1 Linear equations in a commutative ring

2.1 Systems of numbers // 2.2 Systems of numbers defined with respect to an ideal

3 Divisibility ← 3.1 A partial ordering based upon divisibility

4 Numerator systems $N(W, I|b)$ $EN(W, I|b)$

4.1 Special results holding for residue classes

5. Solution systems $S(W, I|a/b)$

~~Equivalence mod I~~

5.1 Strict inclusion and equivalence relations mod I an ideal

5.2 Inclusion and equivalence ~~with mod I~~

Multiplicative, saturated, independent and factored systems ???

6 Square free ideals

7 6.1 The ideal reduction

Mappings $\to$; $:= \to$

Aggregates P_M A_M

Sets of aggregates

Complete classes of aggregates $\mathfrak{C}' := \mathfrak{C}$

Class closures of aggregates

Monovalent aggregates

Univalent aggregates

Ω-factored $\to$ Θ' free

Θ' free $\to$ Θ closed

Θ' semi ideal $\to$ contractive

n.1. (i) Closed system closure

n.2 (ii) Free system closure

n.3 (viii) Semi-ideal closure

n.4 (iv) Uniquely locally soluble system closure

n.7 (vii) Contractive system closure

n.3 (iii) Factored system closure

n.5 (v) Saturated system closure

n.6 (vi) Expansive system closure

Relationships between classes

Further classes of aggregates

Linear equations in a commutative ring

$bx = a \bmod I \equiv bx - a = u \in I$

$x \to cbx = ca \bmod I$

$dx = c \bmod I \to (b \pm d)x = a \pm c \bmod I$

$dy = c \bmod I \to bd\,xy = ac \bmod I$

$by = c \bmod I \to b(x \pm y) = a \pm c \bmod I$

$y = xc + v \ (v \in I) \to by = ac \bmod I$

2.2 Systems of numbers defined with respect to an ideal

Def. 6

(1) $R(W, I)$ rigid part $d \in W$: $dx = dy$ only when $x = y \bmod I$

replace (2) ~~$E(W, I)$ entire part $e \in W$: all $a \in W$ $\exists b(a, e) \in W : a = e\,b(a, e)$~~

by (4) → (3) $\bmod I$ replace

Gp. on (3) $T(W, I)$ torsion part $t \in W \setminus I$: $\exists u \in W \setminus I$ $ut \in I$

$\overline{I} \equiv \overline{I} \cup I$

(4) I_5

(i) $b \in R \Leftrightarrow$ all $g \in W$ $bg \in I$ only when $g \in I$

(3) → (ii) $E(W, I)$

(iii) $R(W, I), E(W, I) \in M(W)$ replace $\in M_f(W)$

(iv) $E(W, I)$ nonvoid $\exists 1^{(e)} \in W$ where $e - e\,1^{(e)} e \bmod I$

s.t. $1^{(e)} b = b \bmod I$ all $b \in W$. $1^{(e)}, 1^{(f)}$ two such numbers

$1^{(e)}, 1^{(f)} \bmod I$ $1^{(e)} \in E(W, I)$

(v) $E(W, I) \subseteq R(W, I)$

(vi) $b = d \bmod I$. $b \in R\langle E \rangle$ iff $d \in R\langle E \rangle$ b unit element $\bmod I$ if d is one

(4) → (vii)

5 3.0 Divisibility

Def $B|A\{U,I\}$: $a\in A$, $b\in B$ $\exists x(a,b)\in U$ $u(a,b,x)\in I$

5 $a = bx(a,b) + u(a,b,x)$

4p.m (i) $C|B\{V,I\}$, $B|A\{U|I\} \to C|A\{UV,I\}$

31 6 (iii) $B|A\{U,I\} \to B|AC\{CU,I\}$ all $C\subseteq W$

6 (iv) $B|A\{U,I\}$, $E|C\{V,I\} \to BE|AC\{UV,I\}$

6 (v) $B|A\{U,I\}$ $C|C\{V,I\} \to BC|AC\{UV,I\}$

6 (vi) $C\subseteq A$, $F\subseteq B$, $U\subseteq V$ $I\subseteq J$ $B|A\{U,I\} \to$

$F|C\{V,J\}$

7 (vii) $B|A\{U|I\} \Leftrightarrow (B+I)|A\{U,I\} \langle B|(A+I)\{U,I\}\rangle$

$\{(B+I)|(A+I)\{U,I\}\}$ /// $U+I$???

part order found on divisibility ?? 3.1 A partial ordering based upon divisibility. (1) (2) ;

7 Def. (1) $a\leq b \bmod I$ $\exists x\in W$ $u\in I$ $bx = a+u$

(2) $a \overset{\Omega}{=} b \bmod I \equiv a\leq b, b\leq a \bmod I$

8 (i) $a\leq b, b\leq c \bmod I \to a\leq c \bmod I$

8 (ii) $a\leq b \bmod I \to ac\leq b \bmod I$ all $c\in W$ P $ac\leq bc \bmod I$

8 (iii) $a\leq b$ $c\leq f \bmod I \to ac\leq bf \bmod I$

8 (iv) $a=a'$, $b=b' \bmod I$ $a\leq b \bmod I$ iff $a'\leq b' \bmod I$

E&R (v) $a\in R(W,I)\langle E(W,I)\rangle$ $a\leq b \bmod I \to b\in R\langle E\rangle$

3p.m. duplicate 8-9 (vi) 29 ? $b\in E(W,I)$ " (1) $a\leq b \bmod I$ all $a\in W$. " (2) $ab\leq c \bmod I$ iff $a\leq c \bmod I$ " (3) $a\leq c \bmod I$ iff $a\leq bc \bmod I$ " (4) $ab\leq c \bmod I$ iff $a\leq bc \bmod I$

9 (vii) E monoid $\to \overset{\Omega}{=}$ equivalence relationship

10 (viii) $b\in T(W,I)$ $a\leq b \bmod I \to a\in T$

4. Numerator systems

~~$C\{A/B;I\}$ $BX\subseteq A+I$ $b\in C\}_b$~~

Def

(1) $N(W,I|b)=bW+I$ numerator system of b mt. I

(2) $\mathcal{O}(W,I|b)$: $o\in W$ $bo\in I$ orthog system

(3) $E\overset{\text{def}}{=}N(W,I|b)$ $a\in W$: $\mathcal{O}(b)\subseteq\mathcal{O}(a)$ extended num syst

transp $(\ )$ $C\subseteq W$ $\overline{C}$ langs $X\subseteq W$: $WX\subseteq C+I$ partial closure $C\{A/B;I\}$ $B\subseteq W\to A$

(i) $N(W,I|b)$: $a\in W$ $\exists x(a,b)\in W$ $u(a,b,x)\in I$

$a=bx(a,b)+u(a,b,x)$, $a\equiv b \bmod I$ iff $a\in N(b)$

(iii) $I\subseteq N(b)$ all $b\in W$

(iv) $b\in\overline{I}\to N(b)=I$

(v) $b=b'\bmod I\to N(b)=N(b')$

(vi) $a=a'\bmod I$ $a\in N(b)$ iff $a\in N(b')$

(vii) $N(a)N(b)\subseteq N(ab)\subseteq N(a)\cap N(b)$

(viii) $a\equiv b\bmod I\to N(a)\subseteq N(b)$

?? ~~$N(b)\in AP(W)$~~ $N(b)\in\overline{I}(W)$?

(ix) $B:=\overset{I}{B}$, $C:=\overset{J}{C}$ $\overset{I}{B}\subseteq\overset{J}{C}$ $N(W,\overset{I}{B}|b)\subseteq N(W,\overset{J}{C}|b)$

(x) $N(W,\overset{I}{B}|b)\cup N(W,\overset{J}{C}|b)=N(W,\overset{I\cup J}{B\cup C}|b)$

(xi) $N(W,\overset{I}{B}|b)\vee N(W,\overset{J}{C}|b)=N(W,\overset{I\vee J}{B\vee C}|b)$

(xc) $bv\in I\to N(b)\subseteq\mathcal{O}(v)$

(xci) $E(W,I)$ quasivid $b\in N(b)$ $N(a)\subseteq N(b)$ iff $a\equiv b\bmod I$

(ci) $N(b)\in\overline{\mathbb{I}}(W)$

(xcii) $N(W,I\cap J|b)\subseteq N(W,I|b)\cap N(W,J|b)$

(xciii) (1) $b+v\in E$ (2) $u,b+v\in E$ (3) $u,b+u_2v\in E$: $\mathcal{O}(v)\subseteq N(b)$

(xciv) $N(W,\overset{\infty}{I}|b)\subseteq\overset{\text{def}}{=}N(W,I|b)$

13 (xv) $b \in N(W, I \mid b)$ ~~$b \in \{N(W, I \mid b) / W \in I\}$~~

13 (xvi) $R(W, I)$ nonvoid $\Rightarrow N(W, I \mid b) \subseteq \tilde{N}(W, I \mid b)$

13 (xvii) (1) or (2) of ( ) + $b \vee \in I$: $N(b) \equiv \bar{O}(v) \equiv \tilde{N}(b)$

14 (xviii) (1) or (2) of ( ) + $b \vee \in I$: similar conditions with

I, v, u_1 replaced by J, v', u_1' and also by $I \cap J, v'', u_1''$

$N(I \cap J \mid b) \equiv N(I \mid b) \cap N(J \mid b) \equiv \tilde{N}(I \cap J \mid b) \equiv \tilde{N}(I \mid b) \cap \tilde{N}(J \mid b)$

4.1 Special results

15 Def: $\bar{J}(r)$ least nonneg. residues mod (r). ideal zero denby 0

$0 := \bar{J}(r)_0$?

15 (i) $N(\bar{J}(r), 0 \mid b) \equiv \tilde{N}(\bar{J}(r), 0 \mid b)$

15 remark on $E\tilde{N} \neq N$

16 ## 5. Solution systems

~~$S\{W, I \mid a/\}$~~ $S\{a/b \mid W, I\}$ $S(W, I \mid a/b)$?

Def. With $a \subseteq b \bmod I$, solution system of $bx = a \bmod I$ denoted by $\{a/b\}$

$\{a/b\}_I$?? W, I

5.1 Strict inclusion and equivalence

16 (i) $x = x' \bmod I$. $x \in \{a/b\}$ iff $x' \in \{a/b\}$

22 (ii) $a = a', b = b' \bmod I : \{a/b\} = \{a'/b'\}$

16 (iii) $a \subseteq b \bmod I \quad c\{a/b\} \subseteq \{ca/b\}$ all $c \in W$

17 (iv) $a \subseteq b, c \subseteq d \bmod I \rightarrow \{a/b\}\{c/d\} \subseteq \{ac/bd\}$

17 (v) $a \subseteq b, c \subseteq a \bmod I \rightarrow \{a/b\}\{c/a\} \subseteq \{c/b\}$

19 (vi) $a \subseteq b, c \subseteq d \bmod I \rightarrow \{a/b\} + \{c/d\} \subseteq \{(ad+bc)/bd\}$

28 (vii) $b \in R(W, I)$, $a \subseteq b \bmod I$. All members of $\{a/b\}$ equal

16 (viii) $b \in R(W, I)$, $a \subseteq b \bmod I$. All members of $\{a/b\}$ equal $\bmod I$ // if ?

22 16 (ix) $b \in R(W, I)$. (i) $\{a/b\} \subseteq \{c/d\}$ if $ad = bc \bmod I$. // (2)

$a \subseteq b \bmod I \in \{a/b\} \subseteq \{c/d\} \rightarrow ad \equiv bc \bmod I$

22 (x) $b,d \in R(W,I)$, $a \equiv b \bmod I$. $\{a/b\} \equiv \{c/d\}$ iff $ad = bc \bmod I$

23 (xx) $c \in E(W,I)$, $c \mid 1 \{1,0\} \to c\{a/b\} = \{ca/b\}$

5.2 Inclusion and equivalence modulus an ideal

23 Def. (i) $U, V \subseteq W$ $U \subseteq V \bmod I$ $u \in U$ $\exists\, v(u) \in V$ e $w(u,v) \in I$

$u = v(u) + w(u,v)$

(ii) $U \equiv V \bmod I$: $U \subseteq V, V \subseteq U \bmod I$

23 (i) $b \in R(W,I)$, $a \equiv b \bmod I$. $\{a/b\} \subseteq \{c/d\} \bmod I \to$

$ad = bc \bmod I$

24 (ii) $b,d \in R(W,I)$, $a \equiv b, c \equiv d \bmod I$. $\{a/b\} \equiv \{c/d\} \bmod I \to$

$ad = bc \bmod I$

24 (iii) $b \in R(W,I)$, $a \equiv b \bmod I$ $a = a'$, $b = b'$ $c = c' \bmod I \to$

$c\{a/b\} \equiv \{c'a'/b'\} \bmod I$

24 (iv) $b,d \in R(W,I)$, $a \equiv b, c \equiv d \bmod I$ $a = a', \ldots, d = d' \bmod I$

$\to \{a/b\}\{c/d\} \equiv \{a'c'/b'd'\} \bmod I$

$a,b,c \in R$ 24 (v) b,d $a,b \in R(W,I)$ $c \subseteq a \equiv b \bmod I$, $a = a'$, $b = b'$, $c = c'$

$a \equiv b$? no $\bmod I \to \{a/b\}\{c/a'\} = \{c'/b'\} \bmod I$

25 (vi) $b,d \in R(W,I)$ $a \equiv b, c \equiv d \bmod I$ $a = a', \ldots, d = d' \bmod I$

$\{a/b\} + \{c/d\} \equiv \{(a'd' + c'd')/b'd'\} \bmod I$

25 (vii) $c \in E(W,I) \to \{ac/b\} \subseteq c\{a/b\} \bmod I$

26 28 remark on use of divisibility properties of $E(W,I)$

28 (viii) $a \in R(W,I)\langle E(W,I)\rangle \to \{a/b\} \subseteq R(W,I)\langle E(W,I)\rangle$

~~( ) $a \equiv b \bmod I$, $a \in R(W,I)\langle E(W,I)\rangle \to b \in R(W,I)\langle E(W,I)\rangle$~~

Def.

29 ( ) $a,b \in M \to ab \in M$ mult systems M

reform ( ) $M \in \mathfrak{M}$ ~~$ab \notin M$~~ either $a \in M$ $b \notin M$ or $a \in M$, $b \notin M \to ab \notin M$

< both $a,b \notin M$ > saturated $\to ab \in M$ saturated < indep. >

mult syst M_S $< M_u >$

nec.? mult syst ( ) $ab \in M \to a \in M$ $b \in M$ factored mult system M_f

abso ( ) $M(W)$ ... $M_f(W)$

sat ind' 30 ( ) $M_f = M_S \cap M_u$.

30 ( ) $R(W,I) < E(W,I) > \in M_f(W)$

31 ( ) $M \in M_u(W) \to W \setminus M \in M_u(W)$

31 ( ) $M \in M_f(W)$ $W \setminus M \in M_u(W)$ $W \setminus M \notin M_S(W)$ $W \setminus M \notin M_f(W)$

31 —

(ii) $B|A\{U,J\}$ $B|J\{V,I\} \to B|A\{U+V,I\}$

32

? 6 Square free ideals

semi-ideal: Def. (1) ideal I $a^2 \in I$ only when $a \in I$ (2) $\mathbb{I}_{QF}$ class $\mathfrak{I}_{QF}(W)$ set

32 (i) $I \in \mathbb{I}_{QF}(W)$ $a \leq b \bmod I$ $ba \in I \to a \in I$

32 (ii) $I \in \mathbb{I}_{QF}(W)$ $a \leq b \bmod I$ $ab \in \overline{I}(W,I)$ iff $a \in \overline{I}(W,I)$

32 (iii) $I \in \mathbb{I}_{QF}(W)$ $\overline{N(W,I|b)} \leq_{EN} N(W,I|b)$.

33 (iv) $I \in \mathbb{I}_{QF}(W)$ (1) $b+v \in E$ $bv \in I$ (2) $b \leq u \bmod I$ $ub+v \in E$ $bv \in I \to N(b) \equiv_{EN} N(b)$

remarks on remls for EN

7. The ideal reduction

Defin $I \in \mathbb{I}(W)$

(1) $(a)_I$ class $b \in W : b = a \bmod I$ W_I - number

(2) a' and b' belonging to $(a)_I \in (b)_I$

(α) $(a)_I = (b)_I$ if $a' = b' \bmod I$

(β) $(a)_I (b)_I$: class of $c' : c' = a'b' \bmod I$

(δ) $(a)_I \dot{+} (b)_I$: $\quad c' = a' \pm b' \bmod I$

(3) W_I system of W_I -numbers together with equality and arithmetic operations ↑

(4) $W_I(0)$ ideal in W_I : $(0)_I$

(Expl) $(a)_I = (0)_I$ iff $a \in I$

(ii) $(a)_I \in R(W_I, W_I(0))$ iff $a \in R(W, I)$

(iii) $(a)_I \in E(W_I, W_I(0))$ iff $a \in E(W, I)$

(iv) $(a)_I \in N(W_I, W_I(0) \mid (b)_I)$ iff $a \in N(W, I \mid b)$

(v)(1) Set of all W-numbers in all $(x)_I \in W_I$ satisfying $(b)_I (x)_I = (a)_I$ is $\{a/b\}$. (2) $b \in R(W, I) \to (x)_I$ and $\{a/b\}$ consist of same numbers

Remark on use of ideal reduction in theory of solution systems

(1) Def. (A) $T_S(W, I)$ all $a \in W \setminus I$ $a^2 \in I$

(vii) $a \equiv b \bmod I$, $a \notin I$ $b \in T_S(W, I) \to a \in T_S(W, I)$

Def $E(W, I) = \bigcap_{a \in W} \{(a + I)/''W\}$

(ii) $E(W, i)$ complete system $e \in W$: $x(a,e)$ each $a \in W$, $x(a,e) \in W$

$a = e\,x(a,e) \bmod I$

Remark on extended system $\tilde{N}(b)$ $b = u^r v^s \dots z^t$ $I \in \mathbb{I}_{QF}(W)$

1. Linear equations in a commutative ring

It is proposed to study the systems of solutions of equations of the form

$$(\ ) \qquad bx = a \bmod I$$

where, W being a prescribed commutative ring, $a, b, x \in W$, and I being a system of numbers in W, the above equation is to be interpreted in the sense that $u \in I$ exists for which $bx - a = u$.

The following requirements are demanded of the equations considered:

(A) That equations can be multiplied throughout by a member of W in the sense that any solution x of equation (1) should also satisfy the equation

$$cbx = ca \bmod I$$

for all $c \in W$.

(B) That equations can be added and subtracted in the sense that if, in conjunction with equation (1), $dx = c \bmod I$ also, then

$$(b \pm d)x = a \pm c \bmod I$$

(C) That equations can be multiplied in the sense that if in conjunction with (1), $dy = c \bmod I$, then

$$bd\,xy = ac \mod \underline{I}$$

(D) that solutions form an additive system in the sense that if in conjunction with (1), $by = c \mod I$, then

$$b(x \pm y) = a \pm c \mod I$$

(E) that solutions form a multiplicative system in the sense that in conjunction with (1), $y = xc + v$ where $v \in I$ satisfies the equation

$$by = ac \mod \underline{I},$$

for all $c \in W$, $v \in I$.

Conditions (A, E) impose upon the system I the restriction that $WI \subseteq \underline{I}$, namely that I should be a semi-ideal in W. Conditions (B, D) imply that I should be additively perfect. Condition (C) entails that I should possess both of these properties, i.e. that I is an ideal in W. In the following it is tacitly assumed that $I \in \underline{\underline{I}}(W)$.

The following subsystems of W with respect to I are considered.

Definition. $R = R(W, I)$, the rigid part of W with respect to $\underline{I}$, is the complete system of numbers $d \in W$ for which, for all $x, y \in W$, $dx = dy$ only when $x = y \mod \underline{I}$.

$E = E(W, I)$, the entire part of W with respect to I, is the complete system of numbers $e \in W$ for which, for all $a \in W$, ~~a number~~ at least one number $b(a,e) \in W$ exists such that $a = eb(a,e) \bmod I$.

$T = T(W, I)$ the torsive part of W with respect to I, is the complete system of numbers $t \in W \setminus I$ ~~for~~ ~~which~~ partnered by a number u also in $W \setminus I$ such that $ut \in I$; $\overline{T} = \overline{T}(W, I)$ ~~$= T(W, I) \cup I$~~ $= T(W, I) \cup I$.

(In the previous notes $R(W, I)$ is $D(W, I)$.)

( ) $b \in R^{(W,I)}$ if and only if for all $g \in W$, $bg \in I$ only when $g \in I$. (If $bg \in I$ only when $g \in I$, then for all pairs $x, y \in W$, $b(x-y) \in I$ ~~only when $x = y$~~ i.e. $bx = by \bmod I$, only when $x = y$. If, for all pairs $x, y \in W$, $b(x-y) \in I$ only when $x - y \in I$ then, in particular taking $x = g$, $y = 0$, $bg \in I$ only when $g \in I$.)

~~( ) $E(W, I) \subseteq R(W, I)$~~

( ) $R(W, I)$, $E(W, I) \in M(W)$. (With $b, d \in R$, the condition $bdx = bdy \bmod I$ implies, since $b \in D$, that $dx = dy \bmod I$ and in turn, since $d \in R$, that $x = y \bmod I$. ~~If $e \in E$, for~~ Select $a \in W$. If $a \in E$, $b(a,e) \in W$ exists

such that $a = eb(a,e)$ and in turn, if $f \in E$, $c(b,f) \in W$ exists such that $b(a,e) = fc(b,f)$ and then $a = efc(b,f)$.)

~~( ) $E(W,I) \subseteq R(W,I)$.~~

W contains $1^{(e)}$ st.:

( ) Let $E(W,I)$ be nonvoid. A number $1^{(e)}$ ~~obtained from the~~ occurring in the relationship $e = 1^{(e)}e \bmod I$ where $e \in E(W,I)$ functions as a unit element of W in the sense that $1^{(e)}b = b \bmod I$ for all $b \in W$. If $1^{(e)}$ and $1^{(f)}$ are ~~either~~ two numbers either both derived from e as described, or derived from two members $e, f \in E$, then $1^{(e)} = 1^{(f)} \bmod I$. For all unit elements $1^{(e)}$ defined as above, $1^{(e)} \in E(W,I)$.

(Let $e = 1^{(e)}e + u$ where $u \in I$. Select $b \in W$, so that $c \in W$ exists for which $b = ec + v$ where $v \in I$. Then $1^{(e)}b = 1^{(e)}ec + 1^{(e)}v = ec + w$ where $w = 1^{(e)}v - cu \in I$. Accordingly $1^{(e)}b - b = w - u \in I$: $1^{(e)}b = b \bmod I$ for all $b \in W$. ~~Since~~ In particular $1^{(f)} = 1^{(e)}1^{(f)} \bmod I$ and $1^{(e)} = 1^{(f)}1^{(e)} \bmod I$, so that $1^{(e)} = 1^{(f)} \bmod I$. That $1^{(e)} \in E$ follows from the relationship $b = 1^{(e)}b \bmod I$ holding for all $b \in W$.)

( ) $E(W,I) \subseteq R(W,I)$. (If $E(W,I)$ is void, the given relationship is evidently correct. Otherwise W possesses a number $1^{(e)}$ for which $g = 1^{(e)}g \bmod I$ for all $g \in I$.

Since $1^{(e)}_{0} g \in I$ only when $g \in I$, $1^{(e)} \in R$ and R is nonvoid. Let d, e be any members of R, respectively (E) $f \in W$ exists such that $d = ef \bmod I$. If $eg \in I$, $dg \in I$ and, since $d \in R$, $g \in I$. Accordingly $e \in R$.)

( ) Let $b = d \bmod I$. Then $b \in R(W, I) \langle E(W, I) \rangle$ if and only if $d \in R(W, I) \langle E(W, I) \rangle$. b is a unit element of W with respect to I if and only if d is one. (Let $b = d + u$ where $u \in I$. $bg \in I$ if and only if $dg \in I$ for all $g \in W$. If, corresponding to each $c \in W_0$, $g(e, c)$ exists such that $c = bg(e, c) \bmod I$, then $c = dg(e, c) \bmod I$ also. If $ba = a \bmod I$ for all $a \in W$, then $da = a \bmod I$ for all $a \in W$ also.)

2. Divisibility

A statement concerning the existence of a solution $x \in W$ of equation ( ) is an assertion concerning the divisibility with respect to I of a by b in W. Divisibility properties of two numbers are special cases of such properties of two systems of numbers.

Definition. The notation $B \mid A \{U, I\}$ indicates that for each pair $a \in A \subseteq W$, $b \in B \subseteq W$, numbers $x(a, b) \in U \subseteq W$ and $u(a, b, x) \in I$ can be found for which $a = bx(a, b) + u(a, b, x)$.

( ) If $C|B\{V,I\}$ and $B|A\{U,I\}$, then $C|A\{UV,I\}$.

(Select a pair $a\in A, c\in C$ and any $b\in B$. Since $B|A\{U,I\}$, $x\in U$ exists such that $a=bx+u$ where $u\in I$. Similarly $y\in V$ exists such that $b=cy+v$ where $v\in I$. Thus $z=xy\in UV$ exists such that $a=zc+w$, where $w=v+xu\in I$ and accordingly $C|A\{UV,I\}$.)

( ) If $B|A\{U,I\}$, then $B|AC\{CU,I\}$ for all $C\subseteq W$.

(Any member of AC has the form ac where $a\in A, c\in C$. Select a pair $b\in B$, $ac\in AC$. Then $x\in U$ exists such that $a=bx+u$ where $u\in I$. Accordingly $z=xy\in CU$ exists such that $ac=bz+v$ where $v=cu\in I$.)

( ) If $B|A\{U,I\}$ and $E|C\{V,I\}$ then $BE|AC\{UV,I\}$.

(Any two numbers taken from BE and AC have the forms be and af respectively, where $a\in A$, $b\in B$, $c\in C$ and $f\in E$. Since $B|A\{U,I\}$, $x\in U$ exists such that $a=bx+u$ and, since $E|C\{V,I\}$, $y\in V$ exists such that $e=fy+v$. Accordingly $z=xy\in UV$ exists such that $ae=bfz+w$ where $w=bxu+fyv+uv\in I$.)

( ) If $B|A\{U,I\}$ and $C|C\{V,I\}$ then $BC|AC\{UV,I\}$.

(Set F=C in the preceding result.)

( ) Let $C\subseteq A$, $F\subseteq B$, $U\subseteq V$ and $I\subseteq J$. If $B|A\{U,I\}$ then $F|C\{V,J\}$. (If for all pairs $a\in A$ and $b\in B$,

$x(a,b) \in U$ and $u(a,b,x) \in I$ exist such that $a = bx(a,b) + u(a,b,x)$, then this property holds in particular for all pairs $a \in C \subseteq U$, $b \in F \subseteq B$: ~~and $x(a,b)$~~ $x(a,b) \in U$ and $u(a,b,x) \in J$ belong to V and J respectively.)

( ) $B|A\{U,I\}$ if and only if $(B+I)|A\{U,I\}$ ~~and if and only if $\langle B|(A+I)\{U,I\}\rangle$ and if and only if $\{(B+I)|(A+I)\{U,I\}\}$~~. (~~Any pair of numbers taken from $A+I$ and $B+I$ have the forms $a+v$ and $b+w$ respectively, where $v,w \in I$. Select such a pair. Since~~ If $B|A\{U,$ Since $A \subseteq A+I$, $B \subseteq B+I$, ~~the~~ ~~and~~ $B|A\{U,I\}$ if ~~$B+I$~~ $(B+I)|(A+I)\{U,I\}$, from the preceding result. Any pair of numbers taken from $A+I$ and $B+I$ have the forms $a+v$ and $b+w$ respectively, where $v,w \in I$. Select such a pair. If $B|A\{U,I\}$, $x \in U$ ~~exists such~~ and $u \in I$ exist such that $a = bx+u$, and then $a+v = (b+w)x+y$ where $y = u+v-xw \in I$: ~~The~~ $(B+I)|(A+I)\{U,I\}$. The preceding two results are proved in the same way.)

The divisibility of a by b establishes a partial ordering between a and b.

Definition. The notation $a \leq b \bmod I$ indicates that $x \in W$ and $u \in I$ ~~exist~~ for which ~~x~~ $bx = a+u$ exist. The notation $a \doteq b \bmod$ indicates that $a \leq b$, $b \leq a \bmod I$.

( ) If $a \equiv b$, $b \equiv c \bmod I$, then $a \equiv c \bmod I$. (This is a corollary to ( ) above.)

( ) Let $a \equiv b \bmod I$. For all $c \in W$, $ac \equiv b \bmod I$ and $ac \equiv bc \bmod I$. (The first result is a corollary to ( ) above. If $x \in W$ and $u \in I$ exist such that $a = bx + u$, then, for all $c \in W$, $ac = bcx + v$ where $v = uc \in I$.)

( ) If $a \equiv b$, $c \equiv f \bmod I$, then $ac \in bf \bmod I$. (This is a corollary to ( ) above.)

( ) Let $a = a'$, $b = b' \bmod I$. $a \equiv b \bmod I$ if and only if $a' \equiv b' \bmod I$. (Let $a = a' + v$, $b = b' + w$ where $v, w \in I$. If $x \in W$, $u' \in I$ exist such that $a' = b'x + u'$ then $a = bx + y$ where $y = u' - v + xw \in I$: $a \equiv b \bmod I$. The converse assertion is proved in the same way.)

( ) If $a \in R(W, I)\langle E(W, I)\rangle$ and $a \equiv b \bmod I$, then $b \in R(W, I)\langle E(W, I)\rangle$. (Let $a = bx + u$ where $u \in I$. If $bg \in I$ for some $g \notin I$, then $ag \in I$ also and $a \notin R$: if $a \in R$, $b \in R$. If $a \in E$ then, corresponding to each $c \in W$, $y(a,c) \in W$ exists such that $c = ay(a,c) + v(a,c,y)$ where $v(a,c,y) \in I$, and then $c = bxy(a,c) + v(a,c,y) + bz + w$ where $z = xy(a,c)$ and $w = v(a,c,y) + uy(a,c) \in I$: $b \in E$ also.)

~~( ) Let $b \in E(W, I)$. If $a \equiv b \bmod I$ then, for all $c \in W$, $abc \equiv c \bmod I$ if and only if $a \equiv c$~~

(1,2,3,9) ?? ( ) Let $b \in E(W, I)$, $a \equiv b \bmod I$ for all $a \in W$. For all

$a, c \in W$, $ab \leq c \bmod I$ if and only if $a \leq c \bmod I$, $a \leq c \bmod I$ if and only if $a \leq bc \bmod I$, and $ab \leq c \bmod I$ if and only if $a \leq bc \bmod I$. (If $b \in E$, ~~$x(a,b) \in W$ and $u(a,b,x) \in I$ exist such that~~ then corresponding to each $a \in W$, $x(a,b) \in W$ and $u(a,b,x) \in I$ exist such that $a = bx(a,b) + u(a,b,x)$: $a \leq b \bmod I$ for all $a \in W$. That $ab \leq c$ if $a \leq c$ follows from ( ) above. If $ab \leq c$, $x \in W$ exists such that $cx = ab + u$ where $u \in I$. Since $b \in E$, ~~$y \in W$~~ exists $y \in W$ such that $x = by + v$ where $v \in I$ and then $bcy = ab \bmod I$ or, since $b \in E \subseteq D$, $cy = a \bmod I$ and $a \leq c$. If $a \leq bc$, then $x \in W$ exists such that $a = c(bx) + u$ where $u \in I$, so that $a \leq c \bmod I$. If $a \leq c$, $x \in W$ and $u \in I$ exist such that $cx = a + u$. Since $b \in E$, $y \in W$ and $v \in I$ exist such that $x = by + v$, and then $bcy = a + w$ where $w = u - cv \in I$: $a \leq bc$. The last result ~~in the above group follows~~ follows from the preceding two.)

( ) If E is nonvoid, $\underline{\underline{\in}}$ is an equivalence relationship. (If E is nonvoid, $1_e \in W$ exists such that $b = 1_e b + u(b,e)$ where $u(b,e)$ for all $b \in W$: $b \leq b$ for all $b \in W$. The conditions $a \leq b$, $b \leq a$ imply ~~the~~ that $b \leq a$, $a \leq b$: if $a \underline{\underline{\in}} b$, $b \underline{\underline{\in}} a$. ( ) above implies that if $a \underline{\underline{\in}} b$, $b \underline{\underline{\in}} c$ then $a \underline{\underline{\in}} c$.)

( ). Let $b \in T(W,I)$. If $a \equiv b \bmod I$, then $a \in T(W,I)$.
(Let $a = bx + u$ where $u \in I$. If $b \in T$, $g \in W \setminus I$ exists such that $bg \in I$, and then $ag \in I$.)

As was shown in the previous notes, results ( ) hold with $\leq$ replaced by $\leq$ and with E replaced by R.)

3. Numerator systems

Definition. $N(W,I|b) = bW + I$ is the numerator system of b with respect to I in W

$O(W,I|b)$, the ~~orthogonal~~ system orthogonal to b with respect to I in W is the complete system of numbers $g \in W$ for which $bg \in I$.

$\tilde{N}(W,I|b)$, the extended numerator system of b with respect to I in W, is the complete system of numbers $a \in W$ for which $O(W,I|b) \leq O(W,I|a)$

With $C \subseteq W$, $\bar{C}$, the partial closure of C with respect to I in W is the ~~complete~~ largest system $X \subseteq W$ such that $WX \subseteq C + I$.

(In the previous notes, $\tilde{N}$ is Z.)

(1,2): ( ) $N(W,I|b)$ is the complete system of numbers $a \in W$ for which $x(a,b) \in W$ and $u(a,b,x) \in I$ exist

such that $a = bx(a,b) + u(a,b,x)$. $a \equiv b \bmod I$ if and only if $a \in N(W, I|b)$. (These results follow directly from the definitions involved.)

( ) $I \subseteq N(W, I|b)$ for all $b \in W$. (Since $0 \in W$, $I = bO + I \subseteq bW + I$)

( ) If $b \in \overline{I}$, $N(W, I|b) = I$. (If $b \in X$ where $WX \subseteq I + I$, then $bW + I \subseteq I + I + I \subseteq I$. Also $I \subseteq N(b)$, so that $N(b) = I$)

( ) If $b = b' \bmod I$, then $N(W, I|b) = N(W, I|b')$. (~~Let $b = b' + u$ where $u \in I$~~ From ( ) above, $a \equiv b$ if and only if $a \equiv b'$.)

( ) Let $a = a' \bmod I$. Then $a \in N(W, I|b)$ if and only if $a' \in N(W, I|b)$. (This result also follows from ( ) above.)

( ) $N(a)N(b) \subseteq N(ab) \subseteq N(a) \cap N(b)$. ($(aW + I)(bW + I) \subseteq abW^2 + (aW + bW)I + I^2 \subseteq abW + I$. $N(ab) = a(bW) + I \subseteq aW + I = N(a)$. Similarly $N(ab) \subseteq N(b)$.)

( ) If $a \equiv b \bmod I$, $N(a) \subseteq N(b)$. (For all $c \in N(a)$, $c \subseteq a$ and then $c \subseteq a \subseteq b$: $c \in N(b)$)

( ) If $B \subseteq C$, $N(W, B|I) \subseteq N(N, C|I)$. (If $a = bx + u$ where $u \in B$, then $u \in C$ also.)

( ) ~~$N(B|b) \cup N(C|b$~~ $N(W, B|b) \cup N(W, C|b) \subseteq N(W, B \cup C|b)$. (Since $B \subseteq B \cup C$, $N(B|b) \subseteq N(B \cup C|b)$. Similarly for $N(C|b)$.

and $N(B|b) \cup N(C|b) \subseteq N(B \cup C|b)$. If $a \in N(B \cup C|b)$, then $a = bx + u$ where $u \in B \cup C$. If $u \in B$, $a \in N(B|b)$ and if $u \in C$, $a \in N(C|b)$.)

( ) $N(W, B|b) \vee N(W, C|b) = N(W, B \vee C|b)$. (Since ~~$N(B)$~~ $N(B|b), N(C|b) \subseteq \Pi(W) \in \mathbb{P}(W)$, the general member of $N(B|b) \vee N(C|b)$ has the form $a+c$ where $a \in N(B|b)$, $c \in N(C|b)$. Similarly the general member of $B \vee C$ is $u+v$ where $u \in B$, $v \in C$. If $a = bx+u$, $c = by+v$, then $a+c = bz+u+v$ where $z = x+y$: $N(B|b) \vee N(C|b) \subseteq N(B \vee C|b)$. If $f = bz+u+v$, then $f-u = bz+v$: $f-u \in N(C|b)$. $u \in B \subseteq N(B|b)$. Hence $N(B \vee C|b) \subseteq N(B|b) \vee N(C|b)$.)

( ) If $bv \in I$, then $N(W, I|b) \subseteq O(W, I|v)$. (Let $a = bx+u$ where $u \in I$. Then $av = bvx + uv \in I$: $a \in O(v)$.)

( ) Let $E(W, I)$ be nonvoid. $b \in N(W, I|b)$; and $N(W, I|a) \subseteq N(W, I|b)$ if and only if $a \equiv b \bmod I$. (That $b \in N(b)$ when E is nonvoid follows from ( ) above. If $a \equiv b$, $N(a) \subseteq N(b)$ from ( ) above. When E is nonvoid, $a \in N(a)$ so that $a \in N(b)$ when $N(a) \subseteq N(b)$.)

( ) $N(W, I|b) \in \mathbb{SI}(S)$ for all $b \in W$. (Since $W(bW+I) = bW^2 + WI \subseteq bW + I$, $N(b) \in SI(S)$. If $a = bx+u$ and $c = by+v$ with $u, v \in I$, then $a \pm c = b(x \pm y) + u \pm v$: $N(b) \in \mathbb{AP}(W)$.)

( ) $N(W, I \cap J | b) \subseteq N(W, I|b) \cap N(W, J|b)$. (This result follows from ( ), since $I \cap J \subseteq I, J$.)

( ) Let either (1) $v \in W$ exist such that $b + v \in E(W, I)$ or (2) $u_1, v \in W$ exist such that $u_1 b + v \in E(W, I)$ or (3) $u_1, u_2, v \in W$ exist such that $u_1 b + u_2 v \in E(W, I)$. Then $\breve{O}(W, I|v) \subseteq N(W, I|b)$. (Assumption (3) is considered; assumptions (1,2) are dealt with more easily. Let $u_1 b + u_2 v - e \in E$. With $a \in \breve{O}(v)$, $y \in W$ exists such that $a = ye + w$. Since $av \in I$, $vye \in I$. But $e \in E$ and hence $e \in D$, so that $vy \in I$. Then $b(u_1 y) = ey - u_2 vy = a + z$ where $z = -u_2 vy \in I - w - u_2 vy \in I$ and accordingly $a \in N(b)$: $\breve{O}(v) \subseteq N(b)$.)

( ) $N(W, I|b) \subseteq \tilde{N}(W, I|b)$ for all $b \in W$. (With $a = bx + u$ where $u \in I$, $ag \in I$ for all g such that $bg \in I$.)

~~( ) $N(W, I|b) \subseteq \tilde{N}(W, I|b)$.~~

( ) If $R(W, I)$ is nonvoid, $\overline{N(W, I|b)} \subseteq \tilde{N}(W, I|b)$. ($\overline{N(b)}$ is the largest system $X \subseteq W$ for which $WX \subseteq bW + I$. Select $a \in X$. With $d \in R$, $x(a,d) \in W$ and $u(a,d,x) \in I$ exist such that $ad = bx(a,d) + u(a,d,x)$. For all g such that $bg \in I$, $adg \in I$ and, since $d \in R$, $ag \in I$: $a \in \tilde{N}(b)$.)

( ) $b \in \overline{N(W, I|b)}$. ($bW \subseteq bW + I$.)

( ) Let conditions (1) or (2) of ( ) hold, with $bv \in I$.

Then $N(W,I|b) \equiv \bar{O}(W,I|v)$ and $N(W,I|b) \equiv \tilde{N}(W,I|b)$ |A

(If conditions (1) or (2) of ( ) hold, then $\bar{O}(v) \subseteq N(b)$, from ( ). If $bv \in I$, $N(b) \subseteq \bar{O}(v)$, from ( ), ~~From the~~ It was shown in the previous notes that if both conditions hold as described $\bar{O}(v) \equiv \tilde{N}(b)$. For a direct proof of the second results, firstly $N(b) \subseteq \tilde{N}(b)$ from ( ). Select $a \in \tilde{N}(b)$, and let $a = ye + w$. Since $bv \in I$, $av \in I$ and, since $e \in R$, $yv \in I$. Again $b(u, y) = ey - u_2 vy = a \bmod I$, so that $a \in N(b)$: $\tilde{N}(b) \subseteq N(b)$.)

( ) Let either (1) $v \in W$ exist such that $bv \in E(W,I)$ or (2) $u_1, v \in W$ exist such that $u_1 b + v \in E(W,I)$ and, for the number b v involved, let $bv \in I$. Let similar conditions with I, v, u_1 replaced by J, v', u_1' ~~hold, with~~ and also with I, v, u_1 replaced by $I \cap J, v'', u_1''$ hold. ~~hold~~. Then $N(W, I \cap J|b) = N(W,I|b) \cap N(W,J|b) = \tilde{N}(W, I \cap J|b) \equiv \tilde{N}(W,I|b) \cap \tilde{N}(W,J|b)$. (From ( ), $N(W, I \cap J|b) \subseteq N(W,I|b) \cap N(W,J|b)$. Under the stated conditions, from ( ), $N(W,I|b) = \tilde{N}(W,I|b)$, $N(W,J|b) \equiv \tilde{N}(W,J|b)$; $N(W, I \cap J|b) \equiv \tilde{N}(W, I \cap J|b)$ and, from the previous notes ~~$\tilde{N}(W, I \cap J|b)$~~ $\tilde{N}(W,I|b) \cap \tilde{N}(W,J|b) \subseteq \tilde{N}(W, I \cap J|b)$. Hence $N(W, I \cap J|b) = N(W,I|b) \cap N(W,J|b)$ and the remaining results follow.)

Definition. $\bar{J}(r)$ is the complete system of least nonnegative residues mod r, and in $\bar{J}(r)$ the single element ideal zero is denoted by 0.

( ) $N(\bar{J}(r), 0 \mid b) \equiv \tilde{N}(\bar{J}(r), 0 \mid b)$ for all $b \in \bar{J}(r)$. (Let $b = b_1 m$, $r = s_1 m$ where $(b_1, s_1) = 1$. When $bg = b_1 m g = s_1 m$ mod r, $b_1 g = s_1 \bmod s_1$ and, since $(b_1, s_1) = 1$, $g = s_1 \bmod s_1$. $\bar{O}(b) = \bar{O}(\bar{J}(r), 0 \mid b) \equiv s_1 \bar{J}(r)$. Again, taking $a = a_1 l$, $r = f_1 l$ with $(a_1, f_1) = 1$, $\bar{O}(a) = f_1 \bar{J}(r)$. $\bar{O}(b)$ contains the number $s_1 | = s_1$. All members of $\bar{O}(a)$ have the form μf_1; thus when $\bar{O}(b) \leq \bar{O}(a)$, $s_1 = \mu f_1$ for some $\mu \in \bar{J}(r)$. The equations $r = s_1 m = \mu f_1 m$ and $r = f_1 l$ then reveal that $l = \mu m$ for some $\mu \in \bar{J}(r)$. Then $a = a_1 \mu m$ and the equation $bx = a \bmod r$ is soluble, since $m = (b, r) : a \in \tilde{N}(\bar{J}(r), 0 \mid b)$ and $\tilde{N}(\bar{J}(r), 0 \mid b) \leq N(\bar{J}(r), 0 \mid b)$. But $N(\bar{J}(r), 0 \mid b) \leq \tilde{N}(\bar{J}(r), 0 \mid b)$, so that $N(\bar{J}(r), 0 \mid b) = \tilde{N}(\bar{J}(r), 0 \mid b)$.)

(It was shown in the previous notes that $\tilde{N}(W, I \mid b) = \tilde{N}(W, \tilde{I} \mid b)$ and that $\tilde{N}(W, I \mid a) \wedge \tilde{N}(W, I \mid b) \leq \tilde{N}(W, I \mid ab)$. These results do not appear to have counterparts holding for $N(W, I \mid b)$.

4. Solution systems

Definition . With $a \equiv b \bmod I$, the complete system in W of solutions of equation (1) is denoted by $\{a/b\}$.

~~( ). Let $a \equiv b \bmod I$. $c\{a/b\} \subseteq \{ca/b\}$ for all $c \in W$. (From (1) $b(cx) = ca \bmod I$: $z = cx$ is a solution~~

( ) Let $x \equiv x' \bmod I$. $x \in \{a/b\}$ if and only if $x' \in \{a/b\}$ (If $x' \in \{a/b\}$ then $bx' = a + u$ where $u \in I$ and then $bx = a + u + bv$ where $x' = x' + v$ for all $v \in I$)

( ) Let $a \equiv b \bmod I$. $c\{a/b\} \subseteq \{ca/b\}$ for all $c \in W$. (From (1), $b(cx) = ca \bmod I$: $z = cx$ is a solution of the equation $bz = ca \bmod I$). Taking $b = 2$, $a = 4$, $c = 2$ in $J(6)$, $\{a/b\} \equiv 2, 5$ and $c\{a/b\} \equiv 4$. $\{ca/b\} \equiv 1, 4$: $1 \in \{ca/b\}$ but $1 \notin c\{a/b\}$. In this case $c\{a/b\} \subset \{ca/b\}$.

©@℮
bp 5,4

( ) If $b \in R(W, I)$ and $a \equiv b \bmod I$, all members of $\{a/b\}$ are equal mod I. (If $bx = a$, $by = a \bmod I$, then $bx = by \bmod I$ and, since $b \in R$, $x = y \bmod I$.)

( ) Let $b \in R(W, I)$. $\{a/b\} \subseteq \{c/d\}$ if ~~and only if~~ $ad = bc \bmod I$. (If $\{a/b\}$ is void, $\{a/b\} \subseteq \{c/d\}$; if in and if $a \equiv b \bmod I$ and $\{a/b\} \subset \{c/d\}$, then $ad \equiv bc \bmod I$.

(1,2)

~~it is possible that~~ this case $c\{a/b\}c\{a/b\}$.

( ) Let $a\leq b, c\leq d \bmod I$.

$r\{a/b\}\{c/d\}\leq\{ac/bd\}$ (If $bx=a+u$, $dy=c+v$ with $u,v\in I$, then $bd^{xy}_{\neq}=ac+w$ where $w=$ ~~cu+~~ $av+cu+uv\in I$: $z=xy$ is a solution of the equation $bz=ac \bmod I$.), Taking $b=1, a=2, d=2, c=4$ in $J(6)$, $\{a/b\}\equiv 2$, $\{c,d\}\equiv 2,5$ and $\{a/b\}\{c/d\}=4$. ~~Since~~ $\{ac/bd\}=1,4$ $1\in\{ac/bd\}$ but $1\notin\{a/b\}\{c/d\}$. In this case $\{a/b\}\{c/d\}\subset\{ac/bd\}$.

( ) Let $a\leq b$, $c\leq a \bmod I$.

$r\{a/b\}\{c/a\}\leq\{c/b\}$. (If $bx=a+u$, $ay=c+v$ with $u,v\in I$, then $bxy=c+w$ where $w=v+yu\in I$: $z=xy$ is a solution of the equation $bz=c \bmod I$.) ~~Taking $b=1, a=2, c=4$ as in the preceding paragraph $\{a/b\}\{c/a\}=4$. $\{c/b\}$~~. In $J(6)$, $\{a/b\}\{c/a\}\equiv\{c/b\}$. Since the congruence relationship $bx=a \bmod r$ is soluble, ~~m exists such that $b=b_1m$,~~ a has the form $a=a_1m$ where $m=(b,r)$ and, with $b=b_1m$, $r=s_1m$, so that $(b_1,s_1)=1$, and x_1 the unique solution of the relationship $b_1x_1=a_1 \bmod s_1$ in the range $0\leq x_1<s_1$, the members of $\{a/b\}$ are ~~given by~~ x_1+is_1 $(i:0,m-1)$. Since ~~the relationship $ay=c \bmod r$ is soluble, and~~ $m|a, m|r$, (a,r) has the form τm, so that a and r have the forms $a=a'\tau m$, $r=r'\tau m$ where $(a',r')=1$. The relationship $ay=c \bmod r$ is soluble: c has the form $c=c_1\tau m$ and, y_1 being the unique solution of the relationship

$a'y_1 = c_1 \bmod r'$ in the range $0 \le y_1 < r'$, the members of $\{c/a\}$ are $y_1 + jr'$ $(j: 0, \tau m - 1)$. Lastly, with z_1 the unique solution of the relationship $b_1 z_1 = c_1 \tau \bmod s_1$ in the range $0 \le z_1 < s_1$, the members of $\{c/b\}$ are $z_1 + ks_1$ $(k: 0, m-1)$. Since $s_1 = r'\tau$, the relationship $b_1 x_1 = a_1 \bmod s_1$ implies that $b_1 x_1 = a_1 \bmod r'$; similarly $b_1 z_1 = c_1 \tau \bmod r'$. Also the two relationships $b_1 x_1 = a_1$ $a'y_1 = c_1 \bmod r'$ imply that $a' b_1 x_1 y_1 = a' c_1 \tau \bmod r'$. But $(a', r') = 1$ so that $b_1 x_1 y_1 = c_1 \tau \bmod r'$, and, since $bz_1 = c_1 \tau$ $\bmod r'$, $b_1 (z - x_1 y_1) = 0 \bmod r'$. The condition $(b_1, s_1) = (b_1, r'\tau) \neq 1$ implies that $(b_1, r') = 1$, so that $z - x_1 y_1 = 0 \bmod r'$. The conditions $(b_1, r'\tau) = 1$ and $b_1 x_1 = a'\tau \bmod s'\tau$ imply that $\tau | x_1$. Similarly $\tau | z_1$, so that $z - x_1 y_1 = 0 \bmod \tau$ and in consequence $z_1 = x_1 y_1 \bmod r'\tau$: $z_1 = x_1 y_1 + \mu s_1$ for some integer μ. To show that a representative member of $\{c/b\}$ may be expressed as the product of a member of $\{a/b\}$ and one of $\{c/a\}$ it has to be demonstrated that for each k in the range $0 \le k < m$, i and j in the ranges $0 \le i < m$, $0 \le j < \tau m$ can be found such that $(x_1 + is_1)(y_1 + jr') = z_1 + ks_1 \bmod s_1 m$. Since $\tau | x_1$, x_1 has the form $x'\tau$, and the required relationship reduces to (*) $(x' + ir')s_1 j = (k + \mu - iy_1)s_1 \bmod s_1 m$. ~~The relationship $x_1 b_1 = a_1 \bmod s_1$ has a solution with x_1 as~~ Since $b_1 x_1 b_1 = a_1 \bmod s_1$, $(x_1, s_1) | a_1$: $(x'\tau, r'\tau) | a'\tau$ and $(x', r') | a'$. But $(a', r') = 1$, so that $(x', r') = 1$ also.

With k $(0 \le k \le m-1)$ & given, to find i and j $(0 \le i \le m-1, 0 \le j \le m-1)$ such that (*) $\{x'+ir'\}s_1 j = \{k+\mu-iy_1\}s_1 \bmod s_1 m$, with $(x',r')=1$

Let $z=(m,x')$, $m=m'z$, $z'=(m',z)$ and $m'=m''z'$ so that $m=m''z''$ where $z''=z'z$. All factors λ of m fall into two classes: λ such that λ/z'' when $\lambda \nmid m''$, and λ such that λ/m'' when $\lambda \nmid z''$. If λ/m'' then $\lambda \nmid z''$ then λ/z and λ/x', but $\lambda \nmid m''$ and, since $(x',r')=1$ $\lambda \nmid r'$ also. Thus for all λ such that λ/z'', $\lambda \nmid x'+m''$ but λ/x'. If λ/m'' then $\lambda \nmid z$. If λ/x' then, since λ/m also and $(m,x')=z$, λ/z, λ/z'' and $\lambda \nmid m''$. Accordingly $\lambda \nmid x'$. Hence if λ/m'', $\lambda \nmid x'+m''r'$. For all factors λ of m $\lambda \nmid x'+m''r'$: $(x'+m''r', m)=1$. With $i=m''$, $((x'+ir')s_1, s_1 m)=s_1$: j in the range $0 \le mj \le m-1$ can be found such the congruence relationship (*) has a solution j by taking it which may be taken to be the special solution, in the range $0 \le mj \le m-1$, of the relationship $(x'+ir')j=\{k+\mu-iy_1\} \bmod m$. It has been shown that each member of $\{c/b\}$ can be represented exhibited as the product of a member of $\{a/b\}$ and one of $\{c/a\}$ where, in particular, the member of $\{a/b\}$ is the same in each representation. ( ) Let $a \le b$, $c \le d \bmod I$.

$\forall \{a/b\}+\{c/d\} \le \{(ad+bc)/bd\}$. (If $bx=a+u$, $dy=c+v$ with $u,v \in I$, then $bd(xy)=d(bx)+b(dy)=ad+bc+w$ where $w=du+bv \in I$: $z=xy$ is a solution of the equation $bdz=ad+bv \bmod I$.) remark pp. 5, 41

For certain commutative rings W it is possible to show that in $\mathfrak{J}(r)$, $\{a/b\}+\{c/d\}\equiv\{(ad+bc)/bd\}$; in particular this is so for the systems W of least nonnegative residues mod r. 20

With $b=b_1m$, $a=a_1m$, $r=s_1m$, and $(b_1,s_1)=1$ and $x=x_1$ the unique solution of the congruence relationship $b_1x=a_1 \bmod s_1$, $\{a/b\}$, the system of solutions of the equation $bx=a \bmod r$ is the set x_1+is_1 $(i:0;m-1)$. Similarly, with $d=d_1n$, $c=c_1n$ $r=t_1n$ $(d,t_1)=1$ and y_1 defined by $d_1y_1=c_1 \bmod t_1$, $\{c/d\}$ is the set y_1+jt_1 $(j:0;n-1)$. $\{a/b\}+\{c/d\}$ is represented by the mn numbers $x_1+y_1+is_1+jt_1$ $(i:0;m-1/j:0;n-1)$. Since m/r and n/r, it follows that m, n and r have the forms $m=m_1h$, $n=n_1h$ and $r=r_1m_1n_1h$ where $(m_1,n_1)=1$, and then $b=b_1m_1h$, $d=d_1n_1h$. Since $m_1n_1h \mid bd$ and m_1n_1h/r, $(bd,r)=\tau m_1n_1h$ where $\tau\geq 1$. Either τ/b or τ/d; suppose the former to be the case. Then $\tau m_1h=\tau m/b$; also $\tau m_1h=\tau m/r$ and with $b=b_1m$, $r=s_1m$, $(b_1,s_1)\geq\tau$. If $\tau>1$, $(b_1,s_1)>1$ contrary to the definitions of b_1 and s_1. Hence $\tau=1$, $(bd,r)=m_1n_1h$ and $(b_1d_1h,r_1)=1$. $bd=b_1d_1h\,m_1n_1h$ and $ad+bc=h(a_1d_1+b_1c_1)m_1n_1h$. With $z=z_1$ the unique solution of the relationship $b_1d_1hz=(a_1d_1+b_1c_1)h \bmod r_1$, $\{(ad+bc)/bd\}$ is the set $z_1=kr_1$ $(k:0;m_1n_1h-1)$. Since $s_1=r_1n_1$, the condition $b_1x_1=a_1 \bmod s_1$ implies that $b_1x_1=a_1 \bmod r_1$ and hence that

$b_1 d_1 h x_1 = a_1 d_1 h \bmod r_1$. Similarly $b_1 d_1 h y_1 = c_1 b_1 h \bmod r_1$.

Accordingly $b_1 d_1 h(z_1 - x_1 - y_1) = (a_1 d_1 + b_1 c_1)h - a_1 d_1 h - c_1 b_1 h = 0 \bmod r_1$.

But $(b_1 d_1 h, r_1) = 1$. Thus $z_1 = x_1 + y_1 \bmod r_1$, and z_1 has the form $z_1 = x_1 + y_1 + k' r_1$ for some integer k', and the general member of $\{(ad+bc)/bd\}$ is $z = x_1 + y_1 + k'' r_1$ where $k'' = k + k'$. Since $(m_1, n_1) = 1$, integers m', n' exist such that $m' m_1 + n' n_1 = 1$. Then $z = x_1 + y_1 + k'' m' r_1 m_1 + k'' n' r_1 n_1 = x_1 + y_1 + i s_1 + j t_1$ where $i = k'' m'$, $j = k'' n'$: ~~The general member of~~ $\{(ad+bc$ z may be represented as a member of $\{a/b\} + \{c/d\}$. In the case under consideration $\{(ad+bc)/bd\} \subseteq \{a/b\} + \{c/d\}$ and, from the general converse result derived above, $\{(ad+bc)/bd\} = \{a/b\} + \{c/d\}$.

—o—

$b = b_1 m \quad r = s_1 m \quad (b_1, s_1) = 1 \quad b_0 = b_1 m_0 = s_1 m$

$m_0 \cdot b_1 0 = s_1 \bmod s_1$ ⇒ $b_1 0 = 0 \bmod s_1$

$\mathcal{O}(b) \equiv {}_0 S \quad a = a_1 l \quad r = f_1 l \quad {}_1 a f = a_1 l f = f_1 l$

$a_1 f = {}_1 0 \bmod f_1 \quad \mathcal{O}(a) = fS$ is $0 = {}_0 rf$? $\mathcal{O}(b) \subseteq \mathcal{O}(a)$

${}_0 0 = {}_0 1 0 \in \mathcal{O}(b)$ all members of $\mathcal{O}(a)$ have the form ${}_0 rf$

if ${}_0 0 \neq {}_0 rf$ for some $r \in S$, ${}_0 0 \notin \mathcal{O}(a)$ and $\mathcal{O}(b) \not\subseteq \mathcal{O}(a)$.

$\mathcal{O}(a) = fS$, $\mathcal{O}(b) = rfS \rightarrow a = a_1 m$?

$bx = a$
$by = c$
$b(xy) = ac$
$bx = a$
$dx = c$

particular if $ad = bc \bmod I$. Supposing that $\{a/b\}$ is nonvoid,
let $bx = a + u$ where $u \in I$. Then $bdx = ad + du = bc + w + du$ where $w, du \in I$: $bdx = bc \bmod I$ and, since $b \in R(W, I)$, $dx = c \bmod I$: $x \in \{c/d\}$ and $\{a/b\} \subseteq \{c/d\}$. Conversely, assuming that $a \leq b$, and taking any $x \in \{a/b\}$, $bx = a + u$ with $u \in I$ again. ~~$w \in I$ exists such~~ Since $\{a/b\} \subseteq \{c/d\}$, $w \in I$ exists such that $dx = c + w$ and then $bdx = ad + du$, $bdx = bc + bw$ so that $ad = bc + bw - du$: $ad = bc \bmod I$.)

( ) Let $b, d \in R(W, I)$ with $a \leq b \bmod I$. $\{a/b\} \equiv \{c/d\}$ if and only if $ad = bc \bmod I$. (From the preceding result, interchanging a, b and c, d, $\{a/b\} \subseteq \{c/d\}$ and $\{c/d\} \subseteq \{a/b\}$, i.e. $\{a/d\} \equiv \{c/d\}$ if $ad = bc \bmod I$. ~~If $\{a/b\}$ is nonvoid, and $ad = bc$ then $\{a/b\} \subseteq \{c/d\}$, $\{c/d\}$. $\{c/d\}$ is also nonvoid.~~ The condition $\{a/b\} \equiv \{c/d\}$ implies, in particular that $\{a/b\} \subseteq \{c/d\}$. Since $\{a/b\}$ is assumed nonvoid, the preceding result implies that $ad = bc \bmod I$.)

reversible ( ) Let $a = a', b = b' \bmod I$ ~~and either $b \in R(W, I)$ or $b' \in R(W, I)$.~~ Then $\{a/b\} \equiv \{a'/b'\}$. (For any $x \in W$ such that $bx = a \bmod I$, $b'x = a' \bmod I$ also: $\{a/b\} \subseteq \{a'/b'\}$. ~~That converse assertion~~ $\{a'/b'\} \subseteq \{a/b\}$ is also evident.)

( ) Let $c \in E(W, I)$ and $c|I\ \{I, O\}$. Then $c\{a/b\} = \{ca/b\}$.

(From ( ), $c\{a/b\} \subseteq \{ca/b\}$. If $\{ca/b\}$ is void, $\{ca/b\} \subseteq c\{a/b\}$. Otherwise, select z such that $bz = ca + w$ where $w \in I$. Since $c \in E$, $x \in W$ exists such that $z = cx + v$ where $v \in I$ and then $cbx = ca + w - bv$ where $w - bv \in I$. Since $c \in E$, $c \in R$ and hence $u \in I$ exists such that $bx = a + u$. Again, since $c|I\ \{I, O\}$, $t \in I$ exists such that $u = ct$ and then $z = c(x + t)$. But $x \in \{a/b\}$, so that, from ( ), $x + t \in \{a/b\}$ also : $z = cx'$ where $x' \in \{a/b\}$: $\{ca/b\} \subseteq c\{a/b\}$.)

Definition . With $U, V \subseteq W$, the notation $U \subseteq V \bmod I$ means that to each $u \in U$ correspond $v(u) \in V$ and $w(u, v) \in I$ such for which $u = v(u) + w(u, v)$. $U \equiv V \bmod I$ means indicates that $U \subseteq V$, $V \subseteq U \bmod I$.

The statement $U \equiv V \bmod I$ is weaker than $U = V$. In the latter, all members of U feature in V and conversely; in the former it is possible that no member of U belongs to V and conversely.

( ) Let $b \in R(W, I)$ and ~~$b|a \bmod I$~~ $a \subseteq b \bmod I$. If $\{a/b\} \subseteq \{c/d\} \bmod I$ then $ad = bc \bmod I$. (Taking any $x \in \{a/b\}$, $bx = a + u$ where $u \in I$. $v \in I$ exists such ~~for which~~ that $d(x + v) = c + w$ where $w \in I$, and

then $bdx = ad + du$, $bdx = bc + bw - bdw$ so that $ad = bc + bw - bdw - du : ad = bc \bmod I$.)

( ) Let $b, d \in R(W, I)$ and $a \leq b$, $c \leq d \bmod I$. If $\{a/b\} \equiv \{c/d\} \bmod I$, then $ad = bc \bmod I$. (This is a corollary to the preceding result.)

2': ( ) Let $a \leq b \bmod I$, $b \in R(W, I)$ and $a = a'$, $b = b'$, $c = c' \bmod I$. Then $c\{a/b\} \equiv \{c'a'/b'\} \bmod I$. (Since $a \leq b$, $ca \leq b$. Select any $x \in \{a/b\}$, $z \in \{ca/b\}$ so that $bx = a + u$, $bz = ca + v$ where $u, v \in I$. Then $bz = bcx + w$ where $w = cu + v \in I$. $bz = bcx \bmod I$ and, since $b \in R$, $z = cx \bmod I$. Finally $\{ca/b\} \equiv \{c'a'/b'\}$.)

3': ( ) Let $a \leq b$, $c \leq d \bmod I$, $b, d \in R(W, I)$ and $a = a'$, ..., $d = d' \bmod I$. Then $\{a/b\}\{c/d\} \equiv \{a'c'/b'd'\} \bmod I$. Since $a \leq b$ and $c \leq d$, $ac \leq bd$. Select any $x \in \{a/b\}$, $y \in \{c/d\}$ and $z \in \{ac/bd\}$ so that $bx = a + u$, $dy = c + v$, $bdz = ac + w$ where $u, v, w \in I$. Then $bdxy = bdz + t$ where $t = av + cu + uv - w \in I$. Since $b, d \in R$, $bd \in R$ and $xy = z \bmod I$. Finally $\{ac/bd\} \equiv \{a'c'/b'd'\}$.)

4': ( ) Let $c \leq a \leq b \bmod I$, $a, b \in R(W, I)$ and $a = a'$, $b = b'$, $c = c' \bmod I$. Then $\{a/b\}\{c/a'\} \equiv \{c'/b'\} \bmod I$. (Since $c \leq a \leq b$, $c \leq b$. Select any $x \in \{a/b\}$, $y \in \{c/a\} \equiv \{c/a'\}$ and $z \in \{c/b\}$, so that $bx = a + u$, $ay = c + v$ and

$bz = c \bmod I$ where $u, v \in I$. Then $abxy = ac + av + cu + uv$. 25

Since $a \in R$, $bxy = c \bmod I$. Hence $bxy = bz \bmod I$ and, since $b \in R$, $xy = z \bmod I$. Finally $\{c/b\} \equiv \{c'/b'\}$.)

( ) Let $a \le b$, $c \le d \bmod I$, $b, d \in R(W, I)$ and $a = a', \ldots, d = d' \bmod I$. Then $\{a/b\} + \{c/d\} \equiv \{(a'd' + c'd')/b'd'\} \bmod I$.

(Since $a \le b$ and $c \le d$ then $ad \le bd$, $cd \le bd$ and $ad + cd \le bd$. Select any $x \in \{a/b\}$, $y \in \{c/d\}$ and $z \in \{(ad+bc)/bd\}$, so that $bx = a + u$, $dy = c + v$ where $u, v \in I$ and $bdz = ad + bc \bmod I$. Then $bd(x+y) = b(dx) + b \cdot d(bx) + b(dy)$ $= ad + bc + bv + du$ so that $bd(x+y) = ad + bc \bmod I$. Since $b, d \in R$, $bd \in R$ and $z = x + y \bmod I$. Finally $\{(ad+bc)/bd\} \equiv \{(a'd' + b'c')/b'd'\}$.)

( ) If ~~Let $ac \le b$~~ ~~Let~~ $c \in E(W, I)$, then $\{ac/b\} \le c\{a/b\}$ $\bmod I$. (If $\{ac/b\}$ is void, the result is true. Otherwise, suppose that $bz = ca + w$ where $w \in I$. Since $c \in E$, $x \in W$ and $v \in I$ exist such that $z = cx + v$, and then $cbx = ca + w - bv$. Since $c \in E$, $c \in R$. Thus $u \in I$ exists such that $bx = a + u$: $x \in \{a/b\}$. $z = cx + v$ and $\{ac/b\} \le c\{a/b\} \bmod I$.)

~~Inclusion relationships for solution systems may be derive based upon assumptions concerning the~~

Inclusion relationships for solution systems based upon assumptions concerning divisibility properties of $E(W,I)$ may also be given. For example: let $bd \in E(W,I)$; then $\{ac/bd\} \leq \{a/b\}\{c/d\} \bmod I$. (Since $bd \in E$, $b, d \in E$ from ( ): $\{ac/bd\}$, $\{a/b\}$ and $\{c/d\}$ are all nonvoid. Let $a = bx+u$, $c = dy+v$, $bdz = ac+w$ where $u, v, w \in I$. Then $bdz = c(bx+u)+w$. Since $b \in E$, $b \in R$ and $dz = cx+t$ where $t \in I$. ~~Letting $c = dy+e$ where $e \in I$,~~ Again $dz = x(dy+v)+t$ and, since $d \in R$, $z = xy+s$ ~~where~~ $\bmod I$.) But this result is a simple corollary to ( ): since $b, d \in E$ it follows that $a \leq b$, $c \leq d \bmod I$ for all $a, c \in W$ and also that $b, d \in D$. Again, results based upon the assumption that numerators belong to $E(W,I)$ may be given. For example: let $ac \in E(W,I)$; then $\{ac/bd\} \leq \{a/b\}\{c/d\}$, $\bmod I$. (If $\{ac/bd\}$ is void, the result is

numerators involved may also be derived. For example: Let $a \leq b$, $ac \equiv bd \pmod{I}$ where $ac \in E(W, I)$; then $\{ac/bd\} \leq \{a/b\}\{c/d\}$ (mod I). (If $\{ac/bd\}$ is void, the result is evidently correct. Otherwise, assuming that $ac \leq bd$, let $bdz = ac + w$ where $w \in I$. Since $ac \in E$, $a, c \in E$ from also $bd \in E$ from ( ); and $y \in W$, $g \in I$ exist such that $bz = ax + g$, $dz = cy + h$. Thus $bdz^2 = (axe + g)(cy + h)$, so that $acz = acxy + t$ where $t \in I$. Since $ac \in E$, it follows that $ac \in D$ and in consequence that $z = xy \pmod{I}$. But, since $bz = ax + g$, $bxy = ax \pmod{I}$ and, since it follows from ( ) that $bd \in E$ and, from ( ), that $b, d \in E$

evidently correct. Otherwise, assume that $ac \leq bd$. Since $ac \in E$, $a, c \in E$ from ( ). Also, from ( ), $bd \in E$ and, from ( ), $b, d \in E$. Since $ac \leq bd$, $z \in W$ and $w \in I$ exist such that $bdz = ac + w$ and, from ( ), $z \in E$, since $bd, ac \in E$. From (,) $x, y \in E$ and $g, h \in I$ exist such that $bz = ay + g$, $dz = cx + h$. Thus $bdz^2 = (ay + g)(cx + h)$, so that $acz = acxy + t$ where $t \in I$. Since $ac \in E$ it follows that $ac \in D$ and in consequence that $z = xy \pmod{I}$. But, since $bz = ay + g$, $bxy = ay \pmod{I}$

and, since $y \in E \subseteq R$, $bx = a \bmod I$: $x \in \{a/b\}$. Similarly $y \in \{c/d\}$ and $\{ac/bd\} \subseteq \{a/b\}\{c/d\}$.) However,
the conditions $ac \leq bd$ with ~~$b, d \in$~~ $ac \in E$ imply ~~that $b, d \in E \subseteq R$ and the stated result is a consequence of ( ).~~ Again a similar proof yields the result that if $b, d \in E(W, I)$ then $\{ac/bd\} \subseteq \{a/b\}\{c/d\}$. But if $bd \in E$, $b, d \in R$ and the result given is again a ~~consequence of ( ).~~

that $bd \in E$ and the stated result is a consequence of its predecessor which itself is a simple corollary to ( ). Similar counterparts to (-) may also be given.

( ) Let $a \in R(W, I) \langle E(W, I) \rangle$. Then $\{a/b\} \subseteq R(W, I) \langle E(W, I) \rangle$ for all $b \in W$. (If $\{a/b\}$ is void, the result is correct. ~~If $a \leq b$ then $b \in R\langle E \rangle$. Let $bx = a + u$ where $u \in I$.~~ ~~Select~~ Otherwise, select $x \in \{a/b\}$, so that $bx = a + u$ where $u \in I$. ~~Since $a \leq b$, $b \in R\langle E \rangle$.~~ If $g \notin I$ exists such that $xg \in I$, then $ag \in I$ and $\bullet a \notin R$ contrary to assumption ~~Since~~ If $a \in E$, then to each $c \in W$ correspond $d(a,c) \in W$ and $e(a,c,d) \in I$ such that $c = ad(a,c) + e(a,c,d)$: to

each $c \in W$ correspond ~~$bd(a,c) \in W$ and~~ $f(x,c) = bd(a,c) \in W$ and $g(x,c,f) = e(a,c,d) - ud(a,c) \in I$ such that $c = xf(x,c) + g(x,c,f) : x \in E$.)

( ) Let $a \equiv b \bmod I$. If $a \in R(W,I) \langle E(W,I) \rangle$ then $b \in R(W,I) \langle E(W,I) \rangle$ (let $bc = a + u$ where $u \in I$. If $c \notin I$ exists such that $bc \in I$, then $ac \in I$ and $a \notin R$. Hence if $a \in R$, $b \in R$ also. If $a \in E$, then to each $c \in W$ correspond $d(a,c) \in W$ and $e(a,c,d) \in I$ such that $c = ad(a,c) + e(a,c,d)$: to each $c \in W$ correspond $f(b,c) = xd(a,c) \in W$ and $g(b,c,f) = e(a,c,d) - ud(a,c) \in I$ such that $c = bf(b,c) + g(b,c,f) : b \in E$.)

Definition. A system $M \neq \mathbb{M}$ of numbers which is such that $ab \in M$ for all $a, b \in M$ is a multiplicative system. $\mathbb{M}$ is the class of multiplicative systems

A multiplicative system M which is ~~such that~~ for which $ab \notin M$ when either $a \in M, b \notin M$ or $a \notin M, b \in M$ ~~$\langle a, b \notin M \rangle$~~ when $a, b \notin M$ is a saturated ⟨an independent⟩ multiplicative system

A multiplicative system M for which $ab \in M$ only when $a, b \in M$ is a factored multiplicative system.

$\mathbb{M}_s$, $\mathbb{M}_u$ and $\mathbb{M}_f$ are the classes of saturated, independent and factored multiplicative systems respectively.

$M(W)$ is the set of multiplicative systems in $M \subseteq W$. The symbols $M_S(W)$, $M_U(W)$ and $M_f(W)$ have corresponding meanings.

( ) $M_f = M_S \cap M_U$. (Let $M \in M_f(W)$. If $a \in M$ and $b \notin M$, then $ab \notin M$, since if $ab \in M$ then $b \in M$, violating the condition that $b \notin M$: $M_f \subseteq M_S$. If $a \notin M$, $b \notin M$ then $ab \notin M$, since if $ab \in M$, then $a, b \in M$: $M_f \subseteq M_U$. Hence $M_f \subseteq M_S \cap M_U$. Let $M \in M_S(W)$. The condition $ab \in M$ implies that the twin conditions $a \in M$, $b \notin M$ cannot hold: either $a, b \in M$ or $a \notin M$, $b \notin M$. Let $M \in M_U(W)$ also. If $ab \in M$, the conditions $a \notin M$, $b \notin M$ are do not hold: the single condition $a, b \in M$ holds: $M_S \cap M_U \subseteq M_f$.)

( ) $R(W, I)\langle E(W, I)\rangle \in M_f(W)$ (Let $a, b \in R$. If $abg \in I$ then, since $a \in R$, $bg \in I$ and, since $b \in R$, $g \in I$: $abg \in I$ only when $g \in I$: $R \in M(W)$. Let $ab \in R$. If $g \notin I$ exists such that $bg \in I$ then $abg \in I$ and $ab \notin R$: $b \in R$ and similarly $b \in R$: $R \in M_f(W)$. Let $a, b \in E$ and select $g \in W$. Since $a \in E$, $y \in W$ and $u \in I$ exist such that $g = ay + u$. Since $b \in E$, $x \in W$ and $v \in I$ exist such that $y = bx + v$ and then $g = abx + w$ where $w = u + av \in I$: $ab \in E$: $E \in M(W)$. Select $g \in W$. Si-

Let $ab \in E$ and select $g \in W$. ~~x exist~~ $x \in W$ and $v \in I$ exist such that $bg = ab_{\pi} + {}_{\pi}v$. Since $b \in R$, $ab \in E$, $ab \in R$ and $b \in R$. Thus $0 = ax + u$ with $u \in I : a \in E$. Similarly $b \in E$.) : $E \in M_f(W)$.)

( ) If $M \in M_u(W)$ then $\overline{W \setminus M} \in M_u(W)$. (If $M \in M_u(W)$, $ab \in W \setminus M$ when $a, b \in W \setminus M$: $W \setminus M \in M(W)$. Also, since $M \in M(W)$, ~~$ab \in W \setminus (W \setminus M)$~~ when $ab \notin W \setminus M$ when $a, b \notin W \setminus M$: $W \setminus M \in M_u(W)$.)

(1, 2, 3) ( ) If $M \in M_f(W)$, $W \setminus M \in M_u(W)$ but $W \setminus M \notin M_s(W)$ and hence $W \setminus M \notin M_f(W)$. (Since $M_f \subseteq M_u$, $W \setminus M \in M_u(W)$. Also, since $M \in M_s(W)$, when $a \notin W \setminus M$ and $b \in W \setminus M$, $ab \in W \setminus M$: ~~$M \notin M_s$~~ $W \setminus M \notin M_s(W)$ and, since $M_f \equiv M_u \cap M_s$, $W \setminus M \notin M_f(W)$.)

( ) ~~Let~~ If $B|A\{U, T\}$ and $B|J\{V, I\}$ then $B|A\{U+V, I\}$. (Select $a \in A$, $b \in B$. Since $B|A\{U, T\}$, $g \in W$ and $v \in J$ exist such that $a = bg + v$. Since $B|J\{V, I\}$, $z \in V$ and $u \in I$ exist such that $v = bz + u$. Thus $x = y + z \in U + V$ and $u \in I$ exist such that $a = bx + u$: $B|A\{U+V, I\}$.)

5. Square-free ideals.

Definition An ideal I for which $a^2 \in I$ only when $a \in I$ is said to be square-free. $\mathbb{I}_{QF}$ is the class of square-free ideals and $\mathbb{I}_{QF}(W)$ the set of square free ideals $I \subseteq W$.

( ) Let $I \in \mathbb{I}_{QF}(W)$. If $a \equiv b \bmod I$ and $ba \in I$ then $a \in I$. (Let $bx = a + u$ so that $abx = a^2 + au$. If $ab \in I$, then $a^2 = abx - au \in I$ and $a \in I$.)

( ) Let $I \in \mathbb{I}_{QF}(W)$ and $a \equiv b \bmod I$. $ab \in \overline{T}(W, I)$ if and only if $a \in T(W, I)$. (~~Let $bx = a + u$ where $u \in I$. If $a \in T$, $g \notin I$ exists such that $ag \in$~~ from ( ),

~~(If $a \in T$, $a \notin I$. Since, $ya \in I$ when $a \equiv b$ for all $b \in I$, & $b \notin I$.~~

Since $I \in \mathbb{I}_{QF}(W)$, the condition $ab \in I$ implies that $a \in I$; hence $ab \notin I$. When $a \in T$, $g \notin I$ exists such that $ag \in I$ and, for this g, $abg \in I$ also: $ab \in T$ if $a \in T$. Let $bx = a + u$ where $u \in I$. If $ab \in T$ then $b^2x \in T$. $g \notin I$ exists such that $b^2xg \in I$ so that $(bxg)^2 \in I$ and $bxg \in I$, or, since ~~$bxa =$~~ $bx - u$, $ag \in I$: $a \in T$ if $ab \in T$.)

( ) If $I \in \mathbb{I}_{QF}(W)$, $\overline{N(W, I|b)} \subseteq \tilde{N}(W, I|b)$. ($\overline{N(b)}$ is the largest system $X \subseteq W$ for which $WX \subseteq bW + I$. Select $a \in X$ and any $g \in W$ for which $bg \in I$. $x(a, g) \in W$ and $u(a, g, x) \in I$ exist such that $ag = bx(a, g) + u(a, g, x)$. Since $bg \in I$,

$ag^2 \in I$ and, since $I \in \mathbb{I}_{QF}(W)$, $ag \in I$: for all g such that $bg \in I$, $ag \in I$ also: $a \in \tilde{N}(b)$. Note: ( ) is the same result subject to the condition that $R(W,I)$ should be nonvoid.)

( ) Let $I \in \mathbb{I}_{QF}(W)$. If either (1) $v \in W$ exists such that $b+v \in E(W,I)$, $bv \in I$ or (2) $u, v \in W$ exist such that $b \equiv u \bmod I$, $ub+v \in E(W,I)$, $bv \in I$, then $N(W,I|b) = \tilde{N}(W,I|b)$. (From ( ), $N(b) \subseteq \tilde{N}(b)$. Assume case (2) to hold and select any $a \equiv b$. v. Since $ub+v \in E$, $x \in W$ and $bx \in I$ exist such that $(ub+v)x = ua+w$. Since $a \equiv b$ and $bv \in I$, $av \in I$ and $vxv^2 \in I$. Since $I \in \mathbb{I}_{QF}(W)$, $xv \in I$. Hence $ubx = ua+t$ where $t \in I$. Since $b \equiv u$, $bx \equiv u$ and, since $a \equiv b$, $a \equiv u$ so that $bx - a \equiv u$. But $u(bx-a) \in I$ so that, since $I \in \mathbb{I}_{QF}(W)$, $bx \equiv a \bmod I$: $a \in N(b)$: $\tilde{N}(b) \subseteq N(b)$. Note: Since $N(u) \subseteq \tilde{N}(u)$ the condition $b \equiv u$, i.e. $b \in \tilde{N}(u)$, is weaker than $b \subseteq u$, i.e. $b \in N(u)$.)

If $I \in \mathbb{I}_{QF}(W)$, as was shown in the preceding notes, the following results hold: $\tilde{N}(W,I|b) \in \mathbb{I}_{QF}(W)$; $\tilde{N}(ab) = \tilde{N}(a) \cap \tilde{N}(b)$; $\tilde{N}(a^m) = \tilde{N}(a^n)$ $(m,n:\neq)$; if $a \equiv b$ and $ab \equiv c$, then $a \equiv bc \equiv c$; if $a \equiv b$ than $a \equiv ab$; if $a, c \equiv b$ and $ab = bc \bmod I$, then $a = c \bmod I$. They do not appear to

hold for $N(b)$ and the partial ordering $\subseteq \xi$.

6. The ideal reduction

Definition. Let $I \in \mathbb{I}(W)$.

(i) $(a)_I$ is the class of numbers $b \in W$ for which $b = a \bmod I$; ~~such a class is a W_I-number~~

(ii) With a', b' any numbers of W belonging to $(a)_I$ and $(b)_I$ respectively (1) $(a)_I = (b)_I$ if and only if $a' = b' \bmod I$; (2) $(a)_I (b)_I$ is the class of numbers c' such that $c' = a'b' \bmod I$; (3) $(a)_I \pm (b)_I$ are the classes of numbers c' for which $c' = a' \pm b' \bmod I$

(iii) ~~$(0)_I$ is the $W_I(0)$ is the single element ideal~~

(iii) W_I is the system of ~~classes $(a)_I$~~ W_I-numbers together with the arithmetic operations as defined above; it is the I-reduction of W.

(iv) $W_I(0)$ is the ideal in W_I consisting of the single element $(0)_I$.

( ) $(a)_I = (0)_I$ in W_I if and only if $a \in I$. (~~If $a \in I$,~~ Taking a in $(a)_I$ and 0 in $(0)_I$ to represent these classes respectively. If $a \in I$, $a - 0 \in I$ and $(a)_I = (0)_I$. If $(a)_I = (0)_I$, ~~$a - 1$ $a - 0 \in I$ and~~ $a - 0 = a \in I$)

( ) $(a)_I \in R(W_I, W_I(0))$ if and only if $a \in R(W, I)$ ($(a)_I \in W_I(0)$ if and only if $0 \in I$ and $(a)_I (0)_I \in W_I(0)$ if and only if $a0 \in I$. Let $a \in R$.

If $(a)_I(g)_I \in W_I(0)$ then $ag \in I$ and hence $g \in I$ and in consequence $(g)_I \in W_I(0)$. Thus $(a)_I \in R(W_I, W_I(0))$ if $a \in R$. Let $(a)_I \in R(W_I, W_I(0))$. If $ag \in I$ then $(a)_I(g)_I \in W_I(0)$ and hence $(g)_I \in W_I(0)$ and in consequence $g \in I$. Thus $a \in R$ if $(a)_I \in R(W_I, W_I(0))$.

( ) $(a)_I \in E(W_I, W_I(0))$ if and only if $a \in E(W, I)$.

(~~Let $b,c,d,e \in W$. If $b = cd+e$ then $(b)_I = (c)_I(d)_I + (e)_I$ If $(b)_I = (c)_I(d)_I + (e)_I$ then $f \in I$ exists such that $b = cd+e+f$.~~ Let $a \in E$. ~~$x(a$~~ and select $(g)_I \in W_I$. $x(a,g) \in W$ and $u(a,g,x) \in I$ exist such that $g = ax(a,g) + u(a,g,x)$, and then $(x(a,g))_I \in W_I$ and ~~$(u(a,g,x))_I \in W_I(0)$~~ exists such that $(g)_I = (a)_I(x(a,g))_I$ in W_I ~~$+ (u(a,g,x))_I$~~. Thus $(a)_I \in E(W_I, W_I(0))$ if $a \in E$. Let $(a)_I \in E(W_I, W_I(0))$ and select $g \in W$. $(x(a,g))_I \in W_I$ ~~and $(u(a$~~ exists such that $(g)_I = (a)_I(x(a,g))_I$ in W_I and then $g = ax(a,g) + u(a,g,x)$ for some $u(a,g,x) \in I$. Thus $a \in E$ if $(a)_I \in E(W_I, W_I(0))$.)

( ) $(a)_I \in N(W_I, W_I(0) | (b)_I)$ if and only if $a \in N(W, I|b)$

(Let $a \in N(b)$. $x \in W$ and $u \in I$ exist such that $a = bx + u$ so ~~and~~ that ~~$(a)_I = (b)_I$~~ $(x)_I \in W_I$ exists for which $(a)_I = (b)_I(x)_I$ ~~; so~~ ; Thus $(a)_I \in N(W_I, W_I(0) | (b)_I)$ if $a \in N(b)$.

Let $(a)_I \in N(W_I, W_I(0) | (b)_I)$. $(x)_I \in W_I$ exists such that $(a)_I = (b)_I(x)_I$ ~~so~~ in W_I, so that $u \in I$ exists such that

$a = bx + u$. Thus $a \in N(b)$ if $(a)_I \in N(W_I, W_I(0)|(b)_I)$.)

It was shown in the previous notes that $(a)_I \in \tilde{N}(W_I, W_I(0)|(b)_I)$ if and only if $a \in \tilde{N}(W, I|b)$.

( ) ~~With $a \leq b \bmod I$,~~ The set of all W-numbers in all W_I-numbers $(x)_I$ satisfying the equation $(b)_I(x)_I = (a)_I$ in W_I is $\{a/b\}$. Furthermore, if $b \in R(W, I)$, $(x)_I$ and $\{a/b\}$ consist of the same numbers. (The equation $(b)_I(x)_I = (a)_I$ has a solution $(x)_I$ in W_I if and only if $(a)_I \in N(W_I, W_I(0)|(b)_I)$, i.e if and only if $a \leq b \bmod I$. If this condition is violated, the set of all W-numbers in all W_I-numbers $(x)_I$ satisfying the equation $(b)_I(x)_I = (a)_I$ is void, as is $\{a/b\}$. Assuming that $a \leq b \bmod I$, select $x' \in (x)_I$ satisfying equation ( ). Then $u \in I$ exists such that $bx' = a + u$ and $x' \in \{a/b\}$. If $x' \in \{a/b\}$, $u \in I$ exists such that $bx' = a + u$ and then $(b)_I(x')_I = (a)_I$ so that x' belongs to a W_I-number, namely $(x')_I$ satisfying equation (*))

The numerator set $N(W, I|b)$ and extended numerator set $\tilde{N}(W, I|b)$ associated with the single number $b \in W$ are those associated with the system of numbers b' for

which $b=b' \bmod I$. The solution system $\{a/b\}$ of the equation $bx=a \bmod I$ is that of all equations $b'x=a' \bmod I$ for which $a=a', b=b' \bmod I$. The theory of the equation $bx=a \bmod I$ is that of a system of equations $b'x=a' \bmod I$ as described. By working in W_I, the reduction of W with respect to I, the theory of the system of equations $b'x=a' \bmod I$ with $a=a', b=b' \bmod I$ is reduced to that of the single equation $(b)_I (x)_I = (a)_I$ and may accordingly be presented in simpler terms.

$\mathfrak{T}_S(W,I)$ is the complete system of numbers $a \in W \setminus I$ for which $a^2 \in I$.

( ) If $a \equiv b \bmod I$ with $a \notin I$ and $b \in \mathfrak{T}_S(W,I)$, then $a \in \mathfrak{T}_S(W,I)$. (Since $x \in W$ and $u \in I$ exist such that $bx=a+u$, $b^2x^2=a^2+w$ where $w \in I$ and, since $b^2 \in I$, $a^2 \in I$.)

Definition. $E(W,I) = \bigcap_{a \in W} \{(a+I)/''W\}$ is the entire part of E with respect to I.

( ) $E(W,I)$ is the complete system of numbers $e \in W$ for which, for each $a \in W$, at least one number ~~$x(a,e) \in W$ exists such and one number $u(a,e,x) \in I$ exist such that $a = e x(a,e) + u$~~ $x(a,e) \in W$ exists such that $a \equiv e\,x(a,e) \bmod I$. ($(a+I)/''W$ is the set of all $b \in W$ such that $bx(a,b) \in a+I$ for at least one $x(a,b) \in W$. ~~$bx(a,b) \in a+I$~~ if and only if $bx(a,b) \equiv a \bmod I$. $\bigcap_{a \in W} \{(a+I)/''W\}$ is the set of all $b \in W$ such that for each $a \in W$ at least one $x(a,b) \in W$ exists for which ~~bx~~, $bx(a,b) \equiv a \bmod I$.)

( ) That the extended numerator set $\tilde{N}(W,I|b)$ may be a considerably extended version of the numerator set $N(W,I|b)$ may be shown by considering the case in which $I \in \mathbb{I}_{QF}(W)$ and $b = u^r v^s \dots z^t$. $\tilde{N}(W,I|b)$ contains $N(W,I|b)$. Using the result that if $a \leq b$ and $ab \leq c$ ~~then~~ then $a \leq c$ (with $a = u^{r-1} v^s \dots z^t$, $b = u$, $c = u^r v^s \dots z^t$ and continuing) it may be shown that $\tilde{N}(W,I|b)$ also contains $N(W,I|uv\dots z)$. If also $u \leq v \leq \dots \leq z$, then $\tilde{N}(W,I|b)$ also contains $N(W,I|u)$

(remember mod r integers form rational ring)