It is a famous theorem that every fmla in this structure is equiv. to a fmla w/o quantifiers
From this it can be shown that the only definable subsets (with parameters) of $\mathbb{R}$ are finite sets, intervals, and Boolean combinations of these.

In particular: $\mathbb{N}$ is not definable as a subset of $\mathbb{R}$ in $\mathcal{R}$!

Definability in $\mathcal{N}$

Again: $\mathcal{N} = \langle \mathbb{N}, <, S, +, \cdot, 0 \rangle$

Consider simpler structure:
$\mathcal{N}_{pr} = \langle \mathbb{N}, + \rangle$
"Presburger Arithmetic"

Q: How much simpler are definable sets in $\mathcal{N}_{pr}$ compared to $\mathcal{N}$?

Notice: can define $0, S, <$ in $\mathcal{N}_{pr}$ (how!?)

It follows: definable sets in $\mathcal{N}_{pr}$ same as in $\mathcal{N}_{pr}^{+} = \langle \mathbb{N}, \leq, S, +, 0 \rangle$

Can we define multiplication in $\mathcal{N}_{pr}$?

Fact: $A \subseteq \mathbb{N}$ is definable in $\mathcal{N}_{pr}$ iff A is eventually periodic (i.e. $\exists M, d$ s.t. $\forall n \geq M$ we have $n \in A \Leftrightarrow n = M + kd$ for some $d \in \mathbb{N}$)

↳ won't prove

In particular all definable sets in $\mathcal{N}_{pr}$ are recursive

$\Rightarrow$ Set of squares $S = \{n^2 : n \in \mathbb{N}\}$ not definable in $\mathcal{N}_{pr}$

Hence: multiplication not definable in $\mathcal{N}_{pr}$ — if it were, S would be too.
$k \in S \Leftrightarrow \exists n\,(k = n \cdot n)$

(On other hand: $+$ is definable in $\langle \mathbb{N}, S, \cdot \rangle$ — exercise)

Turns out: adding $\cdot$ to mix increases complexity of definable sets a great deal!!

Theorem (Gödel) Every (partial) recursive function is definable in $\mathcal{N}$. Every r.e. set is definable in $\mathcal{N}$.

From this we get:

Corollary For $A \subseteq \mathbb{N}^k$, A is definable in $\mathcal{N}$ iff $A \in \bigcup \Sigma^0_n$ (i.e. iff A is arithmetical)

↑ this corollary justifies terminology!

Let's prove corollary first

pf. (sketch) ($\Rightarrow$) if A defined by $\varphi(\bar{x})$, may assume φ in prenex n.f.
- so φ is quantifier free, or $\exists_n$ or $\forall_n$ for some n.
- if q.f. check: set defined by φ (i.e. A) is recursive
  ↳ induct on construction of q.f. fmlas — use that polynomials are recursive and rec. sets closed under $\wedge$ and $\neg$.
- if $\exists$, then $A \in \Sigma^0_1$,
  if $\forall$, then $A \in \Pi^0_1$,
- now induct ... $\exists_n \Rightarrow A \in \Sigma^0_n$
  $\forall_n \Rightarrow A \in \Pi^0_n$

$QF \subseteq \Delta^0_1$

Notice: doesn't establish exact relation between $\exists_n$ and Σ^0_n and $\forall_n$ and Π^0_n etc...

($\Leftarrow$) Follows from theorem: if we can define every r.e. relation (Σ^0_1) w/ a fmla, then can define every Π^0_1 relation by taking negations. Now induct: get Σ^0_2 by adding $\exists$'s to a Π^0_1, etc...

Now prove theorem:

Pf: - suffices to prove every recursive f definable: r.e. sets are domains of recursive f, so defined by $\exists y(f(\vec{x})=y)$

- induct on construction of f: show basic fnctns definable, and definable fnctns closed under composition, minimization, prim recursion.

Basic f: projections π^n_i, constant 0 maps c_n, and successor all definable, resp. by:

$\varphi(x_1, \ldots, x_i, \ldots, x_n, y) := y = x_i$

$\varphi(x_1, \ldots, x_n, y) := y = 0$

$\varphi(x, y) := y = S(x)$

Compositions: Sps $f(x_1,\dots,x_k) = h(g_1(\vec{x}),\dots,g_m(\vec{x}))$ and we have

$\chi(y_1,\dots,y_m,z)$ defining (graph of) h

$\tau_i(x_1,\dots,x_k,y)$ defining g_i via

Then: $\varphi(\vec{x},z) := \exists y_1\dots\exists y_m\,(\tau_1(\vec{x},y_1) \wedge \tau_2(\vec{x},y_2) \wedge \dots \wedge \tau_m(\vec{x},y_m) \wedge \chi(y_1,\dots,y_m,z))$

"$g_1(\vec{x})=y_1$ … $g_m(\vec{x})=y_m$ $h(y_1,\dots,y_m)=z$"

defines f.

Minimalization: Sps $f(\vec{x}) = \mu n\,(g(\vec{x},n)=0)$ and sps $\chi(\vec{x},n,y)$ defines "$g(\vec{x},n)=y$"

Then f is defined by

$$\varphi(\vec{x},z) := \exists y\,(\chi(\vec{x},y,0) \wedge \forall y'(y'<y \Rightarrow \exists z'(z'\neq 0 \wedge \chi(\vec{x},y',z') \wedge z=y))$$

Primitive recursion: the tricky one!

Sps f is defined by the recursion:

$$f(0,\vec{x}) = g(\vec{x})$$
$$f(n+1,\vec{x}) = h(f(n,\vec{x}), n, \vec{x})$$

and we have fmlas $\chi(\vec{x}, y)$ for $g(\vec{x}) = y$

and

$\tau(a, b, \vec{x}, c)$ for $h(a,b,\vec{x}) = c$

then f is defined by the "formula"

$$\varphi(n, \vec{x}, z) := (n = 0 \wedge \chi(\vec{x}, z)) \vee (n \neq 0 \wedge \exists \ell_0 \exists \ell_1 \cdots \exists \ell_{n-1} [\chi(\vec{x}, \ell_0) \wedge \tau(\ell_0, 0, \vec{x}, \ell_1) \wedge \tau(\ell_1, 1, \vec{x}, \ell_2) \wedge \cdots \wedge \tau(\ell_{n-1}, n-1, \vec{x}, z)])$$

↳ not a fmla since # of $\exists \ell_i$ quantifiers depends on n.
- need to do some coding - Gödel saw how

Want: definable $\gamma(\ell, i)$ s.t. for any n and sequence $\ell_0, \ldots, \ell_{n-1}$ there is ℓ s.t. $\gamma(\ell, i) = \ell_i$ $\forall i < n$.

Could use p.r. Gödel fcn $(\ell)_i$ if we knew this was definable (we don't yet)

Instead we use: $\beta(a,b,i)$ s.t. $\forall n$ and all $\ell_0, \ldots, \ell_{n-1}$ $\exists e$ s.t. $\forall i<n$, $\beta(a,b,i) = \ell_i$

(β stores information in remainders instead of prime powers)

Defn Gödel's β function is the map
$\beta(a,b,i) = \text{rem}(a, 1+(i+1)b)$

where $\text{rem}(x,y)$ = remainder in division x/y

Notice: β is definable in $\mathcal{N}$ (+,·) by
$\varphi(a,b,i,z) :=$
$\exists q [q \cdot (1+(i+1)b) + z = a$
$\wedge z < (1+(i+1)b)]$

(where 1 denotes $S(0)$, etc)

Lemma if $n > 0$, then for every sequence $\ell_0, \ldots, \ell_{n-1}$ there are a, b s.t. $\beta(a,b,i) = \ell_i$ $\forall i<n$

Before we prove, observe then we can use β to get def'n for R above: replace the clause $\exists \ell_0 \ldots \exists \ell_{n-1}$ (...) by:

"$\exists a \exists b \; \forall i < n \; \exists \ell_i \exists \ell_{i+1}$
$[\beta(a,b,i) = \ell_i \wedge \beta(a,b,i+1) = \ell_{i+1}$
$\wedge g(\vec{x}) = \ell_0 \wedge h(\ell_i, i, \vec{x}) = \ell_{i+1}$
$\wedge \ell_n = y]$"

(this is informally written - can you write formally?)

So need only prove Lemma.
We'll need:

Chinese remainder theorem (CRT): if $b_0, \ldots, b_{n-1}$ are relatively prime pairwise, and $\ell_0, \ldots, \ell_{n-1}$ is a sequence s.t. $\ell_i < b_i$ $\forall i < n$ then there is $a \in \mathbb{N}$ s.t. $\ell_i = \text{rem}(a, b_i)$ $\forall i < n$

(i.e. a solves the system of congruences $a \equiv \ell_i \pmod{b_i}$)

Pf of Lemma from CRT:

- Let $k > \max\{n, \ell_0, \ldots, \ell_{n-1}\}$

- Let $b = k!$
- For $i < n$ let $b_i = 1 + (i+1)b$
  $= 1 + (i+1)k!$
- clearly $\ell_i < b_i$ $\forall i < n$ (by choice of k)
- We claim b_i are pairwise coprime:
  - if b_i, b_j shared prime factor p, then $p \mid b_j - b_i$ i.e.
    $p \mid b(j-i)$ i.e. $p \mid k!(j-i)$
  - but then since $|j-i| < k$ we have $j-i \mid k!$ hence must be $p \mid k!$ i.e. $p \mid b$
  - but then since $p \mid b_i = 1 + (i+1)b$ gives $p \mid 1$ contradiction

Hence b_i satisfy hypotheses of CRT
Let a be as guaranteed by CRT
then $\text{rem}(a, b_i) = \ell_i$ $\forall i$
i.e. $\text{rem}(a, 1 + (i+1)b) = \ell_i$ $\forall i$
ie $\beta(a, b, i) = \ell_i$ ✓ $\forall i$

Proof of CRT: pigeonhole argument!

- For any d let $r(d) = (d_0, \ldots, d_{n-1})$ where $d_i = \text{rem}(d, b_i)$
- notice: at most $b_0 \cdot b_1 \cdot \ldots \cdot b_{n-1} = t$ many possible $r(d)$'s.

↱ so then $r(d) = (\ell_0, \ldots, \ell_{n-1})$ for some $d < t$

- let claim r is 1-1 for $d \in \{0, 1, \ldots, t-1\}$
- if not there are $e < d < t$ s.t. $r(e) = r(d)$
- so $d_i = e_i$ $\forall i \le n$
- so $b_i \mid d - e$ $\forall i$

$\Rightarrow$ (since b_i coprime) $b_0 \cdot b_1 \cdots b_{n-1} \mid d - e$

but $b_0 \cdots b_{n-1} > d - e$

contradiction ✓