ON SURREAL NUMBERS AND THEIR NUMBER THEORY: AN INTRODUCTION TO THE OMNIFIC INTEGERS

SIDDHARTH KOTHARI

Abstract.

1. Introduction to the Characters

Definition 1.1 (Omnific integer)**.** A surreal number x is said to be an *omnific integer* if $x = \{x-1 \mid x+1\}$.

One of the reasons that this is a *good definition* is that all of the regular integers are omnific integers as well, and none of the other *real numbers* (elements of the set $\mathbb{R}/\mathbb{Z}$) are omnific integers, as one would expect. This can be shown by invoking the *simplicity theorem* (see the appendix for the more on these results regarding the surreal numbers).

We have the following basic result.

Proposition 1.2. *The sum and product of two omnific integers is an omnific integer. Thus, the omnific integers from a sub-ring of* **No***, commonly denoted by* **Oz***.*

Proof. Let $x = \{x-1 \mid x+1\}$ and $y = \{y-1 \mid y+1\}$ be omnific integers. Then by the definition of surreal addition, we have

$$x + y = \{x+y-1, x-1+y \mid x+1+y, x+y+1\} = \{x+y-1 \mid x+y+1\},$$

which shows that $x+y$ is an omnific integer. Next, by the definition of surreal multiplication, we have

$$(xy)^L = \{(x-1)y + x(y-1) - (x-1)(y-1), (x+1)y + x(y+1)\} = \{xy-1\},$$

and

$$(xy)^R = \{(x-1)y + x(y+1) - (x-1)(y+1), x(y-1) + (x+1)y - (x+1)(y-1)\} = \{xy+1\}.$$

Putting the two together we get $xy = \{xy-1 \mid xy+1\}$, which is what we wanted to show. ∎

Again, this matches up with our previous experience: the sum and product of two elements of $\mathbb{Z}$ is again an element of $\mathbb{Z}$ (this is summarized by saying that $(\mathbb{Z}, +, \cdot)$ is a ring).

Consider $\omega = \{0, 1, 2, \cdots \mid \varnothing\}$. By the simplicity theorem $\{\omega - 1 \mid \omega + 1\} = \omega$, since we clearly have $\omega - 1 < \omega < \omega + 1$, and $n < \omega - 1$ for all $n \in \mathbb{Z}^+ \cup \{0\}$ (these are all the options of ω). Thus ω, the least limit ordinal, is also an omnific integer. This should make sense, given that ordinals enumerate sets (albeit infinite ones). More generally, we have the following.

Proposition 1.3. *Let $\alpha \in$* **No** *be an ordinal number. Then α is also an omnific integer.*

Before proving this, it will be helpful to review the notion of an ordinal in the surreal number sense.

Definition 1.4 (Ordinal number)**.** Let x be a surreal number. Then x is said to be an *ordinal number* if it is possible to write $x = \{x^L \mid \varnothing\}$ where x^L is a set of surreal numbers.

Remark 1.5. Throughout this article, we will use the Greek letters $(\alpha, \beta, \gamma, \cdots)$ to denote an ordinal.

Date: 17 November 2024.

Recall that the surreal version of an ordinal number is a surreal number of the from $\alpha = \{x \mid \varnothing\}$, for some set x of surreal numbers. Furthermore, it can be shown that x is the set of ordinal numbers strictly less than α. In the sections to come, we will zoom out a bit to survey the adjoining landscape, as it turns out that several facts (for example, why have we defined **Oz** the way we have?) that *seem* native to the omnific integers actually aren't: there's a more general algebraic framework clunking in the background. Further, we are also interested in the distribution of the irreducible and prime elements in **Oz**. First, recall these notions are defined in the general setting of a ring.

Definition 1.6 (Irreducible and Prime Element)**.** Let R be a ring. Then we have the following.

- A $r \in R$ is said to be an *irreducible* if $r \notin R^\times$ and whenever $r = ab$ for some $a, b \in R$, we have $a \in R^\times$ or $b \in R^\times$. That is, every factorization of r in R involves a unit.
- A $p \in R$ is said to be a *prime element* if whenever $p = ab$ for some $a, b \in R$, we have p divides a or p divides b.

As a matter of fact, this question has not been completely solved for $\mathbb{Z}$ as well. Indeed, that is the content of the celebrated million-dollar Riemann hypothesis!

2. Real Closed Fields and Integer Parts

First, we state some preliminary definitions that will make communication easier.

Definition 2.1 (Ordered field)**.** Let R be a ring and $\leq$ a total ordering on R. Then the ordered pair $(R, \leq)$ is said to be an *ordered ring* if the following two conditions hold for all $a, b, c \in R$:

- $a \leq b \implies a + c \leq b + c$ and,
- $0 \leq a$ and $0 \leq b$ imply that $0 \leq ab$.

A field F with a total ordering $\leq$ is said to be an *ordered field* if the underlying ring is an ordered ring with respect to $\leq$.

Definition 2.2 (Real closed field)**.** Let $(F, \leq)$ be a ordered field. Then F is said to be a *real closed field* if the following two conditions hold.

- For all $x \in F$ such that $x \geq 0$, the square root of x in F exists.
- Any odd-degree polynomial with coefficients in F has at least one root in F.

Remark 2.3. In fact, the following conditions are all equivalent to the definition of a real closed field as stated above. Notice how much they remind one about $\mathbb{R}$, the field of the real numbers!

- F is not algebraically closed, but the field extension $F(\sqrt{-1})$ is algebraically closed.
- F is not algebraically closed, but its algebraic closure is a finite field extension of F.

On the whole, real closed fields are quite exotic. The algebraic numbers over $\mathbb{R}$, the hyperreal numbers, superreal numbers are all real closed. In fact, even the surreal numbers **No** from a real closed field (whose domain is a class), as the following proposition tells us.

Proposition 2.4. *The field of the surreal numbers forms a real closed field.*

We defer the proof for the appendix, as it requires a bit more machinery.

The significance of a real closed field lies in its ability to *model* the behavior of real numbers while extending these properties to a broader set of numbers, such as those found in algebraic structures like the surreal numbers. The fact that the surreal numbers form a real closed field is important because it ensures that surreal numbers share many of the essential characteristics of real numbers, including the ability to solve certain polynomial equations and the existence of square roots for positive elements. In fact, a field being real closed also means that the field is *elementarily equivalent* to as the real numbers. That is, no matter what statement you write (about one of them, using their properties), both fields will *either both make the statement true or both make the statement false.*

One of the key observations about the structure of $\mathbb{Z}$ in $\mathbb{R}$ is that an arbitrarily real number always lies trapped 'between' two integers. More precisely, given any $r \in \mathbb{R}$, it is possible to find unique $n \in \mathbb{Z}$ such that $n \leq r < n+1$. In this case, $n = \lfloor r \rfloor$. The next definition formalizes this intuitive idea.

Definition 2.5 (Integer part)**.** Let $(K, \leq)$ be an ordered field and let $(Z, \leq) \subseteq (K, \leq)$. Then Z is called an *integer part* of K if the following properties are satisfied.

- It is a discretely ordered ring.
- 1 is the minimal positive element in Z.
- For any $x \in K$ there exists an unique $z \in Z$ such that $z \leq a < a+1$. We call z the integer part of a under Z and write $\lfloor a \rfloor$.

Remark 2.6. A discretely ordered ring $(R, \leq)$ is a ring with no element between 0 and 1 ($\nexists x \in R : 0 \leq x \leq 1$ and $x \notin \{0, 1\}$).

The next result explains, once and for all, why **Oz** is the analogue for $\mathbb{Z}$ in **No**.

Proposition 2.7. *The subring* **Oz** *is an integer part of* **No** *in the sense of the previous definition.*

Proof. ■

We can also approach this a bit more generally: we can combine the fact that **No** forms a real-closed field and the following result, which exemplifies the similarity between a real closed field and $\mathbb{R}$.

Theorem 2.8. *Every real closed field admits an integer part.*

A result that will be useful for us in the next section is the following.

Proposition 2.9. *An ordered field is Archimedean if and only if $\mathbb{Z}$ is the unique integer part.*

3. Generalized Power Series: Hahn Series

3.1. **What is a Hahn Series? First Examples and Basic Notions.** Roughly speaking, the notion of a *Hahn series* generalizes the idea of a Taylor series form calculus: the exponents (that the intermediate is raised to) don't have to be integers. Indeed, we allow the exponents to be from *any* group, often called the *value group*. Essentially then, such a power series (just like a Taylor series), is a function from the value group to a *particular field* (where the coefficients lie): the intermediate sitting there doesn't make such a difference! The only condition that must be satisfied is that the formal sum must 'start somewhere'. That is, we should be able to *bound* the elements in the group that get sent to a non-zero coefficient from below.

But how does this relate back to the surreal numbers? We get a hint from one of the key results from Conway's book, *On Numbers and Games*, which introduced the the surreal numbers.

Theorem 3.1. *Let We can express each surreal number x uniquely in the form*

$$x = \sum_{\beta < \alpha} \omega^{y_\beta} \times r_\beta$$

where α is some ordinal and the numbers r_β are non-zero real numbers, and the y_β's are a strictly decreasing sequence of surreal numbers.

Remark 3.2. Thus, **No** contains numbers like $1 + \sum_{n<\omega} \omega^{\frac{1}{n+1}}$ and also $\sum_{n<\omega} \omega^{\frac{1}{\omega(n+1)}}$.

More concretely, we will express **No** as a Hahn series ring (in fact, we will justify this is actually a field). Then, we will go through results that deal with integer parts of such fields and the existence and distribution of irreducible elements *in this generalized context*, before translating them back to the omnific integers. But we're getting ahead of ourselves: recall that we still need to modify the exponent group so that elements can be compared. To this end, we define a *totally ordered group*.

Definition 3.3 (Totally ordered group)**.** Let $(G, \cdot)$ be a group. Then we say that G is a *left ordered group* (resp. *right ordered group*) if there exists a total order $\leq$ on G such that $g_1 \leq g_2 \implies h \cdot g_1 \leq h \cdot g_2$ for all $g_1, g_2, h \in G$ (resp. $g_1 \leq g_2 \implies g_1 h \leq g_2 h$ for all $g_1, g_2, h \in G$). When both the notions coincide (which always happens when G is an abelian group), we simply say that G is *totally ordered group*.

Remark 3.4. If $\leq$ satisfies the property $g_1 \leq g_2 \implies h \cdot g_1 \leq h \cdot g_2$ for all $g_1, g_2, h \in G$, we say that $\leq$ is *translation invariant*. This is modeled on the fact that $a \leq b \implies c + a \leq c + b$ for $a, b, c \in \mathbb{R}$.

Remark 3.5. We will write $(G, \cdot, \leq)$ for a totally ordered group, where G is the underlying set, $\cdot$ is the group operation and $\leq$ is the translation invariant total order on G.

Example. Most of the groups you would've seen are totally ordered: the reals $(\mathbb{R}, +)$, the rationals $(\mathbb{Q}, +)$ and the integers $(\mathbb{Z}, +)$ are all totally ordered by the usual order $\leq$. Even some of the more exotic groups can be endowed with this additional structure—take $\mathbf{GL}_n(\mathbb{R})$ for instance. Define $A \leq B \iff |\det A| \leq |\det B|$ for all $A, B \in \mathbf{GL}_n(\mathbb{R})$. Clearly any two matrices can be compared, since any two non-negative real numbers can be compared, so the order is total. Further, note that if $A \leq B \implies |\det A| \leq |\det B| \implies |\det C| \cdot |\det A| \leq |\det C| \cdot |\det B| \implies |\det(CA)| \leq |\det(CB)| \implies CA \leq CB$ for any $C \in \mathbf{GL}_n(\mathbb{R})$. Thus, this total order respects the group structure as well. In fact, we can put such a relation on the symmetric groups S_n by means of the matrix representation for S_n.

Now we are ready to introduce the key notion that will allow us to revisit the surreal numbers from a different perspective.

Definition 3.6 (Generalized power series)**.** Let $(G, \cdot, \leq)$ be a ordered group and K a field. For a function $s : G \to K$, define the support $\operatorname{supp}(s)$ to be the set

$$\operatorname{supp}(s) = \{g \in G : s(g) \neq 0\}.$$

A *generalized power series with coefficients in K and exponents in G* is any function $s : K \to G$ such that $\operatorname{supp}(s) \subseteq G$ is well-ordered with respect to $\leq$. The set of all such functions is denoted by $K((G))$.

Remark 3.7. We usually (and will!) write a $s \in K((G))$ as the *formal sum*

$$s = \sum_{g \in G} s_g x^g,$$

where s_g denotes the image of g under s, and x can be viewed as an intermediate or a as an *indicator function* $x : G \to \{0, 1\}$, sending everything except g to 0, and g to 1.

Remark 3.8. We use $K((G^{<0}))$ and $K((G^{>0}))$ to denote the set of generalized power series with negative and positive exponents respectively. In general, for a subset S of G, we write $K((S))$ to denote elements of $K((G))$ with support contained in S.

Exercise. Show that $K((S))$ as defined above has the algebraic structure of a $K-$vector space for all $S \subseteq G$.

Example. Let $G = \mathbb{Z}$, the additive group of integers, and $K = \mathbb{C}$, the field of complex numbers. What does $\mathbb{C}((\mathbb{Z}))$ look like? It consists of a whole zoo of creatures, so lets take it apart slowly, unboxing a piece at a time.

First, it contains *finite elements*. These include what we call *polynomials* like $2x + (4 + i\sqrt{3})x^2 + ix^{10}$ and $ei + (29 - 5i)x^{2000}$, but also more exquisite objects which include the intermediate x raised to a negative exponent such as $\frac{1}{x}$ and $\frac{i}{x^2} + i\sqrt{5}\frac{1}{x^{49}} + (3 + 4i)x^5$. Note also $\mathbb{C} \subset \mathbb{C}((\mathbb{Z}))$. One can describe the set of all polynomials over $\mathbb{C}$ with degree at most n by $K((\{0, 1, \cdots, n\}))$.

Next, we have the *Taylor series* of various functions. For example, $1+x+\frac{1}{2}x^2+\frac{1}{6}x^3+\cdots \in \mathbb{C}((\mathbb{Z}))$ is just the familiar Taylor expansion for $f : \mathbb{C} \to \mathbb{C}$ defined by $f(z) = e^z$ at $z = 0$. Observe that $s_g = \frac{1}{n!}$ for $g \in \mathbb{Z}^+ \cup \{0\}$ and $s_g = 0$ for $g \in \mathbb{Z}^-$. The set of the Taylor series are contained in $\mathbb{C}((\mathbb{Z}^+ \cup \{0\}))$.

Remark 3.9. We can remodel this notation just a bit more. Since for any $s \in K((G))$ the set $\text{supp}(s)$ is well-ordered, we know it must be (order) isomorphic[1] to a unique ordinal number, say α, which is called the *order type* of s. Thus, we may write

$$s = \sum_{\beta<\alpha} s_\beta x^{g_\beta}$$

for some enumeration $\{g_\beta : \beta < \alpha\}$ of $\text{supp}(s)$ (that is, we are associating each member of $\text{supp}(s)$ to a member of α, which is an ordinal less than α) and $s_\beta := s_{g_\beta}$. This may remind you of the Cantor or even of the Conway normal form!

It is possible to endow $K((G))$ with a ring structure, with addition defined by

$$\left(\sum_{g\in G} a_g x^g\right) + \left(\sum_{g\in G} b_g x^g\right) := \sum_{g\in G}(a_g + b_g)x^g,$$

and multiplication defined by (you can convince yourself that this is essentially modeled of the distributive property)

$$\left(\sum_{g\in G} a_g x^g\right) \cdot \left(\sum_{h\in G} b_h x^h\right) := \sum_{g\in G}\sum_{h\in G} a_g b_h x^{g+h} = \sum_{n\in G}\sum_{i+j=n} a_i b_j x^n = \sum_{n\in G} s_n x^n,$$

where

$$s_n = \sum_{\substack{(i,j)\in \text{supp}(a)\times\text{supp}(b)\\ i+j=n}} a_i b_j x^n$$

for all $n \in G$. Notice the similarity with the operations defined on the group algebra $K[G]$! This should not come as a surprise, since $K[G]$ is essentially the $s \in K((G))$ that have finite (as opposed to just well-ordered) support[2].

Remark 3.10. To be strict, we must check that the multiplication we defined above is indeed well-defined: the sum defining ab is finite and $\text{supp}(ab)$ is well ordered (and hence $ab \in K((G))$). For the sake of contradiction, assume that there were infinitely many pairs $(i, j) \in \text{supp}(a) \times \text{supp}(b)$. Without loss of generality, assume that there are infinitely many distinct i's. That is, we can find a sequence $i_1 < i_2 < \cdots$ (such that $\exists s : i_k + s = g$). Then, there is a corresponding infinite descending chain in $\text{supp}(b)$: $j_1 > j_2 > \cdots$ where $j_k = g - i_k$ for all k. This contradicts the fact that $\text{supp}(b)$ is well-ordered. Thus, $|\{(i, j) \in \text{supp}(a) \times \text{supp}(b) : i + j = g\}|$ is finite for all $g \in G$.

Further, assume that there exists a infinite descending sequence $c_1 > c_2 > \cdots$ in $\text{supp}(ab)$. The, to each c_k we associate the finite set $S_=\{(i, j) \in \text{supp}(a) \times \text{supp}(b) : i + j = c_k\}$. Let $(x_k, y_k) \in S_k$ be such that x_k is minimal. Next,

As promised, we upgrade $K((G))$ to the elite status of a field [3].

Proposition 3.11. *A Hahn series ring $K((G))$ is a field.*

[1]Two partially ordered sets $(A, \leq_A)$ and $(B, \leq_B)$ are said to be *order isomorphic* if there is a bijection $f : A \to B$ such that $x \leq_A y \iff f(x) \leq_B f(y)$ for all $x, y \in A$ (that is, f is order preserving).

[2]Phrased differently, the support is isomorphic to a unique ordinal number less than ω.

[3]We'll take this moment to introduce the more general notion of a *Hahn field*: a field F such that $K[G] \subseteq F \subseteq K((G))$. In this context, $K[G]$ and $K((G))$ are the edges of the spectrum.

For the proof, see the appendix. Further, we define the order $\leq$ on $K((G))$ y $0 \leq x \iff s_{\min \operatorname{supp}(x)} \geq 0$ for all $x = \sum_{g \in G} s_g x^g \in K((G))$.

Exercise. Check that the order $\leq$ as defined above makes $K((G))$ into a ordered field.

The notions that we've introduced so far are of no use to us in the context of the surreal numbers since the underlying domain there is a proper class and not a set.

Definition 3.12. Let $\mathbf{K}$ denoted a field whose underlying domain is a class (an example would be $\mathbf{K} = \mathbf{On}$) and G be a totally ordered group (whose domain is a set). Define $\mathbf{K}((G))$ to be the class $\bigcup_K K((G))$, where K ranges over all the subfield of $\mathbf{K}$ that are sets.

3.2. **Basic Results.**

Theorem 3.13. *Let K be a field and G a totally ordered abelian group. Then $K((G))$ is algebraically closed if and only if K is algebraically closed and G is divisible.*

Proof. ■

Corollary 3.14.

We can even define a valuation on $K((G))$, as the following proposition shows.

Proposition 3.15. *For a $s \in K((G))$, define $v(s)$ to be* $\min$ *supp*(s) *if $s \neq 0$ and ∞ if $s = 0$. Then v is a valuation.*

Proof. • We must show that $v(ab) = v(a) + v(b)$ for all $a, b \in K((G))$. By the way how multiplication is defined, we have that $\operatorname{supp}(ab) = \{i + j : i \in \operatorname{supp}(a) \text{ and } j \in \operatorname{supp}(b)\} \subseteq G$. Clearly, if we want to minimize $i + j$, we will minimize i and j individually, so $v(ab) = \min \operatorname{sup}(ab) = \min \operatorname{sup}(a) + \min \operatorname{sup}(b) = v(a) + v(b)$.

■

Proposition 3.16. *The invertible elements of $K((G^{\leq 0}))$ are precisely the non-zero elements.*

Proof. Let $a \in K((G^{\leq 0}))$ be invertible. That is, there exists a $b \in K((G^{\leq 0}))$ such that $ab = 1$. Thus, $v(ab) = v(a) + v(b) = v(1) = 0 \implies v(a) + v(b) = 0$. Note the $G^{\leq 0}$, which means that $(a), v(b) \leq 0$. Thus, $v(a) = 0 = v(b)$. This implies that $a = a_0 t^0$ and $= b_0 t^0$ where $a_0, b_0 \in K$ are non-zero (otherwise their valuation would be ∞). ■

Proposition 3.17. *The field $K((G))$ is non-archimedean.*

Proof. ■

Corollary 3.18. *$K((G))$ does not have a unique integer part.*

Proposition 3.19. *Let Z be an integer part for a real ordered field K. Then $Z + K((G^{<0}))$ is an integer part for $K((G))$.*

4. Appendix

4.1. **Abstract Algebra Definitions.** A divisible group G is s group that can be 'divided' by the integers (to as fine of a degree you want!). That is, each element of G is a n^{th} multiple of some other element for each n.

Definition 4.1 (Divisble group)**.** An abelian group $(G, +)$ is said to be divisible if for any positive integer n and $g \in G$, there exists a $y \in G$ such that $ny = g$.

Definition 4.2. Let R be a ring. Then we have the following.

- R is an *unique factorization domain* if it is an integral domain and every non-zero and non-unit element can be expressed as the product irreducible elements of R, that is unique up to the ordering of the irreducibles.
- R is an *integrally closed domain* if the integral closure of R is the field of fractions of R.

Example. The ring of integers, $\mathbb{Z}$, is an integral domain, since

Definition 4.3. A integrally closed domain R is said to be a *Shcreier domain* if every non-zero element of $r \in R$ is primal, that is, if r divides ab, then $r = r_a r_b$ where r_a is such that r_a divides a and r_b divides b.

Definition 4.4. Let K be a field and Γ be a totally ordered abelian group. Before we state the actual definition, we extend the group law and ordering on Γ to $\Gamma \cup \{\infty\}$ by setting :

- $a < \infty$ for all $a \in \Gamma$ and,
- $a + \infty = \infty = \infty + a$ for all $a \in \Gamma$.

A *valuation* v on K is a map $v : K \to \Gamma \cup \{\infty\}$ that satisfies the following properties for all $a, b \in K$.

- $v(a) = \infty \iff a = 0$.
- $v(ab) = v(a) + v(b)$.
- $v(a + b) \geq \min\{v(a), v(b)\}$ with equality if and only if $v(a) \neq v(b)$.

A field with a valuation is called a *valued field*. The valuation ring R_v is the set of $v(a)$ for $a \in K$ such that $v(a) \geq 0$.

Example. The canonical example of a valuation is the $p-$*adic valuation*, which is extremely popular due to its intimate connection with the eccentric $p-$adic numbers.

More precisely, let $K = \mathbb{Q}$, the rational numbers, and $\Gamma = \mathbb{Z}$, the additive group of the integers. Fix a prime $p \in \mathbb{Z}^+$. Then the $p-$adic valuation, denoted by v_p, is defined by $v_p(n) = \max\{e \in \mathbb{Z} : p^e | n\}$ for all $n \in \mathbb{Z}$. We extend this definition to *all rationals* by setting $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$ for all $a, b \in \mathbb{Z}$ with $b \neq 0$. As exercise, show that this is indeed a valuation! Also, note that it actually makes sense (at least in this context) to set $v_p(0) = \infty$, since any integer divides 0.

Definition 4.5. Let K be an ordered field. We say that F satisfies the *Archimedean property* if for all $x, y \in K$, we have that there exists a natural number n such that $nx > y$. Here, $n \in F$ denotes the field element 1 summed with itself n times.