The Radicans

James B. Wilson

April 13, 2002

1 Radices of Integers

Computational mathematics has brought awareness to the use of various bases in representing integers. The standard for most number systems is decimal, which is base 10, or has radix 10.[1] Common examples inclue the radix for: binary, 2; octal, 8; and hexidecimal, 16.

Definition 1.1 *A positive integer r is a radix. A sequence $\alpha = (a_k, \ldots, a_0)$ is a radix r sequence if $0 \leq a_i < r$ when $r > 1$ and $a_i = 1$ if $r = 1$, for all $i = 1, \ldots, k$. The set of all radix r sequences of integers is defined as $\mathbb{N}_{\lrcorner r}$ and is called a* primitive radican *of r.* [2]

The translation of a positive integer to a specific radix in computer science can be done recursively as follows:

$$a_i = \left\lfloor (n - \sum_{j=i+1}^{k} a_j)/r^i \right\rfloor,$$

where $k = \lfloor log_r n \rfloor$. This method ensures the proper allocation of space and takes advantage of the implicit flooring done with integer division in computers. However this recursion runs backwards and so is potentially confussing.[3]

The following direct and more number theoretic recursion offers a greater insight into the mechinisms behind a radix.

$$a_j r^j \equiv n - \sum_{i=0}^{j-1} a_i r^i \pmod{r^{j+1}}$$

where each a_j is restricted to the least residue class. Notice $n = m \cdot r^j + \sum_{i=0}^{j-1} a_i r^i$ and $(r^j, r^{j+1}) = r^j$ so the explicit form can be given through cancelation as $a_j \equiv m \pmod{r}$.

[1] The use of the term *base* is more common than *radix*. However due to the use of the the terms basis and bases later, *base* will be avoided in favor of *radix*.

[2] The set $\mathbb{N}$ includes 0.

[3] Running backwards allows for a program to convert the radix to a reduced precision thus is ideal for floating point situations as well.

The process terminates when $\sum_{i=0}^{j} a_i r^i = n$, which it must at some point. Regardless of the algorithm used, the output is well-defined and unique and is denoted as ${}^{n}\llcorner_r$. Note the length of ${}^{n}\llcorner_r$ is always $\lceil log_r n \rceil$ and 1 when $n = 0$.

Definition 1.2 *An non-negative integer n is said to be* expressed (in the radix r) *by ${}^{n}\llcorner_r = (a_k, \ldots, a_0)$ if for all $i = 1, \ldots, k$, $0 \leq a_i < r$ when $r > 1$ and $a_i = 1$ when $r = 1$ (called a* tally*).*

Proposition 1.3 *The map $(r) : {}^{\mathbb{N}}\llcorner_r \to \mathbb{N}$, defined as $\alpha(r) = a_k r^k + \cdots + a_1 r + a_0$, is well-defined. Furthermore ${}^{\circ}\llcorner_r : \mathbb{N} \to {}^{\mathbb{N}}\llcorner_r$ defined by ${}^{n}\llcorner_r = (a_k, \ldots, a_0)$ is the inverse map of (r), so ${}^{n}\llcorner_r(r) = n$ and ${}^{\alpha(r)}\llcorner_r = \alpha$.* [4]

Typcially the sequence is denoted with the most significant figures to the left and the least significant to the right, just as with decimal notation. The individual coefficients a_i are called *r-dits*, or simply *radits* when r is clear from the context.

Definition 1.4 *Given a set $A \subseteq \mathbb{N}$, define ${}^{A}\llcorner_r = \{{}^{n}\llcorner_r \mid n \in A\}$. Also define ${}^{n}\llcorner_\infty = n$ so that ${}^{A}\llcorner_\infty = A$ and in particlar ${}^{\mathbb{N}}\llcorner_\infty = \mathbb{N}$.*

Before moving on it is important to note several techniques exist to extend the radix representation of a positive integer to its negative: simply fix a new symbol (the minus sign) in front of the number, or for the case of more complex systems, such as the p-adic integers, use infinite sequences. Most of these methods can be extended to the following construction but for simplicity negative integers are ignored.

2 Radix Algorithm

The construction of a radix makes sense to other number systems as well. But as with other principles, the development of radix does not in general follow the integer model. The restrictions that make an integer like radix to exist are considered but the certain useful results can be derived even with radix representations that do not exhibit all the necessary properties.

Lemma 2.1 *Given a right $\mathbb{Z}$-module M and a submodule S, and an integer $r \neq 0$, $a \equiv b \pmod{S}$ if and only if $ar^i \equiv br^i \pmod{Sr^i}$ for all $i \geq 0$.*

Proof: $a + S = b + S$ if and only if $(a + S)r^i = (b + S)r^i$. Furthermore $(x + S)r^i = \{(x + s)r^i \mid s \in S\} = \{xr^i + sr^i \mid s \in S\} = xr^i + Sr^i$. Therefore $a + S = b + S$ if and only if $ar^i + Sr^i = br^i + Sr^i$. $\square$

[4] The notation mimicks the equation $a/b \cdot b = a$ as a mnemonic.

Theorem 2.2 (Radix Algorithm) *Let M be a right $\mathbb{Z}$-module and S a submodule of M with transversal $Tr(S)$ and of finite index r. For every element $a \in M$ there exists a unique sequence ${}^{a}\lrcorner_{S} = \{a_i | i \in \mathbb{N}, a_i \in Tr(S)\}$ such that*

$$a \equiv \sum_{i=0}^{j} a_i r^i \pmod{Sr^j} \tag{1}$$

for all $j \in \mathbb{N}$.

Proof: Proceed with induction. Given an element $a \in M$ there exists a unique $a_0 \in T$ such that $a + S = a_0 + S$ by the definition of T, thus verifying $a \equiv a_0 \pmod{Sr^0}$. Presume the subsequence $a_0, \ldots, a_j$ satisfies Equation (1), which requires $a - \sum_{i=0}^{j} a_i r^i \in Sr^j$. Thus there exists an $s \in S$ such that $a - \sum_{i=0}^{j} a_i r^i = sr^j$. However clearly the order of sr^j in M/Sr^{j+1} divides r. Therefore there exists a $t \in M$ such that $s \equiv tr \pmod{Sr}$.

Once again there exists a unique $a_{j+1} \in Tr(S)$ such that $a_{j+1} \equiv t \pmod{S}$. Applying Lemma-2.1 and substituting yields

$$a_{j+1} r^{j+1} \equiv tr^{j+1} = sr^j = a - \sum_{i=0}^{j} a_i r^i \pmod{Sr^{j+1}}.$$

Therefore ${}^{a}\lrcorner_{S}$ is uniquely defined. $\square$

Proposition 2.3 *If an element is expressible then its expression is unique.*

Proof: Suppose a is expressed by $(a_i)_{i\in\mathbb{N}}$ and $(b_i)_{i\in\mathbb{N}}$. The transitivity of mod equivalence infers $\sum_{i=0}^{j} a_i r^i \equiv \sum_{i=0}^{j} b_i r^i \pmod{Sr^j}$. If $j = 0$ clearly $a_0 \equiv b_0 \pmod{S}$ and since both are in the transversal it follows $a_0 = b_0$. Proceeding with induction, assume $a_i = b_i$ for all $i \leq j$ for some non-negative integer j. Canceling the common sum leaves $a_{j+1} r^{j+1} \equiv b_{j+1} r^{j+1} \pmod{Sr^{j+1}}$, and applying Lemma-2.1 reduces the expression to $a_{j+1} \equiv b_{j+1} \pmod{S}$. By the same argument as above $a_{j+1} = b_{j+1}$, so in fact $(a_i)_{i\in\mathbb{N}} = (b_i)_{i\in\mathbb{N}}$. $\square$

When context allows, we write ${}^{a}\lrcorner_{S}$ as ${}^{a}\lrcorner_{r}$ and ${}^{M}\lrcorner_{S}$ as ${}^{M}\lrcorner_{r}$ since the integer radix is generally of greatest interest. Traditionally the sequence derived from the radix algorithm is written from left to write starting with the most significant radit. Some confussion may arrise of the radix algorithm is not used to compute the sequence.

Example 2.4 *In the ring $\mathbb{Z}/4$, $0 = 1 \cdot 4$. Therefore $0 = 1 \cdot 2^2 + 0 \cdot 2 + 0 \cdot 1$. However ${}^{0}\lrcorner_{2} \neq (1, 0, 0)$ because*

$$1 \cdot 2^2 = 4 \not\equiv 0 - (0 \cdot 2 + 0 \cdot 1) \pmod{2^3}.$$

Example 2.5 *Consider the radix algorithum with the chain* $0 \trianglelefteq \mathbb{Z}/r \times 0 \trianglelefteq \mathbb{Z}/r \times \mathbb{Z}/r$ *where* $r > 1$. *The element* $(1,0) \equiv (0,0) \pmod{\mathbb{Z}/r \times 0}$ *so* $a_0 = 0$. *Next* $(1,0) \equiv a_1 r + 0 = a_1 r \pmod 0$. *Therefore* $(1,0) = a_1 r$ *yet every element of* $x \in \mathbb{Z}/r \times \mathbb{Z}/r$ *has order dividing* r *so* $(1,0) \neq a_1 r$ *for any* a_1 *in any transversal. Therefore* $\mathbb{Z}/r \times \mathbb{Z}/r$ *is not expressible.*

Proposition 2.6 *Every cyclic group is expressible by any subgroup of finite index greater than one.*

Proof: Consider the arbitrary cyclic group $C = \langle g \rangle$ and the subgroup S of finite index $r > 1$ in C. Take an arbitrary element $a \in C$. By the definition of the transversal $Tr(S)$ there exists a unique $a_0 \equiv a \pmod S$. Assume $a \equiv \sum_{i=0}^{j} a_i r^i \pmod{Sr^j}$ for all $j \leq k$, with $a_i \in Tr(S)$, for some k and proceed by induction. Both a and $\sum_{i=0}^{k} a_i r^i$ are in C so $a = gn$ and $\sum_{i=0}^{k} a_i r^i = gm$. Therefore $g(n-m) \equiv 0 \pmod{Sr^k}$ and since g is a generator of C it follows $\langle gs \rangle = B$ for some $s \in \mathbb{Z}$. Therefore $r^k | n - m$

... hmm, requires some more work, r^j could be greater than the group size. □

Definition 2.7 (Radix Algorithm) *Let* $\mathfrak{H} = \{H_i | i \in \mathbb{N}\}$ *be an* r*-regular descending normal series so that* $[H_i, H_{i+1}] = r$ *for all* $H_i \neq 0$ *and* $H_0 = G$. *Let* $\phi_i : \{0, \ldots, r\} \to H_i$ *be a map such that* $\phi_i(m)H_{i+1} = \phi_i(n)H_{i+1}$ *implies* $m = n$ *and for each* aH_{i+1} *there exists an* n *such that* $\phi_i(n)H_{i+1} = aH$.

$$G \xrightarrow{\gamma_0} G/H_1 \xrightarrow{\gamma_1} H_1/H_2 \xrightarrow{\gamma_2} \cdots \xrightarrow{\gamma_i} H_i/H_{i+1} \xrightarrow{\gamma_{i+1}} \cdots$$

where $\gamma_i(aH_i) = a - \phi_i(a_i)$ *where* $\phi(a_i)H_i = aH_i$.

The radix expression *of* $x \in G$ *by* $\mathfrak{H}$ *is the sequence* $(x_i)_{i \in \mathbb{N}}$ *where*

$$x\phi_0(x_0)^{-1} \cdots \phi_j(x_j)^{-1} \in H_{j+1},$$

for all $j \in \mathbb{N}$.

Proposition 2.8 *The radix algorithm is well-defined.*

Proof: When $j = 0$ there exists a unique x_0 such that $\phi_0(x_0)H_1 = xH_1$ which verifies $x\phi_0(x_0)^{-1} \in H_1$. Assume $x\phi_0(x_0)^{-1} \cdots \phi_j(x_j)^{-1} \in H_{j+1}$ for some set of unique x_0 through x_j and proceed with induction.

Once again the definition of ϕ_{j+1} provides for a unique x_{j+1} such that $\phi_{j+1}(x_{j+1})H_{j+2} = x^{-1}\phi_0(x_0)^{-1} \cdots \phi_j(x_j)^{-1}H_{j+2}$. Therefore $x \prod_{i=0}^{j+1} \phi_i(x_i)^{-1} \in H_{j+2}$. By induction $(x_i)_{i \in \mathbb{N}}$ is uniquely determined for all $x \in G$ so the radix algorithm is well-defined. □

Definition 2.9 *A regular descending normal series is a collection* $\mathfrak{H} = \{H_i \mid i \in I\}$ *where* $H_{i+1} \trianglelefteq H_i$ *and* $[H_i, H_{i+1}] = [H_j, H_{j+1}]$ *where* H_i *and* H_j *are not* 0. *A strongly regular descending normal series requires further that* $H_i/H_{i+1} \cong H_j/H_{j+1}$ *when once again* H_i *and* H_j *are non-trivial. The analog exists for ascending normal series.*

Definition 2.10 *Given an r-regular descending normal series $\mathfrak{H}$ with $H_0 = G$, the expression of G by $\mathfrak{H}$ is called a radix expression and r is called the radix. If $\mathfrak{H}$ is strongly regular then G is expressed base r.*

Theorem 2.11 *If $\mathfrak{H}$ is a strongly regular descending normal series then G is isomorphic to $\prod_I G/H_1$ with radix multiplication.*

Proof: blah. □

Example 2.12 *Express D_4 base 2.*

First locate a regular descending normal series:

$$0 \lhd \langle a^2 \rangle \lhd \langle a \rangle \lhd D_4.$$

Next define the ϕ_i functions: $\phi_0(0) = e$ and $\phi_0(1) = b$, $\phi_1(0) = e$ and $\phi_1(1) = a$, and finally $\phi_2(0) = e$ and $\phi_2(1) = a^2$. Now apply the radix algorithm to each element. For instance:

$$\begin{aligned} a &\equiv e = \phi_0(0) \pmod{\langle a \rangle}, \\ a\phi_0(0)^{-1} = ae^{-1} = a &\equiv a = \phi_1(1) \pmod{\langle a^2 \rangle}, \\ a\phi_0(0)^{-1}\phi_1(1)^{-1} = ae^{-1}a^{-1} = e &\equiv e = \phi_2(0) \pmod{0}, \end{aligned}$$

so ${}^{a}\lrcorner_2 = 010$. The same works with ab:

$$\begin{aligned} ab &\equiv b = \phi_0(1) \pmod{\langle a \rangle}, \\ ab\phi_0(1)^{-1} = ab^{-1} = a &\equiv a = \phi_1(1) \pmod{\langle a^2 \rangle}, \\ ab\phi_0(01^{-1}\phi_1(1)^{-1} = ab^{-1}a^{-1} = e &\equiv e = \phi_2(0) \pmod{0}, \end{aligned}$$

and therefore ${}^{ab}\lrcorner_2 = 011$. Notice that in the second step $ab\phi_0(1)^{-1}$ is in $\langle a \rangle$ so in fact the evaluation is in $\langle a \rangle / \langle a^2 \rangle$ not $D_4/\langle a^2 \rangle$ as required.

When completed the algorithm generates the following table uniquely identifying every element.

	e	a	a^2	a^3	b	ab	a^2b	a^3b
$D/4/\langle a \rangle$	$\phi_0(0)$	$\phi_0(0)$	$\phi_0(0)$	$\phi_0(0)$	$\phi_0(1)$	$\phi_0(1)$	$\phi_0(1)$	$\phi_0(1)$
$\langle a \rangle / \langle a^2 \rangle$	$\phi_1(0)$	$\phi_1(1)$	$\phi_1(0)$	$\phi_1(1)$	$\phi_1(0)$	$\phi_1(1)$	$\phi_1(0)$	$\phi_1(1)$
$\langle a^2 \rangle / 0$	$\phi_2(0)$	$\phi_2(0)$	$\phi_2(1)$	$\phi_2(1)$	$\phi_2(0)$	$\phi_2(0)$	$\phi_2(1)$	$\phi_2(1)$
	000	010	100	110	001	011	101	111

Notice the representation need not be unique. For instance take instead the regular descending normal series:

$$H_3 = 0 \lhd H_2 = \langle a^2 \rangle \lhd H_1 = \{e, a^2, b, a^2b\} \lhd H_0 = D_4.$$

Now define: $\phi_0(1) = a$, $\phi_1(1) = b$, *and* $\phi_2(1) = a^2$. *The radix algorithm now generates:*

	e	a	a^2	a^3	b	ab	a^2b	a^3b
H_0/H_1	$\phi_0(0)$	$\phi_0(1)$	$\phi_0(0)$	$\phi_0(1)$	$\phi_0(0)$	$\phi_0(1)$	$\phi_0(0)$	$\phi_0(1)$
H_1/H_2	$\phi_1(0)$	$\phi_1(0)$	$\phi_1(0)$	$\phi_1(0)$	$\phi_1(1)$	$\phi_1(1)$	$\phi_1(1)$	$\phi_1(1)$
H_2/H_3	$\phi_2(0)$	$\phi_2(0)$	$\phi_2(1)$	$\phi_2(1)$	$\phi_2(0)$	$\phi_2(0)$	$\phi_2(1)$	$\phi_2(1)$
	000	001	100	101	010	011	110	111

Notice the results are simply permutations of each other:

$$\begin{array}{cccccccc} 000 & 010 & 100 & 110 & 001 & 011 & 101 & 111 \\ 000 & 001 & 100 & 101 & 010 & 011 & 110 & 111. \end{array}$$

Interchanging the first two rows in the table creates the other.

Proposition 2.13 *If an element is expressible then its expression is unique.*

Proof: Suppose a is expressed by $(a_i)_{i\in\mathbb{N}}$ and $(b_i)_{i\in\mathbb{N}}$. The transitivity of modular equivalence infers $\prod_{i=0}^{j}\phi_i(a_i) \equiv \prod_{i=0}^{j}\phi_i(b_i) \pmod{H_{j+1}}$ for all j. If $j = 0$ clearly $\phi_0(a_0) \equiv \phi_0(b_0) \pmod{H_1}$ implies $\phi_0(a_0)H_1 = \phi_0(b_0)H_1$ so $a_0 = b_0$ by the definition of ϕ_0. Proceeding with induction, assume $a_i = b_i$ for all $i \leq j$ for some non-negative integer j. Using cancelation $\prod_{i=0}^{j+1}\phi_i(a_i) \equiv \prod_{i=0}^{j+1}\phi_i(b_i)$ (mod H_{j+2}) reduces to $\phi_{j+1}(a_{j+1}) \equiv \phi_{j+1}(b_{j+1}) \pmod{H_{j+2}}$ where once again $\phi_{j+1}(a_{j+1}) \equiv \phi_{j+1}(b_{j+1})$ implies $a_{j+1} = b_{j+1}$ by the definition of ϕ_{j+1}. Therefore the expression of a is unique by induction. $\square$

If G is of finite order n then the maximum length required to express any element in G by the radix r is $\lceil log_r n \rceil$. Note clearly $r|n$.

Example 2.14 *Take* $\cdots \trianglelefteq r^i\mathbb{Z} \trianglelefteq \cdots \trianglelefteq r\mathbb{Z} \trianglelefteq \mathbb{Z}$ *for any* $r > 1$. *Define* $\phi_i(n) = nr^i$. *Then every element of* $\mathbb{Z}$ *is expressible.*

Proposition 2.15 *Given a right* $\mathbb{Z}$*-module* M *and a submodule* S *of finite index* r, *and take* $a \in M$ *such that* $a_{\lrcorner r} = \{a_i \mid i \in \mathbb{N}\}$. *Let* $s \in Tr(S)$ *be the element such that* $s + S = S$. *The following are true:*

1. *if* $a = \sum_{i=0}^{j} a_i r^i$ *for some* j *then* $a_k = s$ *for all* $k > j$;
2. $0_{\lrcorner r} = \bar{s}$;
3. *if* $Sr^j = \boldsymbol{0}$ *for some* j *then* $a_i = s$ *for all* $i > j$.

Proof: Take $a = \sum_{i=0}^{j} a_i r^i$ and let $k > j$. Clearly

$$a - \sum_{i=0}^{j} a_i r^i = 0 = 0r^k \equiv sr^k = a_k r^k \pmod{Sr^k}.$$

By Lemma-2.1, $a_k = s$.

Clearly $0 = 0 \cdot 1$ so condition 1 is satisfied leaving ${}^{0}\lrcorner_{S} = \bar{s}$.

Suppose $Sr^j = \mathbf{0}$ for some j. Given that $a \equiv \sum_{i=0}^{j} a_i r^i \pmod{Sr^j}$ it follows $a \equiv \sum_{i=0}^{j} a_i r^i \pmod{\mathbf{0}}$ so $a = \sum_{i=0}^{j} a_i r^i$ in $M/\mathbf{0} \cong M$. Applying condition 1 it follows $a_i = s$ for all $i > j$. $\square$

Selecting various representatives for the transversal generate different associations of numbers.

Example 2.16 *Takeing $Tr(2\mathbb{Z})$ to equal $\{1, 3\}$, instead of $\{0, 1\}$, changes ${}^{0}\lrcorner_{2}$ from $\bar{0}$ to $\bar{1}$ and ${}^{1}\lrcorner_{2}$ from $\bar{0}1$ to $\bar{0}33$. Additionally ${}^{3}\lrcorner_{2}$ becomes simply $\bar{0}3$ instead of the usual $\bar{0}11$. Thus the order of the integers are generally not preserved, with respect the corresponding lexicographic order, by the radix algorithm.*

The goal of a radix is to provide a *normal form* for the elements expressed according to the radix. This requires that the representation be unique. In most situations the ideal conditions would be a finit sequence, but sense the design of the radix algorithm functions for all positive integers, the best condition is to produce a sequence of finite type.

Definition 2.17 *An element a is expressed by S when for some j, $a_i = a_j$ for $i \geq j$ and is furthermore primitive if $a_j = 0$. M is [primitively]expressed by S when every element of M is [primitively]expressible by S. When M is expressed by S, the index $[M : S] = r$ is a radix expressing M and is said to be expressible by r.*

Notice $\cdots \trianglelefteq Sr^{j-1} \trianglelefteq \cdots \trianglelefteq Sr \trianglelefteq S \trianglelefteq R$ and at each step $[R : Sr^{j-1}] = r^j$.

Proposition 2.18 *Given a family of right $\mathbb{Z}$-modules $\{A_i \mid i = 1, \ldots, n\}$, expressible by r, the direct product $\prod_{i=1}^{n} A_i$ is expressible by r.*

Proof: Note $\prod A_i / \prod S_i \cong \prod A_i/S_i$. Therefore $(a_1, \ldots, a_n)\lrcorner_r = (a_1\lrcorner_r, \ldots, a_n\lrcorner_r)$. $\square$

Corollary 2.19 *All finitely generated abelian groups are expressible.*

Proof: The Fundamental Theorem of Finitely Generated Abelian Groups together with Proposition-2.15. $\square$

Example 2.20 ${}^{2}\lrcorner_{2} = \bar{0}10$ *and* ${}^{-2}\lrcorner_{2} = \bar{0}10$. *First* $-2 \equiv 0 \pmod 2$, *and next* $-2 - 0 = -2 \equiv 2 = 1 \cdot 2 \pmod 4$. *Now suppose* $-2 \equiv \sum_{i=1}^{j} 2^i \pmod{2^{j+1}}$ *for some* j. *Then* $-2 - \sum_{i=1}^{j} 2^i \equiv 0 \pmod{2^{j+1}}$ *and so* $-2 - \sum_{i=1}^{j} 2^i \equiv 2^{j+1} \pmod{2^{j+2}}$

$-2 - (2 + 0) \equiv -4 \equiv 4 \pmod 8$ *-2-2-4=-8*

The rational numbers are not expressible.

Notice all primitive expressions are weak direct product (or equivalently a polynomial when M is a ring) with coefficients in $Tr(S)$. Since $Tr(S)$ is a traversal for $M/Tr(S)$ it follows ${}^{a}\lrcorner_{S}$ maps a into $\prod_{\mathbb{N}} M/S$. In particular if M is primitively expressed by S then R is embedded in $\sum_{\mathbb{N}} R/S$. Considering ${}^{a}\lrcorner_{S}$ as a polynomial, even if multiplication is not defined, it is possible to consider substituting r for x in the polynomial. Thus if ${}^{a}\lrcorner_{S} = (a_0, \ldots, a_k, 0, \ldots)$ then

$$ {}^{a}\lrcorner_{S}(r) = \sum_{i=0}^{k} a_i r^i $$

However

$$ a \equiv \sum_{i=1}^{j} a_i r^{i-1} \pmod{Sr^{j-1}} $$

for all $j \in \mathbb{Z}^+$ so for all $j > k$, $a_j \equiv 0$ so $a_j = 0$ since 0 is the unique representative for the coset S, in T. In this way

$$ a \equiv \sum_{i=1}^{k} a_i r^i = {}^{a}\lrcorner_{S}(r) \pmod{Sr^{j}} $$

for all $j > k$, so ${}^{a}\lrcorner_{S}(r) = a$.

Proposition 2.21 *R is primitively expressed by S if and only if*

$$ R \cong \sum_{\mathbb{N}} R/S \cong (R/S)[x]. $$

The substitution map allows for a way to sign the elements of M. Take the positive elements to be $P = {}^{M}\lrcorner_{S}(r)$.

Definition 2.22 (Algebraic Log) *Suppose some subset A of M is expressible by r. The* algebraic log *base r of $a \in A$ is defined as the length minus 1 of ${}^{a}\lrcorner_{r}$ and is denoted $alog_r a$.*

$$ alog_r {}^{a}\lrcorner_{n} = \sum_{i=0}^{j} \frac{\phi(a_i)}{r^{j-i}} $$

where $\phi(a_i) = 0$ when $a_i = 0$ and 1 everywhere else.

Therefore $alog_r 100 = 2$, $alog_r 101 = 2 + 1/r^2$, etc. Usually $log_b x$ is defined as the unique y such that $b^y = x$. Here $alog_r$ is similar but can best be thought of as a map from M to the rationals. Unlike log, $alog_r 0$ is artificially assigned the value 0. For any elements that cannot be expressed by r the $alog$ is not defined, recall the largest set of unexpressables are called negatives.