1.1 Индукция в естествените числа

Най-общо, с *индукция* в множеството на естествените числа доказваме *твърдения* от вида $\forall n P(n)$.

Да си припомним двата принципа за индукция в естествените числа, които са ни известни още от училищната математика:

Принцип на обичайната индукция:

$$\frac{P(0), \quad \forall n \; (P(n) \implies P(n+1))}{\forall n P(n)} \qquad \textbf{(1)}$$

Принцип на пълната индукция:

$$\frac{P(0), \quad \forall n \; (\; (P(0) \; \& \; \ldots \; \& \; P(n)) \implies P(n+1) \;)}{\forall n P(n)} \qquad \textbf{(2)}$$

Тази индукция е известна още като *възвратна* или *силна* индукция (*course-of-values induction*).

Да приложим този принцип в решението на следната задача:

Задача 1.1. Докажете, че всяко естествено число, по-голямо или равно на 2, се разлага на прости множители.

Решение. Нека $P(n) \overset{\text{деф}}{\iff} n$ се разлага на прости множители.

База $n = 2$: очевидно 2 се разлага. Фиксираме $n > 2$ и приемаме, че всички числа $m \leq n$ се разлагат (*индуктивна хипотеза*). Имаме 2 случая:

1 сл. $n + 1$ е просто. Този случай е ясен.

2 сл. $n + 1$ е съставно. Тогава за някои k и l, такива че $2 \leq k \leq n$ и $2 \leq l \leq n$, ще имаме $n + 1 = k.l$. Сега не ни остава нищо друго, освен да приложим индуктивната хипотеза $P(k)$ и $P(l)$. □

Привидно изглежда, че тази задача не може да се реши като се използва обичайна индукция. Всъщност само изглежда. Двата принципа са еквивалентни, т.е. всяко твърдение, което можем да докажем с пълна индукция, можем да докажем и с обикновена индукция.

Задача 1.2. Докажете, че принципът на обичайната индукция е еквивалентен на принципа на пълната индукция.

Решение. Ясно е, че ако $\forall n P(n)$ можем да докажем с обичайна индукция, то (толкова повече) можем и със силна.

Сега обратно, нека $\forall n P(n)$ е изведено с втория индуктивен принцип. Това означава, че за P са били изпълнени условията над чертата на правилото за пълна индукция **(2)**:

$$P(0) \quad \text{и} \quad \forall n \; (\; (P(0) \; \& \; \dots \; \& \; P(n)) \implies P(n+1) \;). \tag{1.1}$$

Трябва да покажем, че $\forall n P(n)$, като използваме принципа **(1)**. Ясно е, че директно не можем да приложим този принцип към свойството $P(n)$, но не е и нужно. По условие ни е дадено, че принципът за обичайната индукция е валиден за *всякакви* едноместни свойства в $\mathbb{N}$, ето защо се ориентираме да приложим **(1)** към свойство, което е по-силно от нашето P (с идея, че тогава и индуктивната хипотеза ще е по-силна). Да пробваме със следното свойство $Q(n)$:

$$Q(n) \overset{\text{деф}}{\iff} P(0) \; \& \; \dots \; \& \; P(n).$$

Сега със "слабия" принцип **(1)** ще се опитаме да покажем, че е вярно "силното" свойство $Q(n)$.

База $n = 0$: по определение

$$Q(0) \iff P(0),$$

а $P(0)$ е вярно, съгласно (1.1), значи и $Q(0)$ ще е вярно.

Да допуснем, че за някое n е вярно $Q(n)$, т.е. верни са $P(0) \; \& \; \dots \; \& \; P(n)$. Но тогава отново от (1.1) ще имаме, че е вярно и $P(n + 1)$. Значи общо можем да твърдим, че е в сила

$$P(0) \; \& \; \dots \; \& \; P(n) \; \& \; P(n+1).$$

Но това е точно $Q(n+1)$! Така индукционната стъпка е проведена и вече можем да твърдим, че $\forall n Q(n)$. Понеже

$$Q(n) \implies P(n),$$

то от $\forall n Q(n)$, разбира се, ще следва и $\forall n P(n)$, което и трябваше да покажем.

Да отбележим, че твърдението $Q(n)$ е по-силно от твърдението $P(n)$, обаче

$$\forall n Q(n) \text{ е еквивалентно на } \forall n P(n),$$

така че не сме доказали нищо повече от това, което трябваше ⌣̈. $\square$

Принципът на пълната индукция можем да препишем еквивалентно, като използваме релацията $<$.

Принцип на пълната индукция

$$\frac{\forall n\ (\ \forall m_{m<n} P(m) \implies P(n)\ )}{\forall n P(n)} \qquad \textbf{(3)}$$

Убедете се, че правилата **(2)** и **(3)** са еквивалентни. Според вас къде изчезна базата на индукцията $P(0)$ в правилото **(3)**?

1.2 Фундирани наредби

Нека A е множество, а $<$ е бинарна релация в A. Тази релация наричаме *строга наредба*, ако тя е антирефлексивна и транзитивна (откъдето лесно се вижда, релацията е и антисиметрична).

Примери:

1) $(\mathbb{N}, <)$;

2) $(2^{\mathbb{N}}, \subset)$;

3) $(Fin, \subset)$, където $Fin = \{M \mid M \subseteq \mathbb{N}\ \&\ M \text{ е крайно}\}$;

4) $(\mathcal{F}_n, \subset)$;

5) $(\mathbb{N}^2, \prec)$, където по определение:

$$(x, y) \prec (x', y') \stackrel{\text{деф}}{\iff} x < x' \ \vee\ (x = x'\ \&\ y < y').$$

Тази наредба се нарича *лексикографска наредба* на $\mathbb{N}^2$. Ясно е, че тя е антирефлексивна. За да съобразим, че е и транзитивна, да приемем, че

$(x,y) \prec (x',y')$ и $(x',y') \prec (x'',y'')$. От първото условие имаме, че $x \leq x'$. Разглеждаме поотделно случаите $x < x'$ и $x = x'$:

1 сл. $x < x'$. Тогава от $x' \leq x''$ получаваме $x < x''$ и значи $(x,y) \prec (x'',y'')$.

2 сл. $x = x'$. Ако $x' < x''$, то ще имаме както по-горе $x < x''$. Ако пък $x' = x''$, със сигурност $y < y'$ и $y' < y''$. Получаваме общо $y < y''$, което заедно с $x = x' = x''$ отново ни дава $(x,y) \prec (x'',y'')$.

Определение 1.1. Нека A е непразно множество. Ще казваме, че строгата наредба $<$ в A е *фундирана* (или че $(A,<)$ е *фундирано множество*), ако не съществува редица $x_0, x_1, x_2, \ldots$ от елементи на A, такава че:

$$x_0 > x_1 > x_2 > \ldots$$

Един еквивалентен начин да кажем, че множеството $(A,<)$ е фундирано е следният: всяко непразно множество $B \subseteq A$ има поне един минимален елемент.

Задача 1.3. Определете кои от изброените по-горе строги частични наредби са фундирани.

Упътване. 1) $(\mathbb{N},<)$ е фундирано.

2) $(2^{\mathbb{N}},\subset)$ не е фундирано. Наистина, да означим с M_n множеството $\mathbb{N} \setminus \{0,\ldots,n\}$. Тогава редицата $M_0, M_1, M_2, \ldots$ е строго намаляваща:

$$M_0 \supset M_1 \supset M_2 \supset \ldots$$

3) $(Fin,\subset)$ е фундирано, защото не може да има строго намаляваща редица от крайни множества.

4) $(\mathcal{F}_n,\subset)$ не е фундирано — разсъждавайте както при $(2^{\mathbb{N}},\subset)$.

5) Лексикографската наредба на $\mathbb{N}^2$ е фундирана.

$\square$