A NOTE ON Z AS A DIRECT SUMMAND OF NONSTANDARD MODELS OF WEAK SYSTEMS OF ARITHMETIC

MERLIN CARL

Abstract. There are nonstandard models of normal open induction (NOI) for which \( \mathbb{Z} \) is a direct summand of their additive group. We show that this is impossible for nonstandard models of IE\(_2\).

1. Introduction

It is shown in [Me] that the additive group of a model of true arithmetic cannot have \( \mathbb{Z} \) as a direct summand. On the other hand, various models of arithmetic with quantifier-free induction (open induction, IOpen) and of IOpen with the condition of normality are known whose additive group does have \( \mathbb{Z} \) as a direct summand. We ask how strong an arithmetic theory needs to be to rule out \( \mathbb{Z} \) as a direct summand of the additive group of a model. In this note, we show that IE\(_2\), i.e. arithmetic with induction restricted to formulas with one bounded existential quantifier followed by a bounded universal quantifier and an open formula, suffices.

We start by noting that IOpen does not suffice to rule out \( \mathbb{Z} \) as a direct summand of the additive group of a nonstandard model:

**Theorem 1.** There are nonstandard \( M \) with \( M \models IOpen \) and \( H \subseteq M \) such that \((M,+) = H \oplus \mathbb{Z}\)

**Proof.** The integer parts of real closed fields constructed by Morgnes-Ressayre ([MR]) obviously have \( \mathbb{Z} \) as a direct summand. \( \square \)

We can even demand that these models are normal:

**Theorem 2.** There are nonstandard \( M \) with \( M \models NOI \) and \( H \subseteq M \) such that \((M,+) = H \oplus \mathbb{Z}\).

**Proof.** Applying Proposition 1 of [GA] to \( \mathbb{R}((\mathbb{Q})) \) gives an example. \( \square \)

2. Main Result

We now show that IE\(_2\) suffices to rule out \( \mathbb{Z} \) as a direct summand of the additive group of a nonstandard model.
**Definition 3.** $E_2$ is the class of formulas in the language $L$ of arithmetic of the form $\exists x < t_1 \forall y < t_2 \phi(x, y, z)$, where $t_1$ is a term not containing $x$, $t_2$ is a term not containing $y$ and $\phi$ is an open formula.

$I E_2$ is the axiomatic system consisting of the basic axioms of arithmetic together with induction for $E_2$-formulas.

**Theorem 4.** Let $M \models I E_2$ be nonstandard. Then there is no $H \subset M$ such that $(M, +) = H \oplus \mathbb{Z}$.

We will prove this by three intermediate results. Assume for the rest of this section that $H$ is such a group complement of $\mathbb{Z}$, we work for a contradiction.

**Lemma 5.** Every element $n$ of $H$ is divisible by every standard prime.

*Proof.* Assume wlog that $n > 0$. Let $\mathbb{P}$ denote the standard primes. Suppose for a contradiction that $n \in H$ and $p \in \mathbb{P}$ are such that $p$ does not divide $n$. Then $IE_2$ proves that there is $m$ such that $pm < n < p(m + 1)$, so such an $m$ exists in $M$. Let $m' \in H$ such that $d := m' - m \in \mathbb{Z}$. Then, since $p$ is standard, we must have $pm' \in H$. Hence $pm' - n \in H$ as well. Furthermore, we have $\mathbb{Z} \ni p(m' - m - 1) = pm' - p(m + 1) < pm' - n < pm' - pm = p(m' - m) = pd \in \mathbb{Z}$, so $pm' - n \in \mathbb{Z}$. Therefore, we get $pm' - n \in H \cap \mathbb{Z}$. But $H \cap \mathbb{Z} = \{0\}$, since 0 must be an element of every subgroup and hence a group complement of $\mathbb{Z}$ cannot contain any other element of $\mathbb{Z}$. So we conclude that $pm' - n = 0$, i.e. $n = pm'$, which implies that $n$ is indeed divisible by $p$, a contradiction. \qed

**Corollary 6.** For any $m \in M$, there is $z \in \mathbb{Z}$ such that $m \equiv_p z$ for all standard primes $p$.

*Proof.* Let $m \in M$, so $m$ can be written in the form $h + z$ for some $h \in H$ and some $z \in \mathbb{Z}$. By the last lemma, $h \equiv_p 0$ for all standard primes $p$, hence $m \equiv_p z$ for all standard primes $p$. \qed

**Lemma 7.** In $M$, there is an infinite irreducible $q$ such that $q \equiv 3 \mod 5$.

*Proof.* Consider the formula $A(n) := \exists m, k < 2n \forall a, b < 2n(n < C \land (m > n \land m = 5k + 3 \land (ab = m \rightarrow (a = 1 \lor b = 1)))$. It is obviously $E_2$. $A(n)$ says that, unless $n < C$, there is a prime between $n$ and $2n$ which is congruent to 3 modulo 5. By the well-known asymptotic variant of Dirichlet’s theorem (such as the Siegel-Walfisz-Theorem, see e.g. Satz 3.3.3 on p. 114 of [Br]), the number $\pi(x; 3, 5)$ of primes below $x$ which are congruent to 3 modulo 5 is $\frac{x}{\log(x)}(1 + O\left(\frac{1}{\log(x)}\right))$. It follows that, for sufficiently large $x$, we have $\pi(2x; 3, 5) - \pi(x; 3, 5) > 0$, so there is such a prime between $x$ and $2x$. Let $C$ be large enough that this
holds for $x \geq C$. Then $A(n)$ holds for all standard natural numbers $n$. As $M \models IE_2$, $M$ satisfies $E_2$-overspill. Hence there is a nonstandard element $n'$ of $M$ such that $M \models A(n')$. As $n'$ is infinite, $n' > C$, so there is an irreducible $q$ between $n'$ and $2n'$ leaving residue $3$ modulo $5$, as desired.

**Remark:** This Lemma fails in models of mere IOpen: The methods in [MM] can be used to construct nonstandard models of IOpen in which there are unboundedly many primes, but all nonstandard primes leave residue $1$ modulo $5$.

Now we can prove the theorem: By the corollary, there must be some standard integer $z$ such that $q \equiv_p z$ for all standard primes $p$. As $q$ is irreducible and infinite, $q$ is not divisible by any standard prime. Hence $z$ is not divisible by any standard prime. So $z \in \{-1, 1\}$. But $z \equiv_5 q \equiv_5 3$, hence this is impossible. Contradiction.

An immediate consequence is that the integer parts constructed in [MR] or [GA] can never be models of $IE_2$:

**Corollary 8.** Let $K$ be a non-archimedean real closed field, and let $Z$ be an integer part of $K$ generated by one of the constructions described in [MR] or [GA]. Then $(Z^{\geq 0}, +, \cdot) \nmid IE_2$.

**Proof.** All of these IP’s have $Z$ as a direct summand. □

By a well-known result of V. Pratt, primality testing is in NP. Therefore, there is a $\Sigma^b_1$-definition of primality, where a $\Sigma^b_1$-formula is a formula starting with one bounded existential quantifier followed by logarithmically bounded quantifiers (see e.g. [HP]). Hence, we can reformulate our $A(n)$ as a $\Sigma^b_1$-formula, which gives us the following result:

**Corollary 9.** If $M \models IS_1^b$ is nonstandard, then $Z$ is not a direct summand of $(M, +)$.

**Question:** The obvious next question is now whether $IE_1$ is already sufficient to exclude $Z$ as a direct summand of a nonstandard model. (This would, in particular, follow if $IE_1 = IE_2$, which is still wide open.) It would also follow if there was an $E_1$-definition of primality. Thus, in particular, it is a consequence of bounded Hilbert’s 10th problem stating that every NP predicate is expressible by a bounded diophantine equation.

3. Generalization

Instead of $Z$, we can consider other initial segments. It turns out that our arguments above allow two immediate generalizations.
Theorem 10. (i) Let $M \models I \Delta_0 + EXP$ and let $N$ be a cut of $M$ (i.e. a proper initial segment closed under the successor function). Then there is no $H \subseteq M$ such that $(M,+) = H \oplus N$.

(ii) Let $M \models IE_2$ and let $N$ be an initial segment of $M$. Then there is no $H \subseteq M$ such that $(M,+) = H \oplus N$.

Proof. (i) Assume otherwise, and define functions $\rho_1 : M \to H$ and $\rho_2 : M \to N$ by $x = \rho_1(x) + \rho_2(x)$ for all $x \in M$. Then $\rho_2$ is a ring homomorphism from $M$ to $N$. (In particular, on sees that $N$ must be closed under addition and multiplication and hence in fact be a model of $I \Delta_0$.) Now we can use the strategy of [Mc]: $I \Delta_0 + EXP$ proves that every positive number is the sum of four squares. Therefore, if $m_1 < m_2$ are elements of $M$, then there are $x_1, x_2, x_3, x_4$ in $M$ such that $m_2 - m_1 = x_1^2 + x_2^2 + x_3^2 + x_4^2$ and thus $\rho_2(m_2) - \rho_2(m_1) = \rho_2(m_2 - m_1) = \rho_2(x_1)^2 + \rho_2(x_2)^2 + \rho_2(x_3)^2 + \rho_2(x_4)^2 > 0$, so $\rho_2(m_2) > \rho_2(m_1)$. Hence $\rho_2$ preserves the ordering $M$. But, unless $H = \{0\}$ (and hence $N$ is not a proper initial segment), there are $m_1, m_2 \in M$ with $\rho_2(m_1) = \rho_2(m_2)$, a contradiction.

(ii) Here, we re-use our argument from above: If such $H$ existed, then every element of $H$ would be divisible by every element of $M$. Therefore, for any $m \in M$, there would be $n \in N$ such that $m \equiv_k n$ for all $k \in M$. But, as $PA$ proves the Dirichlet theorem used above, it follows by $IE_2$-overspill that $M$ contains an irreducible element $a$ such that $a \equiv_5 2$ and hence $a$ is not congruent to any element of $N$ modulo all elements of $M$, a contradiction. □

Remark: In (i), $I \Delta_0 + EXP$ can be replaced by the weaker system $I \Delta_0 + \Omega_1$, which is sufficient to prove Lagrange’s theorem. In (ii), $PA$ can be replaced with any fragment of arithmetic strong enough to prove the asymptotic version of Dirichlet’s theorem.

References

[Br] J. Brüdern. Einführung in die analytische Zahlentheorie. Springer Verlag Berlin Heidelberg (1995)

[CDK] M. Carl, P. D’Aquino and S. Kuhlmann. Real Closed Exponential Fields and Models of Peano Arithmetic. To appear in Forum Mathematicum.

[GA] G. Asatryan. On Ordered Fields with Infinitely Many Integer Parts. Preprint 2008.

[HP] P. Hajek and P. Pudlak. Metamathematics of First-Order Arithmetic. Perspectives in Mathematical Logic, Springer-Verlag, (1998).

[MM] D. Marker, A. Macintyre. Primes and their Residue Rings in Models of Open Induction. Annals of Pure and Applied Logic 43 (1989), pp 57-77

[MR] Mourgues and Ressayre. Every Real Closed Field has an Integer Part. J. Symbolic Logic, Vol. 58, No. 2 (1993), pp. 641-647

[W] Wilmers. Bounded Existential Induction. J. Symbolic Logic ,Vol. 50, No 1 (1985), pp. 72-90
A NOTE ON Z AS A DIRECT SUMMAND OF NONSTANDARD MODELS OF WEAK SYSTEMS OF ARITHMETIC

[Me] E. Mendelson. On non-standard Models for Number Theory. Fraenkel anniversary volume, Magnes Press (1961), 259 - 268.