$\mathbb{Q}$ における $\mathbb{N}$ の定義可能性に関する J. Robinson の定理について（前編）

近藤 友祐 （神戸大学大学院システム情報学研究科）

最終更新：2020 年 10 月 20 日

このノート[*1]とこれに続く「後編」では，次の定理の証明を与える．

定理 1 (J. Robinson, Theorem 3.1 in [7], 1949)**.** 有理数全体の集合 $\mathbb{Q}$ に通常の加法と乗法を入れた構造 $\mathbb{Q} = \langle \mathbb{Q}; +^{\mathbb{Q}}, \cdot^{\mathbb{Q}} \rangle$ において，整数全体の集合 $\mathbb{Z}$ および自然数全体の集合 $\mathbb{N}$ はパラメータなしで定義可能である．すなわち，言語 $\{+, \cdot\}$ におけるパラメータなしの 1 変数論理式 $\varphi_{\mathrm{int}}(v)$, $\varphi_{\mathrm{nat}}(v)$ であって，

$$\mathbb{Z} = \{a \in \mathbb{Q} : \mathbb{Q} \models \varphi_{\mathrm{int}}(a)\}, \qquad \mathbb{N} = \{a \in \mathbb{Q} : \mathbb{Q} \models \varphi_{\mathrm{nat}}(a)\} \tag{1}$$

を満たすものが存在する．しかも，$\varphi_{\mathrm{int}}(v)$ と $\varphi_{\mathrm{nat}}(v)$ は具体的に次のように取ることができる[a]：

$$\varphi_{\mathrm{int}}(v): \quad \forall r \forall s (\psi(r, s, 0) \wedge \forall u (\psi(r, s, u) \to \psi(r, s, u + 1)) \to \psi(r, s, v)), \tag{2}$$
$$\varphi_{\mathrm{nat}}(v): \quad \varphi_{\mathrm{int}}(v) \wedge \pi(v). \tag{3}$$

ここに

$$\psi(r, s, v): \quad \exists x \exists y \exists z (2 + rsv^2 = x^2 + ry^2 - sz^2), \tag{4}$$
$$\pi(v): \quad \exists x \exists y \exists z \exists w (v = x^2 + y^2 + z^2 + w^2). \tag{5}$$

[a] R. Robinson の名を挙げて，$\pi(v)$ として $\exists x \exists y (\varphi_{\mathrm{int}}(x) \wedge (v = x^2 \vee 1 + vy^2 = x^2))$ を選ぶこともできると指摘している．

[7] において，Robinson は言語として環の言語 $\mathcal{L}_{\mathrm{R}} = \{+, -, \cdot, 0, 1\}$ ではなく $\{+, \cdot\}$ を採用している．$\varphi_{\mathrm{int}}(v)$ は一見 $\mathcal{L}_{\mathrm{R}}$-論理式のように思えるが，移項によって $-$ を除去し，“$x = 0$” を表す論理式 “$x + x = x$” および “$x = 1$” を表す論理式 “$(x \cdot x = x) \wedge (x + x \neq x)$” を用いて定数記号 $0, 1$ を除去できる．$\varphi_{\mathrm{int}}(v)$ とは正確にはそのように同値変形して得られる $\{+, \cdot\}$-論理式のことである．ただし，変形の際に量化子が増加するため，論理式の複雑さを評価したいような文脈では安易に同一視することはできない．このノートではそのようなデリケートな問題は扱わないため，現代的（？）に最初から $\mathbb{Q}$ を $\mathcal{L}_{\mathrm{R}}$-構造と考え，$\mathcal{L}_{\mathrm{R}}$-論理式を自由に用いることとする．

[*1] **TODO** としたところは適宜加筆していく．

「前編」では，2 つの主要補題（補題 2 と補題 3）を事実として認めた上で定理 1 の証明を与える．また，最後に少しだけ $\mathbb{Q}$ 以外の代数構造についてすでに知られている結果を紹介する．「後編」では，いくつかの数論の定理を事実と認めた上で補題 2 と補題 3 の証明を与える．

1　記法の約束

$\mathbb{N} = \{0, 1, 2, \ldots\}$ である．$\psi(r, s, v)$, $\pi(v)$, $\varphi_{\mathrm{int}}(v)$, $\varphi_{\mathrm{nat}}(v)$ は定理 1 に掲げたものを指すこととする．

$a \in \mathbb{Q}$ について，$a = u/v$ $(u, v \in \mathbb{Z},\, v \neq 0)$ が**既約分数表示**であるとは，u と v が共通素因数をもたないことをいう．$a = u/v$ が既約分数表示ならば $a = (-u)/(-v)$ も既約分数表示なので，既約分数表示は常に 2 通り存在する．

共通素因数をもたない 2 つの整数 $n \in \mathbb{Z} \setminus \{0\}$ および $m \in \mathbb{N} \setminus \{0, 1\}$ に対し，**Legendre 記号**，あるいは**平方剰余記号** $\left(\frac{n}{m}\right)$ を

$$\left(\frac{n}{m}\right) = \begin{cases} 1 & \text{if } (\exists x \in \mathbb{Z})[x^2 \equiv n \pmod{m}] \\ -1 & \text{o.w.} \end{cases} \tag{6}$$

で定義する[*2]．(n/m) と書くこともある．$(n/m) = 1$ のとき，n は $\boldsymbol{m}$ **を法として平方剰余である**という．$(n/m) = -1$ のとき，n は $\boldsymbol{m}$ **を法として平方非剰余である**という[*3]．混乱を避けるため，この記号は n と m が共通素因数をもたないことが文脈から明らかな場合のみにしか使わないことにする．したがって，$n = 0$ のときどうに定義するかは考えなくてよい[*4]．Legendre 記号に関する諸性質は断りなく用いる．

プログラミングの慣習に倣い，整数 a を正の整数 n で除した際の剰余を a % n で表す．これは標準的には $a \bmod n$ と書かれるものであるが，$a \bmod n$ は長いし，同じ語 “mod” が関係記号としても函数記号としても使われるのが気に食わないのでそうする．

2　定理 1 の証明のアイデア

具体的な議論に入る前に基本的なアイデアを述べておこう．$\mathbb{Q}$ の部分集合 X が**帰納的 (inductive)** であるとは，X が

$$0 \in X \quad \& \quad (\forall a \in \mathbb{Q})[a \in X \Longrightarrow a + 1 \in X] \tag{7}$$

を満たすことであった．そして $\mathbb{N}$ は包含関係について最小の帰納的集合として定義されるのであった[*5]．$\mathfrak{X} \subseteq \mathcal{P}(\mathbb{Q})$ を，$\mathbb{Q}$ の帰納的部分集合全体からなる集合族と定める．$\mathbb{N}$ は，$\mathbb{N} = \bigcap \mathfrak{X}$，つまり各 $a \in \mathbb{Q}$ について

$$a \in \mathbb{N} \quad \Longleftrightarrow \quad \forall X \in \mathcal{P}(\mathbb{Q})[X \text{ inductive } \Longrightarrow\ a \in X] \tag{8}$$

[*2] $\left(\frac{n}{m}\right) = 1$ の証拠となる x は $x \in (0, m)$ としてとれる．実際，$x = ad + x_0$ $(a \in \mathbb{Z}, 0 \leqslant x_0 < m)$ と割り算すれば $n \equiv x^2 = m(a^2 + 2dx_0) + x_0^2 \equiv x_0^2 \pmod{m}$ なので，この x_0 を証拠に $(n/m) = 1$ である．$x_0 = 0$ なら $0 = x_0^2 \equiv n \neq 0$ なので $x = 0$ ではありえないことに注意．

[*3] なんとなく気持ち悪い響きだが，“非平方剰余” の typo ではない．

[*4] $(0/m) = 0$ と定めることが多いようである．

[*5] あるいは別の方法で $\mathbb{N}$ が定義され，それが包含関係について最小の帰納的集合であることが定理として証明される．

を満たす集合である．したがって，2 階の $\mathcal{L}_{\mathrm{R}}$-論理式 $\varphi_{\mathrm{nat2}}(v)$ を

$$\varphi_{\mathrm{nat2}}(v)\colon\quad \forall X(0\in X\wedge\forall u(u\in X\to u+1\in X)\to v\in X) \tag{9}$$

で定めれば

$$a\in\mathbb{N}\quad\Longleftrightarrow\quad\langle\mathbb{Q},\mathcal{P}(\mathbb{Q})\rangle\models\varphi_{\mathrm{nat2}}(a) \tag{10}$$

が成り立つので，これをもって $\mathbb{N}$ は **2 階論理で**定義可能な $\mathbb{Q}$ の部分集合であることがわかった．

しかし我々は $\mathbb{N}$ が **1 階論理で**定義可能であることを示したい．そのために Robinson が考えたのは，

あらゆる帰納的集合からなる集合族 $\mathfrak{X}\subseteq\mathcal{P}(\mathbb{Q})$ を参照するの**ではなく**，
$\mathfrak{X}$ から **1 階論理で定義可能な**帰納的集合からなる集合族 $\mathfrak{X}'\subseteq\mathcal{D}^{+}(\mathbb{Q})$ を
うまく切り取って $\mathbb{N}=\bigcap\mathfrak{X}'$ とできないか？

ということである[*6]．そして実際に整数論の定理を応用することでこれを実現した．具体的には，$s,t\in\mathbb{Q}$ でパラメータ付けられた定義可能集合

$$\begin{aligned}X_{r,s}:=&\{a\in\mathbb{Q}:\mathbb{Q}\models\psi(r,s,a)\}\\=&\{a\in\mathbb{Q}:\mathbb{Q}\models\exists x\exists y\exists z(2+rsa^2=x^2+ry^2-sz^2)\}\in\mathcal{D}^{+}(\mathbb{Q})\end{aligned}$$

からなる集合族 $\mathfrak{A}:=\{X_{r,s}\in\mathcal{P}(\mathbb{Q}):r,s\in\mathbb{Q}\}\subseteq\mathcal{D}^{+}(\mathbb{Q})$ および，パラメータなしで定義な可能集合

$$\begin{aligned}P:=&\{a\in\mathbb{Q}:\mathbb{Q}\models\pi(a)\}\\=&\{a\in\mathbb{Q}:\mathbb{Q}\models\exists x\exists y\exists z\exists w(a=x^2+y^2+z^2+w^2)\}\in\mathcal{D}^{+}(\mathbb{Q})\end{aligned}$$

を考えた．そして $\mathfrak{X}':=\mathfrak{X}\cap(\mathfrak{A}\cup\{P\})$ とすることで $\mathbb{N}=\bigcap\mathfrak{X}'$ となることを示した．

気になるのは謎の $X_{r,s}\subseteq\mathbb{Q}$ は何者かということである．r と s は $\mathbb{Q}$ 全体を走るわけだが，特に $(r,s)=(1,p),(q,p)$（ここに p と q は一定の条件を満たす素数）の場合が重要である．**$X_{1,p}$ や $X_{q,p}$ は，分母が素因数をもたないことを強制する帰納的集合になっている**のである．すなわち，$a\in\mathbb{Q}$ が $a\in X_{1,p}$ や $a\in X_{q,p}$ を満たすとき，a の既約分数表示の分母は p や q や 2 で割り切れない．$a\in\bigcap(\mathfrak{X}\cap\mathfrak{A})$ とすると，a はあらゆる $X_{1,p}$, $X_{q,p}$ たちに属するわけなので，a の分母が素因数をもつ可能性がすべて削られていく．したがって a の要素の分母は ±1 に限られる．このようにして $\bigcap(\mathfrak{A}\cap\mathfrak{X})\subseteq\mathbb{Z}$ がわかる．逆向きの包含関係は容易である．最後に Lagrange の四平方定理を用いて $\mathbb{Q}$ の非負部分 P を定義して負の部分を切り落とし，$\mathbb{N}$ を得る．これが証明のアイデアである．これから正確な議論を始める．

3　2 つの主要補題

定理 1 の証明にあたって次の 2 つの事実を認めることとする．証明は（いくつかの数論の大道具を証明なしに用いて）「後編」で行う．

[*6] $\mathcal{D}^{+}(\mathbb{Q})$ $(\subseteq\mathcal{P}(\mathbb{Q}))$ は，$\mathbb{Q}$ のパラメータを許した $\mathcal{L}_{\mathrm{R}}$-論理式で定義可能な $\mathbb{Q}$ の部分集合全体のこと．

補題 2 (Lemma 3 in [7])**.** p を $p \equiv 3 \pmod 4$ なる素数，t を有理数とし，$t = u/v$ と既約分数として表示する $(u, v \in \mathbb{Z},\ v \neq 0)$．このとき以下は同値である：

(A) $(\exists x, y, z \in \mathbb{Q})[pt^2 + 2 = x^2 + y^2 - pz^2]$;
(B) $2 \nmid v \quad \& \quad p \nmid v$.

補題 3 (Lemma 4 in [7])**.** p を $p \equiv 1 \pmod 4$ なる素数，$q \neq p$ を奇素数であって $(q/p) = -1$ を満たすものとする．t を有理数とし，$t = u/v$ と既約分数として表示する $(u, v \in \mathbb{Z},\ v \neq 0)$．このとき以下は同値である：

(A) $(\exists x, y, z \in \mathbb{Q})[pqt^2 + 2 = x^2 + qy^2 - pz^2]$;
(B) $p \nmid v \quad \& \quad q \nmid v$.

これらの補題は，先ほど導入した記号 $X_{r,s} := \{t \in \mathbb{Q} : \mathbb{Q} \models \psi(r, s, t)\}$ を用いて次のように言い換えられる：

補題 4. p を $p \equiv 3 \pmod 4$ なる素数とする．このとき，任意の $t \in \mathbb{Q}$ について以下が成り立つ：

$$t \in X_{1,p} \iff t \text{ を既約分数表示した時の分母は } p \text{ で割り切れない奇数である．} \tag{11}$$

補題 5. p を $p \equiv 1 \pmod 4$ なる素数，$q \neq p$ を奇素数であって $(q/p) = -1$ を満たすものとする．このとき，任意の $t \in \mathbb{Q}$ について以下が成り立つ：

$$t \in X_{q,p} \iff t \text{ を既約分数表示した時の分母は } p \text{ でも } q \text{ でも割り切れない．} \tag{12}$$

4 $X_{1,p}$ と $X_{q,p}$ の帰納性

まず $p \equiv 3 \pmod 4$ のケースを考える．

命題 6. p を，$p \equiv 3 \pmod 4$ を満たす奇素数とする．このとき $X_{1,p}$ は帰納的集合である．

証明. $0 \in \mathbb{Q}$ の既約分数表示の分母は ± 1 である．± 1 は p で割り切れない奇数なので，補題 4 $(\Leftarrow)$ より $0 \in X_{1,p}$ である．$u \in \mathbb{Q}$ を勝手に取り，$u \in X_{1,p}$ を仮定する．$u = \frac{n}{d}$ $(n, d \in \mathbb{Z},\ d \neq 0)$ と既約分数として表示する．補題 4 $(\Rightarrow)$ より d は p で割り切れない奇数である．いま，$u + 1 = \frac{n+d}{d}$ であり，これは既約分数表示である[*7]．よって $u + 1$ の既約分数表示の分母（つまり d）は p で割り切れない奇数である．再び補題 4 $(\Leftarrow)$ より $u + 1 \in X_{1,p}$ である． □

[*7] $(\because)$ 仮にある素数 r があって $n + d = ra$, $d = rb$ $(a, b \in \mathbb{Z})$ と書けたなら $n = r(a - b)$ となるから $r \mid n$ かつ $r \mid d$ である．これは n/d の既約性に矛盾.

次に $p \equiv 1 \pmod 4$ のケースを考える．これには少し準備が必要となる．

命題 7. p を奇素数とする（ここでは $p \equiv 1 \pmod 4$ は特に仮定しない）．このとき，集合 $[1, p-1] := \{1, 2, \ldots, p-1\}$ の中には p を法として平方剰余であるものと平方非剰余であるものが同数ずつ存在する．

証明. S を p を法とした平方剰余全体とする．

$$\begin{aligned}
S &= \{n^2 \ \% \ p : 1 \leqslant n \leqslant p-1\} \\
&= \left\{n^2 \ \% \ p : 1 \leqslant n \leqslant \frac{p-1}{2}\right\} \cup \left\{n^2 \ \% \ p : \frac{p+1}{2} \leqslant n \leqslant p-1\right\} \\
&= \left\{n^2 \ \% \ p : 1 \leqslant n \leqslant \frac{p-1}{2}\right\} \cup \left\{(p-k)^2 \ \% \ p : 1 \leqslant k \leqslant \frac{p-1}{2}\right\} \\
&= \left\{n^2 \ \% \ p : 1 \leqslant n \leqslant \frac{p-1}{2}\right\} \cup \left\{k^2 \ \% \ p : 1 \leqslant k \leqslant \frac{p-1}{2}\right\} \\
&= \left\{n^2 \ \% \ p : 1 \leqslant n \leqslant \frac{p-1}{2}\right\}
\end{aligned}$$

が成り立つ．

写像 $f\colon [1, \frac{p-1}{2}] \ni a \mapsto a^2 \ \% \ p \in [0, p-1]$ を考える．これは単射である〔$1 \leqslant a < b \leqslant \frac{p-1}{2}$ とする．$a^2 \ \% \ p = b^2 \ \% \ p$ を仮定して矛盾を導く．$(b-a)(b+a) \equiv 0 \pmod p$ である．よって $p \mid (b-a)$ または $p \mid (b+a)$ である．前者について，$0 < b-a < p$ なのでこれはあり得ない．後者についても $0 < b+a < p$ なのでこれもあり得ない．矛盾〕．したがって $|S| = |\mathrm{ran}(f)| = \frac{p-1}{2}$ である．平方非剰余全体は $[1, p-1] \setminus S$ に等しいので，その個数は $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ である． □

命題 8 (Lemma 5 in [7])**.** p が $p \equiv 1 \pmod 4$ を満たす奇素数であるとき，$(q/p) = -1$ を満たす奇素数 $q \neq p$ が存在する．

証明. p は奇素数なので，命題 7 より $(s/p) = -1$ を満たす $s \in \{1, 2, \ldots, p-1\}$ が存在する．そのような s を 1 つ固定する．$(s+p/p) = (s/p) = -1$ なので，$s \neq 1$ かつ $s+p \neq 1$ である．いま，s か $s+p$ のいずれか一方，そして一方のみが奇数である．• s が奇数のとき．$s \neq 1$ を，$s = q_1 q_2 \cdots q_n$ $(n \geqslant 1)$ と素数の積に分解する．ただし各 q_i は素数で，重複を許す．s は奇数なので，各 q_i は奇素数でなければならない．また $p \nmid s$ なので $p \nmid q_i$ である．Legendre 記号の性質 (cf. [13], 系 1.11.5) より $(q_1/p)(q_2/p)\cdots(q_n/p) = (q_1 q_2 \cdots q_n/p) = (s/p) = -1$ である．よって (q_1/p), (q_2/p), …, (q_n/p) の少なくともひとつは -1 に等しくなければならない．そのような q_i をひとつ選んで q とせよ．• $s+p$ が奇数のとき．$s+p \neq 1$ を，$s+p = q'_1 q'_2 \cdots q'_m$ $(m \geqslant 1)$ と素数の積に分解する．ただし各 q'_j は素数で，重複を許す．$s+p$ は奇数なので，各 q'_i は奇素数でなければならない．また $p \nmid (s+p)$ なので $p \nmid q'_j$ である．したがって $(q'_1/p)(q'_2/p)\cdots(q'_m/p) = (q'_1 q'_2 \cdots q'_m/p) = (s+p/p) = (s/p) = -1$ である．よって (q'_1/p), (q'_2/p), …, (q'_m/p) の少なくともひとつは -1 に等しくなければならない．そのような q'_j をひとつ選んで q とせよ． □

命題 9. p を $p \equiv 1 \pmod 4$ を満たす奇素数とし，$q \neq p$ を $(q/p) = -1$ を満たす奇素数とする．このとき $X_{q,p}$ は帰納的集合である．

証明. $0 \in \mathbb{Q}$ の既約分数表示の分母は ± 1 である．± 1 は p でも q でも割り切れないので，補題 5 ($\Leftarrow$) より $0 \in X_{q,p}$ である．$u \in \mathbb{Q}$ を勝手に取り，$u \in X_{q,p}$ を仮定する．$u = \frac{n}{d}$ $(n, d \in \mathbb{Z},\, d \neq 0)$ と既約分数として表示する．補題 5 ($\Rightarrow$) より d は p でも q でも割り切れない．いま，$u + 1 = \frac{n+d}{d}$ であり，これは既約分数表示である．よって $u+1$ の既約分数表示の分母（つまり d）は p でも q でも割り切れない．再び補題 5 ($\Leftarrow$) より $u + 1 \in X_{q,p}$ である． □

5 定理 1 の証明

定理 1 を定理 10 と定理 12 の 2 つに分けて示す．

定理 10. 任意の $a \in \mathbb{Q}$ に対し，$a \in \mathbb{Z} \iff \mathbb{Q} \models \varphi_{\mathrm{int}}(a)$ が成り立つ．

$\varphi_{\mathrm{int}}(v)$ とは $\forall r \forall s(\psi(r, s, 0) \wedge \forall u(\psi(r, s, u) \to \psi(r, s, u + 1)) \to \psi(r, s, v))$ のことであったから，各 $a \in \mathbb{Q}$ に対し，$\mathbb{Q} \models \varphi_{\mathrm{int}}(a)$ であることは

$$(\dagger)_a : \quad (\forall r, s \in \mathbb{Q})[X_{r,s} \text{ inductive } \implies a \in X_{r,s}] \tag{13}$$

であることと同値である．したがって $a \in \mathbb{Z} \iff (\dagger)_a$ を示せばよいので，これを示す．

証明. $\boxed{\Longrightarrow}$ まず，$\psi(r, s, v)$ の定義において v は 2 乗の形でしか出現しないので $\mathbb{Q} \models \forall r \forall s \forall v(\psi(r, s, v) \leftrightarrow \psi(r, s, -v))$ である．したがって, 各 $b \in \mathbb{Q}$ について, $\mathbb{Q} \models \varphi_{\mathrm{int}}(b)$ (つまり $(\dagger)_b$) であることとと $\mathbb{Q} \models \varphi_{\mathrm{int}}(-b)$ (つまり $(\dagger)_{-b}$) であることは同値である．よって，定理の ($\Longrightarrow$) を示すには任意の $n \in \mathbb{N}$ について $(\dagger)_n$ であることを示せば十分である．数学的帰納法で示す．

$n = 0$ のとき．$r^*, s^* \in \mathbb{Q}$ を勝手にとり，X_{r^*,s^*} が帰納的集合であることを仮定する．“帰納的集合” の定義より $0 \in X_{r^*,s^*}$ である．$n = k$ で成立すると仮定する．$n = k + 1$ について示すため，$r^*, s^* \in \mathbb{Q}$ を勝手にとり，X_{r^*,s^*} が帰納的集合であることを仮定する．帰納法の仮定 $(\dagger)_k$ を $r = r^*$, $s = s^*$ として用いることで $k \in X_{r^*,s^*}$ である．“帰納的集合” の定義より $k + 1 \in X_{r^*,s^*}$ である．

$\boxed{\Longleftarrow}$ $a \in \mathbb{Q}$ が $(\dagger)_a$ をを満たしていると仮定する．a の分母がいかなる素数によっても割り切れないことを示せば（a の分母が ± 1 であることがわかり，したがって $a \in \mathbb{Z}$ となるから）十分である．p を勝手な素数とする．• $p = 2$ のとき．命題 6 より $X_{1,3}$ は帰納的集合である．$(\dagger)_a$ を $r = 1$, $s = 3$ として用いて $a \in X_{1,3}$ である．補題 4 より a の分母は奇数である．よって a の分母は p $(= 2)$ で割り切れない．• $p \equiv 3 \pmod 4$ のとき．命題 6 より $X_{1,p}$ は帰納的集合である．$(\dagger)_a$ を $r = 1$, $s = p$ として用いて $a \in X_{1,p}$ である．補題 4 より a の分母は p で割り切れない．• $p \equiv 1 \pmod 4$ のとき．命題 8 より $(q/p) = -1$ を満たす奇素数 $q \neq p$ がとれる．命題 9 より $X_{q,p}$ は帰納的集合である．$(\dagger)_a$ を $r = q$, $s = p$ として用いて $a \in X_{q,p}$ である．補題 5 より a の分母は p で割り切れない． □

第 2 節で導入した記号 $\mathfrak{X}, \mathfrak{A}$ を用いると，結局 $\mathbb{Z} = \bigcap(\mathfrak{X} \cap \mathfrak{A})$ がわかった[*8]わけである．

補題 11. 任意の $a \in \mathbb{Q}$ に対し，$a \geqslant 0 \iff \mathbb{Q} \models \pi(a)$ が成り立つ．

証明. ($\Longleftarrow$) は自明．($\Longrightarrow$): a を $a = n/d$ $(n, d \in \mathbb{Z},\ d \neq 0)$ と表す．$d^2 a$ は非負整数であるから，Lagrange の四平方定理 (cf. [13], 定理 2.4.4) より，$dn = d^2 a = x_0^2 + y_0^2 + z_0^2 + w_0^2$ を満たす $x_0, y_0, z_0, w_0 \in \mathbb{Z}$ が存在する．各辺を $d^2 \neq 0$ で除すことで，結局 $(x, y, z, w) = (x_0/d, y_0/d, z_0/d, w_0/d) \in \mathbb{Q}^4$ を証拠に $\mathbb{Q} \models \pi(a)$ が成立する． □

第 2 節で導入した記号を用いると，$P = \mathbb{Q}_{\geqslant 0}$（$\mathbb{Q}$ の非負部分）がわかったわけである．P は帰納的集合なので $P \in \mathfrak{X}$ である．

定理 12. 任意の $a \in \mathbb{Q}$ に対し，$a \in \mathbb{N} \iff \mathbb{Q} \models \varphi_{\mathrm{nat}}(a)$ が成り立つ．

証明. $a \in \mathbb{N} \iff a \in \mathbb{Z}\ \&\ a \geqslant 0 \iff \mathbb{Q} \models \varphi_{\mathrm{int}}(a)\ \&\ \mathbb{Q} \models \pi(a) \iff \mathbb{Q} \models \varphi_{\mathrm{nat}}(a)$. □

第 2 節で導入した記号を用いると，$\mathfrak{X}' = \mathfrak{X} \cap (\mathfrak{A} \cup \{P\}) \subseteq \mathcal{D}^+(\mathbb{Q})$ を用いて $\mathbb{N} = \bigcap \mathfrak{X}'$ と書けた[*9]わけである．

6 $\mathbb{Q}$ 以外の代数構造

$\mathbb{Q}$ 以外の代数構造をめぐる状況をまとめる．Flath and Wagon ([3], 1991) の記述に基づいているので，情報が古いかもしれない．

$\mathbb{Q}$ の有限次代数拡大

$\mathbb{Q}$ の有限次代数拡大を**代数体** (algebraic number field) あるいは単に**数体** (number field) という．**任意の数体で $\mathbb{Z}$ は定義可能である** (J. Robinson [8], 1951).

$\mathbb{Z}$ 係数モニック多項式（i.e. 最高次の係数が 1）の根となりうる複素数を**代数的整数**といい，その全体がなす環を $\mathbb{A}$ と書く．数体 L の**整数環** $\mathcal{O}_L$ を $\mathcal{O}_L := \mathbb{A} \cap L$ で定める．例えば $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ となる，この意味で $\mathbb{Z}$ は有理整数環とも呼ばれることもある．

定理の証明は 2 つの部分からなる．1 つめは L における $\mathcal{O}_L$ の定義可能性．2 つめは $\mathcal{O}_L$ における $\mathbb{Z}$ の定義可能性．前半は $\mathbb{Q}$ における $\mathbb{Z}$ の定義可能性のアナロジー. 代数的整数論を用いる難しい議論のようだ．後半は比較的簡単らしい．

$$L \underset{\text{definable}}{\overset{\text{difficult}}{\supseteq}} \mathcal{O}_L \underset{\text{definable}}{\overset{\text{easy}}{\supseteq}} \mathbb{Z}. \tag{14}$$

[*8] $a \in \mathbb{Q}$ について，$a \in \bigcap(\mathfrak{X} \cap \mathfrak{A}) \iff (\forall X \subseteq \mathbb{Q})[X \in \mathfrak{A} \cap \mathfrak{X} \implies a \in X] \iff (\forall X \subseteq \mathbb{Q})[(\exists r, s \in \mathbb{Q})[X = X_{r,s}]\ \&\ X \text{ inductive} \implies a \in X] \iff (\forall r, s \in \mathbb{Q})[X_{r,s} \text{ inductive} \implies a \in X_{r,s}] \iff (\dagger)_a \iff \mathbb{Q} \models \varphi_{\mathrm{int}}(a) \iff a \in \mathbb{Z}$.

[*9] $\mathfrak{X}' = \mathfrak{X} \cap (\mathfrak{A} \cup \{P\}) = (\mathfrak{X} \cap \mathfrak{A}) \cup (\mathfrak{X} \cap \{P\}) = (\mathfrak{X} \cap \mathfrak{A}) \cup \{P\}$．したがって $\bigcap \mathfrak{X}' = (\bigcap(\mathfrak{X} \cap \mathfrak{A})) \cap P = \mathbb{Z} \cap \mathbb{Q}_{\geqslant 0} = \mathbb{N}$.

本来興味深いのは左側の包含関係であろう．それについては M. Ziegler ([12], 2012) で議論されている[*10]．

しかしながら右側の包含関係にも面白い問題があるようで，それを紹介する．$\mathcal{O}_{\mathbb{Q}}$ で $\mathbb{Z}$ がディオファントス的（i.e. Σ_1-論理式で定義可能）であることは $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ なので自明である．$\mathbb{Q}$ でない一般の体でこの状況はどうなるか？という問題である．

二次体

$\mathbb{Q}$ の 2 次の代数拡大を**二次体** (quadratic field) という．**任意の二次体 L について，$\mathcal{O}_L$ で $\mathbb{Z}$ はディオファントス的である** (J. Denef and L. Lipshitz [1], 1978).

$$L \text{ number field} \quad \& \quad [L:\mathbb{Q}] = 2 \quad \Longrightarrow \quad \mathcal{O}_L \underset{\Sigma_1\text{-definable}}{\supseteq} \mathbb{Z}. \tag{15}$$

Danef と Lipshitz は “任意の二次体” を “任意の数体” に置き換えられると予想した．これに関して次の部分解が得られている：

総実体，$\mathbb{Q}$ の Abel 拡大

数体 L が**総実** (totally real) であるとは，L の $\mathbb{C}$ への任意の埋め込み $\iota\colon L \hookrightarrow \mathbb{C}$ について $\mathrm{ran}(\iota) \subseteq \mathbb{R}$ が成り立つことをいう[*11]．数体 L が $\mathbb{Q}$ の **Abel 拡大**であるとは，$L/\mathbb{Q}$ が Galois 拡大であって $\mathrm{Gal}(L/\mathbb{Q})$ が Abel 群であることをいう．**L が総実体，総実体の 2 次拡大** (J. Denef [2], 1980)，**$\mathbb{Q}$ の Abel 拡大** (A. Shlapentokh and H.N. Shapiro [10], 1989) **のいずれかならば，$\mathbb{Z}$ は $\mathcal{O}_L$ でディオファントス的である**.

$$L \text{ number field, totally real} \quad \Longrightarrow \quad \mathcal{O}_L \underset{\Sigma_1\text{-definable}}{\supseteq} \mathbb{Z}. \tag{16}$$

$$L, K \text{ number field} \quad \& \quad L/K \quad \& \quad [L:K] = 2 \quad \& \quad K \text{ totally real} \quad \Longrightarrow \quad \mathcal{O}_L \underset{\Sigma_1\text{-definable}}{\supseteq} \mathbb{Z}. \tag{17}$$

$$L/\mathbb{Q}\text{: alg. ext.} \quad \& \quad \text{Abel ext.} \quad \Longrightarrow \quad \mathcal{O}_L \underset{\Sigma_1\text{-definable}}{\supseteq} \mathbb{Z}. \tag{18}$$

代数的整数からなる環 $\mathbb{A}$

$\mathrm{Th}(\mathbb{A})$ は決定可能である (van den Dries [11], 1988)．したがって $\mathbb{A}$ **で $\mathbb{Z}$ は定義可能ではない**.

$$\mathbb{A} \underset{\text{non-definable}}{\supseteq} \mathbb{Z}. \tag{19}$$

作図可能数

定木とコンパスで作図可能な実数 (constructible number) 全体からなる体で $\mathbb{Z}$ が定義可能かどうかは**未解決である**.

7 その他の話題

- B. Poonen ([6], 2009) において，$\mathbb{Z}$ が $\mathbb{Q}$ において $\forall\exists$(多項式 $= 0$) の形の Π_2-論理式

[*10] 追記：B. Poonen ([6], 2009) により，任意の数体 L で $\mathcal{O}_L$ が定義可能であることが示された.

[*11] 体準同型は必ず単射（つまり埋め込み）なので，“任意の体準同型” と言い換えても同じこと……だと思う.

$$\begin{aligned}\varphi_{\mathrm{int}}^{\mathrm{Poonen}}(v)\colon\quad & (\forall a,b)(\exists x_1,x_2,x_3,x_4,y_2,y_3,y_4)\\ & ((a+x_1^2+x_2^2+x_3^2+x_4^2)(b+x_1^2+x_2^2+x_3^2+x_4^2)\cdot\\ & ((x_1^2-ax_2^2-bx_3^2+abx_4^2-1)^2\\ & +\prod_{n=0}^{2309}((n-v-2x_1)^2-4ay^2-4by_3^2+4aby_4^2-4)^2)=0).\end{aligned}$$

で定義可能であることが示されている．

- J. Koenigsmann ([5], 2016) により大幅に次数が下げられた：

$$\begin{aligned}\varphi_{\mathrm{int}}^{\mathrm{Poonen}'}(v)\colon\quad & (\forall a,b)(\exists x_1,x_2,x_3,x_4,y_2,y_3,y_4)\\ & ((a+x_1^2+x_2^2+x_3^2+x_4^2)(b+x_1^2+x_2^2+x_3^2+x_4^2)\cdot\\ & ((x_1^2-ax_2^2-bx_3^2+abx_4^2-1)^2\\ & +((v-2x_1)^2-4ay_2^2-4by_3^2+4aby_4^2-4)^2)=0).\end{aligned}$$

その上で，何やら難しそうな議論によって内側の $\exists$ を $\forall$ に変換し，Π_1 にすることに成功した．ここに全貌は書けない．

参考文献

[1] Denef, J., and Lipshitz, L., *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc., **18** (2), 385–391, 1978.

[2] Denef, J., *Diophantine sets over some rings of algebraic integers, II*, Trans. Amer. Math. Soc., **257** (1), 227–236, 1978.

[3] Flath, D. and Wagon, S., *How to pick out the integers in the rationals: An application of number theory to logic*, American Mathematical Monthly, **98** (9), 812–823, 1991.

[4] Fraïssé, R., Course of Mathematical Logic, vol. 2, Model Theory, Springer, 1974.

[5] Koenigsmann, J., *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, Annals of Mathematics, 2nd series, **183** (1), 73–93, 2016.

[6] Poonen, B., *Characterizing Integers among Rational Numbers with a Universal-Existential Formula*, American Journal of Mathematics, **131** (3), 675–682.

[7] Robinson, J., *Definability and decision problems in arithmetic*, Journal of Symbolic Logic, **14** (2), 98–114, 1949.

[8] Robinson, J., *The undecidability of algebraic ring and fields*, Proc. Amer. Math. Soc., **10**, 950–957, 1951.

[9] Serre, J.-P., A Course in Arithmetic, Springer, 1973.

[10] Shlapentokh, A., and Shapiro, H.N., *Diophantine relationships between algebraic number fields*, Comm. Pure Appl. Math., **42** (8), 1989

[11] van den Dries, L., *Elimination theory for the ring of algebraic integers*, Journal für die reine und angewandte Mathematik, **388**, 189–205, 1988.

[12] Ziegler, M., *Some undecidable field theories*, 2012.
Available at `http://www.michaelbeeson.com/research/papers/Ziegler.pdf`
[13] 雪江明彦，整数論１：初等整数論から p 進数へ，日本評論社，2013.
[14] **TODO:** 文献追加