísel. Potom číslo $P + 1$ není dělitelné žádným prvočíslem. To však je spor." Zde jsou podstatné tyto body: důkaz se provádí nepřímo; sestrojujeme číslo, které — za učiněných předpokladů — není dělitelné žádným prvočíslem. Při sestrojení takového čísla jde, jak vidíme při hlubším logickém rozboru, jednak o udání vlastnosti, kterou má mít sestrojované číslo, jednak o vlastní logickou konstrukci, t. j. určení (udání) — v obecném případě pak důkaz existence — čísla s touto vlastností. Když známe tyto tři body: důkaz se provádí nepřímo; má se sestrojit číslo, které není dělitelné žádným prvočíslem; takové číslo se sestrojí tak a tak, — pak známe již celý důkaz.

Připomeňme si dále důkazy z planimetrie. V těchto důkazech stačí zpravidla vědět, jaké pomocné prvky — body, přímky atd. máme sestrojit, aby důkaz již vyplynul skoro sám sebou.

Všimněme si zase jiné stránky věci. Dejme tomu, že studujeme nějakou složitou křivku, odvodili jsme si již řadu jejích vlastností a nyní chceme dokázat, že má jistou další vlastnost P. Zde bude velmi důležitá volba premis, t. j. bude důležité to, z jakých vlastností křivky budeme vycházet, abychom dokázali, že má vlastnost P. Víme-li, o jaké vlastnosti se může opírat vlastnost P, a jaké s ní zase nesouvisí, pak máme již v rukou aspoň zčásti klíč k důkazu.

Jak vidíme z těchto příkladů, bývá často jádrem a klíčem matematického důkazu jednak volba premis, z nichž při důkaze vycházíme, jednak volba metody důkazu (přímý důkaz nebo nepřímý atd.), především však logická konstrukce (udání nebo důkaz existence) vhodných nových prvků (matematických objektů). Je-li důkaz značně složitý, pak může také především záležet na volbě „etap" důkazu, t. j. volbě pomocných vět, které postupně dokazujeme.

Je však jasné, že volba premis a postupu důkazu není logickou součástí důkazu, nýbrž je zde jaksi před důkazem. Po ryze logické stránce spočívá tedy většinou jádro důkazu v logické konstrukci.

5'8. **Logická konstrukce.** Logickou konstrukcí rozumíme zavedení (udání nebo důkaz existence) určitého nového prvku s jistou předem danou vlastností. Musíme poznamenat, že konstrukcí v obvyklém názorném smyslu (geometrickou konstrukcí) se rozumí něco zcela odlišného od logické konstrukce. Při geometrické konstrukci jde totiž buď o skutečné „hmotné" sestrojení určitého geometrického prvku (bodu, přímky, křivky atd.) předepsaným způsobem — na příklad pomocí pravítka a kružítka — nebo o udání předpisu pro takové sestrojení.

Jak jsme již řekli, jde při logické konstrukci vždy o konstrukci prvku s určitou danou vlastností; jinak řečeno, konstrukcí odpovídáme na otázku „existuje prvek, který má vlastnost P, a když ano, který je to prvek?" Logická konstrukce spočívá tedy (1) v udání vlastnosti, kterou má mít konstruovaný prvek; (2) ve vlastní konstrukci. Vlastní konstrukce pak spočívá buď přímo v udání určitého prvku a důkazu, že má předepsanou vlastnost (je to pak vlastně t. zv. konstruktivní

existenční důkaz) anebo v důkaze existence určitého prvku, který má tuto vlastnost.

Jak vidíme, je logická konstrukce vlastně důkazem existence. Rozdíl mezi oběma je v tom, že při vlastní logické konstrukci jde o důkaz existence jednoho a jen jednoho prvku, a že tento prvek pak vstupuje do úvah jako nový „objekt".

Probereme nyní jednotlivé typy konstrukce.

P ř í m á k o n s t r u k c e spočívá v tom, že skutečně udáme prvek, který má žádanou vlastnost, t. j. — obrazně řečeno — na otázku „existuje prvek, který má vlastnost P, a který je to prvek?" odpovíme „a má vlastnost P". Provádíme tedy vlastně, jak jsme již řekli, konstruktivní existenční důkaz.

P ř í k l a d: Máme konstruovat číslo, které hoví rovnici $x^4 = -1$. Toto číslo přímo udáme: je to číslo

$$\frac{1+i}{\sqrt{2}}.$$

K o n s t r u k c e e x i s t e n č n í m d ů k a z e m. Když máme konstruovat prvek, který má vlastnost P, pak konstrukce spočívá v tom, že dokážeme: 1. existuje jeden a jen jeden prvek, který má vlastnost Q; 2. každý prvek, který má vlastnost Q, má také vlastnost P.

P ř í k l a d: Mohli bychom konstruovat číslo, které není algebraické také tímto způsobem: dokážeme, že číslo, které hoví určité rovnici $f(x) = 0$, nemůže být algebraické; pak dokážeme, že existuje jedno a jen jedno číslo, které je řešením této rovnice.

Logický rozdíl mezi tímto typem konstrukce a konstrukcí přímou je mimo jiné v tom, že zde konstruujeme skutečně „nový" prvek, který je charakterisován jen nepřímo jako jediný prvek, který má vlastnost Q; v jistém smyslu se tedy dá říci, že tento prvek je „vytvořen" teprve existenčním důkazem. Naproti tomu

při přímé konstrukci dostane se konstruovaný prvek — řečeno poněkud obrazně — ze známých prvků známými operacemi.

Konstrukce existenčním důkazem má proto pro výstavbu matematiky velmi značný význam. Tak na příklad implicitně stanovená funkce nebo primitivní funkce k dané funkci jsou po logické stránce výsledky konstrukce tohoto typu. Zvlášť velký význam pak má konstrukce založená na existenčním důkaze úplnou indukcí, kterou konstruujeme posloupnosti.

Nevlastní konstrukce. Někdy se mluví o konstrukci také tehdy, když pouze dokazujeme „existuje x, které má vlastnost P". O skutečnou konstrukci zde nejde, protože nestanovíme žádný určitý, dokonale charakterisovaný prvek, který by měl tuto vlastnost. S případy, kdy dovedeme provést jen takovou „nevlastní konstrukci", nikoli však konstrukci skutečnou, se často setkáváme ve vyšších partiích matematiky.