Chapter II. Computability and Unsolvability for Module Theories.

In the study of a well-defined class of mathematical problems, it is natural to hope for a general computing procedure which resolves all questions of the given type. In the next section, it is shown that no such procedure exists for the full range of module theory questions considered here. That is, there is no recursive procedure for deciding the truth of basic universal Horn sentences as in §6, with respect to any fixed nontrivial ring. This result is proved by constructing a finitely-presented additive relation algebra with a recursively unsolvable word problem.

For additive relation algebras which are *free*, the corresponding word problems are recursively computable for many rings R. Essentially, the free word problems are computable if we can decide when integers divide other integers in R, where these "integers" are 0 or additive multiples $1+1+\ldots+1$ of the ring unit. Such integer divisibility is always computable for rings with nonzero characteristic, but there are rings with characteristic zero for which it is not computable. In the later sections of this chapter, we demonstrate and apply these free word problem results.

§8. Recursively Unsolvable Word Problems and Decision Procedures.

To prove a problem recursively unsolvable, it suffices to show that a solution procedure for the problem would also solve a problem already known to be recursively unsolvable. We use such a reduction here, based upon the result of Novikoff [ ] and Boone [ ] that the word problem for groups is recursively unsolvable. That is, there is a finitely-presented group G with a recursively unsolvable word problem, and we can suppose that G has two generators by the theorem of Higman, Neuman and Neuman [ ]. By the method of [ ], we easily obtain an additive relation algebra presentation that demonstrates the desired recursive unsolvabilities.

8.1. Definitions. Let τ_G be the algebraic type for groups, taken as $\langle \cdot, ^{-1}, 1\rangle$ with arities $\langle 2,1,0\rangle$. Let $\mathfrak{V}$ denote the variety of groups, as τ_G-algebras.

Suppose $G = \mathfrak{P}\{Y|W\}$ is a group presentation with recursively unsolvable word problem, with two generators, say $Y = \{x_1, x_2\}$, and a finite set W of relations, assumed to have form $w_j(x_1, x_2) = 1$ for τ_G-polynomials $w_j(x_1, x_2)$, $j = 1, 2, \ldots, t$. Define $\xi: P(Y, \tau_G) \longrightarrow P(Y, \tau_A)$ recursively by $\xi(x_1) = x_1$, $\xi(x_2) = x_2$, $\xi(1) = x_1 x_1^{\#}$ $\xi(uv) = \xi(u)\xi(v)$ and $\xi(u^{-1}) = \xi(u)^{\#}$. We consider additive relation algebra presentations $\mathfrak{V}_0\{Y|\Delta\}$, where $\mathfrak{V}_0$ is a quasivariety contained in the variety $\mathfrak{V}_A$ of all additive relation algebras and Δ is $\{e_1 = e_2\}$, with

$$e_1 = x_1 x_1^{\#} \wedge x_1^{\#} x_1 \wedge x_2 x_2^{\#} \wedge x_2 x_2^{\#} \wedge \xi(w_1) \wedge \xi(w_2) \wedge \ldots \wedge \xi(w_t) \text{ and}$$

$$e_2 = x_1 x_1^{\#} \vee x_1^{\#} x_1 \vee x_2 x_2^{\#} \vee x_2 x_2^{\#} \vee \xi(w_1) \vee \xi(w_2) \vee \ldots \vee \xi(w_t).$$

Note that $e_1 = e_2$ is equivalent to equality of all the terms $x_1 x_1^{\#}$, $x_1^{\#} x_1$, $x_2 x_2^{\#}$, $x_2^{\#} x_2$, $\xi(w_1)$, $\xi(w_2)$, ..., $\xi(w_t)$.

Given a sufficiently large quasivariety $\mathfrak{V}_0 \subseteq \mathfrak{V}_A$, the (two generator and one relation) presentation above will have a recursively unsolvable word problem for $\mathfrak{V}_0$.

8.2. Proposition. Suppose R is a nontrivial ring with unit and M is a free R-module with infinite free generating set $B = \{b_1, b_2, b_3, \ldots\}$. If $\mathfrak{V}_0$ is a quasivariety of additive relation algebras ($\mathfrak{V}_0 \subseteq \mathfrak{V}_A$) such that $\mathrm{Rel}_*(M)$ is in $\mathfrak{V}_0$, then $\mathfrak{V}_0\{Y|\Delta\}$ has a recursively unsolvable word problem.

Proof: Assume the hypotheses, and consider the diagram:

$$\begin{array}{ccccc} P(Y,\tau_G) & \xrightarrow{\xi} & P(Y,\tau_A) & & \\ \eta\downarrow & & \downarrow\eta_0 & & \\ G & \xrightarrow[\mu]{} & A & \xrightarrow[\nu]{} & \mathrm{Rel}_*(M) \end{array}$$

Here, $G = \mathfrak{P}\{Y|W\}$, $A = \mathfrak{V}_0\{Y|\Delta\}$, η is the canonical τ_G-homomorphism onto G, and η_0 is the canonical τ_A-homomorphism onto A. Defining ξ as in 8.1, calculation shows that the image of $\xi\eta_0$ is a subset of A which is a group generated by Y under the operations $\langle \cdot, {}^{\#}, x_1 x_1^{\#} \rangle$, and that the relations of W are satisfied in this group. Therefore, there exists a unique group homomorphism preserving x_1 and x_2 from G into this image, and this homomorphism can be regarded as a function $\mu: G \longrightarrow A$ such that $\eta\mu = \xi\eta_0$.

Clearly G is denumerably infinite, say with enumeration $G = \{g_1, g_2, g_3, \ldots\}$. Consider the group monomorphism $\nu_0 : G \longrightarrow Aut(B)$ defined by $\nu_0(g_k)(b_i) = b_j$ iff $g_i g_k = g_j$ for $i,j,k \geq 1$, which is a Cayley representation of G in the permutation group of B. Since B freely generates M, $\nu_0(g_k)$ determines a unique R-linear map $M \longrightarrow M$, and we let $\nu_1(g_k)$ denote its graph in $Rel_*(M)$, $k \geq 1$. For the τ_A-homomorphism $\eta_1 : P(Y,\tau_A) \longrightarrow Rel_*(M)$ such that $\eta_1(x_j) = \nu_1(x_j)$ for $j = 1,2$, we can show that $\eta_1(e_1) = \eta_1(e_2)$, since both equal 1 in Rel(M). Now $Rel_*(M)$ is in $\mathfrak{V}_0$, so there exists a τ_A-homomorphism ν from A into $Rel_*(M)$ such that $\eta_0\nu = \eta_1$. Calculation shows that $\nu(\mu(g)) = \nu_1(g)$ for all g in G, and it follows that $\mu\nu$ is one-one.

Since $\mu\nu$ is one-one, so is μ. So, $\eta(p) = \eta(q)$ iff $\eta_0(\xi(p)) = \eta_0(\xi(q))$ for $\langle p,q\rangle$ in $P(Y,\tau_G)^2$. But $\eta(p) = \eta(q)$ is not a recursively computable predicate on $P(Y,\tau_G)^2$ since G has recursively unsolvable word problem. Since ξ is recursively computable, it follows that the predicate $\eta_0(u) = \eta_0(v)$ for $\langle u,v\rangle$ in $P(Y,\tau_A)^2$ is not recursively computable. Therefore, $\mathfrak{V}_0\{Y|\Delta\}$ has a recursively undecidable word problem. ∎

8.3. Corollary. For any nontrivial ring R, there is no recursive decision procedure for membership in any of $\mathfrak{U}_A(R)$, $\mathfrak{U}_B(R)$, $\mathfrak{U}_L(R)$, $\mathfrak{U}_{AC}(R)$ and $\mathfrak{U}_{RC}(R)$. That is, we can not recursively decide whether an arbitrary basic universal Horn sentence is true for R-modules in any of these five theories.

Proof: By Proposition 8.2, we can't even recursively compute the predicate on pairs $\langle u,v\rangle$ in $P(Y,\tau_A)^2$ which is true iff

$$(\forall x_1, x_2)((e_1 = e_2) \Rightarrow (u = v))$$

is satisfied for all additive relation algebras in $\mathfrak{A}(R)$. This proves the result for $\mathfrak{U}_A(R)$, and the remaining cases follow immediately by using the recursive basic universal Horn sentence translation functions of 6.4. ∎

The above result is the main point of this section. These unsolvability results can be sharpened or applied in a number of ways. We conclude with two such improvements, from [ ] and [ ].

8.4. Proposition. Suppose R is a nontrivial ring with unit and M is a free R-module with infinitely many free generators. Let $\mathcal{L}_0$ be any quasivariety of lattices which contains Su(M). Then there is a lattice presentation with five generators and one relation which has a recursively unsolvable word problem for $\mathcal{L}_0$. This presentation is defined independently of the choice of R and $\mathcal{L}_0$.

8.5. Proposition. Given a finite commutative abelian category diagram with specified exactness relations, there is no general procedure for computing whether a given pair of diagram maps must be exact (as a consequence of the specified commutative diagram structure and exactness hypotheses).

§9. Division of Elements Corresponding to Integers in a Ring.

For each ring R, there is a unique ring homomorphism preserving the unit from the ring of integers into R. Elements in the image of this homomorphism are either 0, or sums $1+1+\ldots+1$ of the ring unit (one or more terms), or negatives of such sums. In this section, we investigate the properties of these elements, especially their division properties. Our treatment is adapted from [TISL, §2].

9.1. Definitions and Properties. Let **Z** denote the ring of integers, and let $\zeta_R: \mathbf{Z} \longrightarrow R$ denote the unique ring homomorphism preserving 1, for any ring R with unit. Elements of $\zeta_R[\mathbf{Z}]$ are called **Z**-*images* in R. For n in **Z** and r in R, let $n \cdot r$ denote $\zeta_R(n)r$ in R. For integers m and n and a ring R, $\mathrm{Div}_R(m,n)$ denotes the predicate

$$(\exists r)(r \in R \;\&\; m \cdot r = n \cdot 1)$$

on $\mathbf{Z} \times \mathbf{Z}$. That is, $\mathrm{Div}_R(m,n)$ holds if $\zeta_R(m)$ divides $\zeta_R(n)$ (on the left) in R. Let **Z**(d) denote the ring of integers modulo d for $d \geq 1$, as usual. Note that we allow the trivial ring **Z**(1).

9.1a. For each n in **Z**, $\zeta_R(n) = n \cdot 1$ and $\zeta_R(n)$ is a central element of R, so division on the left is equivalent to division on the right for **Z**-images. Note also that $\zeta_R(n)^{-1}$ is a central element of R if $\zeta_R(n)$ is invertible in R.

9.1b. R is a **Z**-algebra under the scalar multiplication $n \cdot r$, with $0 \cdot r = 0$, $n \cdot r = r + r + \ldots + r$ (n times) if $n \geq 1$, and $n \cdot r = -(r + r + \ldots + r)$ ($|n|$ times) if $n \leq -1$. Recall the usual identities: $mn \cdot r = m \cdot (n \cdot r)$, $(m+n) \cdot r = m \cdot r + n \cdot r$, $m \cdot (r+s) = m \cdot r + m \cdot s$, $1 \cdot r = r$ and $n \cdot rs = (n \cdot r)s = r(n \cdot s)$, for m and n in **Z** and r and s in R.

9.1c. If R has zero characteristic, then ζ_R is one-one and all the **Z**-images $n \cdot 1$ are distinct. If R has nonzero characteristic $d \geq 1$, then $n \cdot 1 = m \cdot 1$ in R iff $n \equiv m \pmod{d}$.

9.1d. For R a ring and integers m and n, $\mathrm{Div}_R(m,n)$ is true iff $\mathrm{Div}_R(|m|,|n|)$ is true. If m divides n in **Z**, then $\mathrm{Div}_R(m,n)$ is always true. In particular,

$Div_R(m,0)$ is always true. If $n \neq 0$, then $Div_R(0,n)$ is true iff R has nonzero characteristic d such that d divides n in **Z**.

When R has a nonzero characteristic $d \geq 1$, then the **Z**-image divisibility predicate $Div_R(m,n)$ is computable from d.

9.2. Proposition. Suppose R is a ring with characteristic $d \geq 1$. For m and n in **Z**, $m \cdot 1$ divides $n \cdot 1$ in R iff the g.c.d. of d and m divides n in **Z**.

Proof: Assume the hypotheses, so $d \cdot 1 = 0$. Let c be the g.c.d. of d and m, so there are x, y, z and w in **Z** such that $cx = d$, $cy = m$ and $c = dz + mw$.

Suppose $m \cdot 1$ divides $n \cdot 1$, say $m \cdot r = n \cdot 1$ for some r in R. If c doesn't divide n, then $n = sc + t$ for some s in **Z** and t with $0 < t < c$. Therefore, $0 < tx < cx = d$ and $tx \cdot 1 = (n - sc)x \cdot 1 = nx \cdot 1 - sd \cdot 1 = nx \cdot 1 = xm \cdot r = xcy \cdot r = dy \cdot r = 0$. But if $tx \cdot 1 = 0$, then d is not the characteristic of R. This contradiction proves that c divides n.

Now suppose c divides n, say $n = cv$ in **Z**. Then $(m \cdot 1)(wv \cdot 1) = mwv \cdot 1 = (c - dz)v \cdot 1 = cv \cdot 1 = n \cdot 1$, so $m \cdot 1$ divides $n \cdot 1$ in R. ■

9.3. Corollary. Suppose R is a ring with characteristic $d \geq 1$, and $S = \mathbf{Z}(d)$. Then $Div_R(m,n)$ is equivalent to $Div_S(m,n)$ for all integers m and n.

For rings R with characteristic zero, divisibility of **Z**-images can be determined for all integers if it is known when $p^{k+1} \cdot 1$ divides $p^k \cdot 1$, for all primes p and $k \geq 0$. For each prime p, we need only determine the smallest nonnegative integer k such that $Div_R(p^{k+1},p^k)$ is true, if there is such a k.

9.4. Definitions and Properties. Let $\mathbf{N}[0,\infty]$ denote the chain (totally ordered set) consisting of the nonnegative integers $\{n: n \geq 0\}$, ordered as usual, together with a maximum element denoted by ∞. Note that $\mathbf{N}[0,\infty]$ is a complete lattice, with $\sup Y = \infty$ for $Y \subseteq \mathbf{N}[0,\infty]$ iff $\infty \in Y$ or Y is an infinite set.

If p is a prime and R is a ring, let the p-*degree* of R, denoted by $dgr_R(p)$ or dgr(p,R), be the smallest integer k in $\mathbf{N}[0,\infty]$ such that $Div_R(p^{k+1},p^k)$ is

true, with $dgr_R(p) = \infty$ if there is no such k.

If p is prime and $n \neq 0$ in **Z**, the p-*exponent* of n, denoted by $expt_n(p)$, is the largest integer k such that p^k divides n in **Z**. Note that $expt_{-n}(p) = expt_n(p)$.

9.4a. Suppose R is a ring and p is prime. For $i,j \geq 0$ in **Z**, $Div_R(p^i,p^j)$ is true iff $i \leq j$ or $dgr_R(p) \leq j$. (Since $Div_R(p^i,p^j)$ is true for $i \leq j$ by 9.1d, assume $i > j$. If $p^i \cdot s = p^j \cdot 1$ for some s in R, then $p^{j+1} \cdot t = p^j \cdot 1$ for $t = p^{i-j-1} \cdot s$, so $dgr_R(p) \leq j$. If $dgr_R(p) \leq j$, say $p^{k+1} \cdot r = p^k \cdot 1$ in R for $k = dgr_R(p)$, then $p^i \cdot u = p^j \cdot 1$ for $u = r^{i-j}$.)

9.4b. Suppose R is a ring, p is prime, and $dgr_R(p) = k < \infty$. Then the maximum p-height possible for an R-module element is k. (Note that 1 in ${}_RR/p^kR$ has p-height k, since $p^{k-1} \cdot 1$ in p^kR implies $dgr_R(p) < k$. If $j > k$ and $(p^j \cdot 1)v = 0$ for v in ${}_RM$, then $(p^k \cdot 1)v = 0$ because $p^j \cdot 1$ divides $p^k \cdot 1$ in R.) If $dgr_R(p) = \infty$, then R-modules may have elements with arbitrarily large p-heights j (such as 1 in ${}_RR/p^jR$).

9.4c. If R has characteristic $d \geq 1$, then $dgr_R(p) = expt_d(p)$ for all primes p (apply 9.2). In this case, $dgr_R(p)$ is 0 except for at most finitely many primes p, and $dgr_R(p)$ is never ∞.

9.4d. For p prime, $dgr_R(p) = 0$ iff $p \cdot 1$ is an invertible element of R.

For rings R with characteristic zero, $Div_R(m,n)$ is true if $n = 0$ and false if $m = 0$ and $n \neq 0$. The other cases are shown in the next result.

9.5. Proposition. Suppose R is a ring with characteristic zero, and m and n are nonzero integers. Then the following conditions are equivalent:

9.5a. $Div_R(m,n)$ is true, that is, $m \cdot 1$ divides $n \cdot 1$ in R.

9.5b. For each prime p dividing m, $expt_m(p) > expt_n(p)$ implies that $dgr_R(p) \leq expt_n(p)$.

9.5c. For each prime p, if $i = expt_m(p)$ and $j = expt_n(p)$, then $p^i \cdot 1$ divides $p^j \cdot 1$ in R.

Proof: Assume 9.5a, so $m \cdot r = n \cdot 1$ for some r in R. Suppose $i = expt_m(p) > expt_n(p) = j$ for p prime, so $m = p^{j+1}x$ and $n = p^jy$ for x and y in **Z**, and y is

not divisible by p. Then $pa + yb = 1$ for some a and b in $\mathbf{Z}$, so $bm \cdot r = bn \cdot 1 = p^j yb \cdot 1 = p^j(1 - pa) \cdot 1 = p^j \cdot 1 - p^{j+1}a \cdot 1$ in R. Therefore, $p^{j+1} \cdot t = p^j \cdot 1$ for $t = xb \cdot r + a \cdot 1$ in R, and $j \geq dgr_R(p)$. This proves 9.5a $\Rightarrow$ 9.5b.

Assume 9.5b, and let $i = expt_m(p)$ and $j = expt_n(p)$ for p prime. If p doesn't divide m, then $i = 0 \leq j$ and $Div_R(p^i, p^j)$ is true by 9.4a. If p divides m, then either $i \leq j$, or $i > j$ and so $dgr_R(p) \leq j$ by 9.5b. Hence $Div_R(p^i, p^j)$ is true in all cases by 9.4a. Therefore, 9.5b $\Rightarrow$ 9.5c.

Assuming 9.5c, there exists r such that $m \cdot r = n \cdot 1$ (use 9.1a and the prime power factorizations of m and n). Therefore, 9.5c $\Rightarrow$ 9.5a. ∎

Based on 9.2 and 9.5, we will develop a unified approach to $\mathbf{Z}$-image divisibility conditions for all rings.

9.6. Definitions and Properties. Let Pr denote the set of all primes. A p-*degree function* is any function $f: Pr \longrightarrow \mathbf{N}[0,\infty]$, and $\mathbf{N}[0,\infty]^{Pr}$ denotes the set of all p-degree functions. Order p-degree functions pointwise: $f \leq g$ iff $f(p) \leq g(p)$ for all primes p. A p-degree function g such that $g(p) \neq \infty$ for all primes p and $g(p) = 0$ for all but finitely many primes p is said to have *finite height*. A p-degree function h such that $h(p) = \infty$ except for at most finitely many primes p is said to be ∞-*cofinite*.

For $n \neq 0$, let $expt_n$ denote the p-degree function $p \longmapsto expt_n(p)$. Define p-degree functions $div_{m,n}$ for integers m and n as follows: If $n = 0$, then $div_{m,n}(p) = \infty$ for all primes p. If $n \neq 0$ and $m = 0$, then $div_{m,n} = expt_n$. For nonzero m and n and p prime:

$$div_{m,n}(p) = \begin{cases} expt_n(p) & \text{if } expt_m(p) > expt_n(p), \\ \infty & \text{if } expt_m(p) \leq expt_n(p). \end{cases}$$

9.6a. Under pointwise order, $\mathbf{N}[0,\infty]^{Pr}$ is a complete distributive lattice (a denumerable product of chains $\mathbf{N}[0,\infty]$). Arbitrary meets and joins are also computed pointwise.

9.6b. The set of all p-degree functions g of finite height is an ideal of the lattice $\mathbf{N}[0,\infty]^{Pr}$. A p-degree function g has finite height iff the subset

$\{f: f \le g\}$ of $\mathbf{N}[0,\infty]^{Pr}$ is finite iff $\sum_{p \in Pr} g(p)$ is finite. For $n \neq 0$, $expt_n$ is a p-degree function of finite height, hence so is $div_{0,n}$. The function $n \longmapsto expt_n$ is a one-one correspondence between the positive integers and the set of p-degree functions of finite height. The reciprocal function takes g to $\prod_{p \in Pr} p^{g(p)}$, a form of the prime power factorization of an integer n if g has finite height. If R has characteristic $d \ge 1$, then $dgr_R = expt_d$ by 9.2. For nonzero m and n, m divides n in $\mathbf{Z}$ iff $expt_m \le expt_n$ in $\mathbf{N}[0,\infty]^{Pr}$.

9.6c. The set of all ∞-cofinite p-degree functions h is a dual ideal of $\mathbf{N}[0,\infty]^{Pr}$. The functions $div_{m,n}$ are ∞-cofinite, except for the finite height case $m = 0$ and $n \neq 0$ of 9.6b. For every ∞-cofinite p-degree function h, there exist integers $m,n \ge 1$ such that $div_{m,n} = h$. (Apply 9.5, using

$$m = \prod_{p \in J} p^{h(p)+1} \text{ and } n = \prod_{p \in J} p^{h(p)} \text{ for } J = \{p \in Pr: h(p) < \infty\}.$$

If J is empty, let $m = n = 1$.)

It is useful to define a lattice incorporating all the patterns of Z-image divisibility that are possible for a ring.

9.7. Definitions and Properties. Suppose R is a ring with unit. Let $\{\mathbf{0},\mathbf{I}\}$ denote the two element lattice with $\mathbf{0} < \mathbf{I}$, let $zchar_R = \mathbf{0}$ if R has nonzero characteristic, and let $zchar_R = \mathbf{I}$ if R has zero characteristic. Define

$$\mathcal{J} = \{\langle x,f\rangle: x \in \{\mathbf{0},\mathbf{I}\},\ f:Pr \longrightarrow \mathbf{N}[0,\infty],\ x = \mathbf{0} \Rightarrow f \text{ has finite height}\}.$$

(Using 9.7 through 9.10, we will see that $\mathcal{J}$ is exactly the set of pairs of form $\langle zchar_R, dgr_R\rangle$, and that such a pair completely determines the Z-image divisibility pattern of R.)

9.7a. $\mathcal{J}$ is a sublattice, in fact a lattice ideal, of the distributive product lattice $\{\mathbf{0},\mathbf{I}\} \times \mathbf{N}[0,\infty]^{Pr}$, and $\mathcal{J}$ is complete. Joins of infinite subsets of $\mathcal{J}$ are not necessarily the same in $\mathcal{J}$ as in $\{\mathbf{0},\mathbf{I}\} \times \mathbf{N}[0,\infty]^{Pr}$ (consider $\{\langle \mathbf{0},f\rangle$: f has finite height$\}$). Infinite meets are the same.

9.7b. If R is a ring with unit, then $\langle zchar_R, dgr_R\rangle$ is in $\mathcal{J}$ (9.4c). For all integers m and n, $Div_R(m,n)$ is true iff:

$$dgr_R \le div_{m,n} \text{ and (if } m = 0 \text{ and } n \neq 0, \text{ then } zchar_R = \mathbf{0}).$$

(Use 9.1d, 9.2, 9.4c and 9.5.)

9.7c. Suppose R and S are rings with unit. Then $Div_S(m,n)$ implies $Div_R(m,n)$ for all integers m and n iff

$$\langle zchar_R, dgr_R\rangle \le \langle zchar_S, dgr_S\rangle \text{ in } \mathcal{J}.$$

(As in 7.1, *smaller* rings satisfy *more* formulas.)

9.7d. R has nonzero characteristic $d \ge 1$ iff $\langle zchar_R, dgr_R\rangle = \langle \mathbf{0}, expt_d\rangle$. If $zchar_R = \mathbf{0}$ and $dgr_R = f$, then the characteristic of R is $\prod_{p\in Pr} p^{f(p)}$, which is an integer by 9.6b because f has finite height.

9.7e. Suppose R is a ring with unit, M is an R-module, and $dgr_R(p) = k < \infty$ for a prime p. Then $Im\ p^j\cdot 1_M = Im\ p^k\cdot 1_M$ and $Ker\ p^j\cdot 1_M = Ker\ p^k\cdot 1_M$ for all $j \ge k$. If R is commutative and S is the ring of endomorphisms of M, then $\langle zchar_S, dgr_S\rangle \le \langle zchar_R, dgr_R\rangle$. (If $p^{k+1}\cdot r = p^k\cdot 1$ in R, then $p^{k+1}\cdot s = p^k\cdot 1$ in S, where $s(v) = rv$ for all v in M. If $zchar_R = \mathbf{0}$, then the characteristic of S divides the characteristic of R, and we can use 9.6b and 9.7d.)

In Corollary 9.3, we showed that the particular rings $\mathbf{Z}(d)$ displayed all the patterns of divisibility of $\mathbf{Z}$-images possible for arbitrary rings with nonzero characteristic. We can also construct particular rings of zero characteristic with all the possible patterns of $\mathbf{Z}$-image divisibility for arbitrary rings with zero characteristic.

9.8. Definitions and Properties. Let $\mathbf{Q}$ denote the field of rational numbers, and let $\mathbf{Q}_p$ denote the subring of $\mathbf{Q}$ consisting of fractions m/n in lowest terms such that p doesn't divide n. Recall also the rings $\mathbf{Z}(d) = \mathbf{Z}/d\mathbf{Z}$ for $d \ge 1$.

9.8a. For all primes p and q, $dgr(p,\mathbf{Z}(q^k))$ is k if $q = p$ and is 0 if $q \ne p$ (use 9.4c).

9.8b. For all primes p and q, $dgr(p,\mathbf{Q}_p)$ is ∞ if $q = p$ and is 0 if $q \ne p$. Note that $dgr(p,\mathbf{Z}) = \infty$ and $dgr(p,\mathbf{Q}) = 0$ for all primes p.

9.8c. Suppose $\{R_j: j \in J\}$ is a (possibly infinite) set of rings with unit, and R is the product ring $\prod_{j\in J} R_j$. Then

$$dgr(p,R) = \sup\{dgr(p,R_j): j \in J\} \text{ in } \mathbf{N}[0,\infty]$$

for all primes p.

9.9. Definitions and Properties. For a p-degree function f and p prime, define the rings

$$S_f(p) = \begin{cases} \mathbf{Z}(p^{f(p)}) & \text{if } f(p) < \infty, \\ \mathbf{Q}_p & \text{if } f(p) = \infty. \end{cases}$$

For each pair $\langle x,f \rangle$ in $\mathcal{J}$, define the product ring

$$S(x,f) = \begin{cases} \prod_{p \in Pr} S_f(p) & \text{if } x = \mathbf{0}, \\ \mathbf{Q} \times \prod_{p \in Pr} S_f(p) & \text{if } x = \mathbf{I}. \end{cases}$$

For $x = \mathbf{0}$, f has finite height, so all but finitely many factors $S_f(p)$ are trivial rings $\mathbf{Z}(1)$.

9.9a. Suppose $\langle x,f \rangle$ is in $\mathcal{J}$ and $S = S(x,f)$. Then S is a commutative ring, with nonzero characteristic $\prod_{p \in Pr} p^{f(p)}$ if $x = \mathbf{0}$ and zero characteristic if $x = \mathbf{I}$ (the factor $\mathbf{Q}$ forces zero characteristic for $S(\mathbf{I},f)$ when f has finite height). For all primes p, $f(p) = dgr(p,S(x,f))$ (use 9.8a,b,c). Therefore, $\langle zchar_S, dgr_S \rangle = \langle x,f \rangle$.

By 9.7b and 9.9a, there is a one-one correspondence between members of $\mathcal{J}$ and $\mathbf{Z}$-image divisibility patterns for rings. The significance of the order in $\mathcal{J}$ is shown by 9.7c. Note that $S(\mathbf{0},f)$ is isomorphic to $\mathbf{Z}(d)$ if $f = expt_d$, so that the case $x = \mathbf{0}$ below is essentially a restatement of 9.3 using 9.7d.

9.10. Corollary. For each ring R, $\langle zchar_R, dgr_R \rangle$ is the unique member $\langle x,f \rangle$ of $\mathcal{J}$ such that for $S = S(x,f)$, $Div_R(m,n)$ is equivalent to $Div_S(m,n)$ for all integers m and n.

For R with nonzero characteristic, we know that $Div_R(m,n)$ is recursively computable as a predicate on $\mathbf{Z} \times \mathbf{Z}$ by 9.2. For characteristic zero, the analysis is given next.

9.11. Proposition. Suppose R has characteristic zero. Then $Div_R(m,n)$ is a recursively computable predicate on $\mathbf{Z} \times \mathbf{Z}$ iff $dgr_R(p) \leq k$ is a recursively computable predicate for primes p and integers $k \geq 0$. In particular,

$Div_R(m,n)$ is recursively computable if dgr_R is a recursive p-degree function.

Proof: Since $dgr_R(p) \leq k$ is equivalent to $Div_R(p^{k+1},p^k)$, the forward implication of the first part follows. The reverse implication of the first part follows from 9.5, and the second part is clear. ■

The criteria of 9.11 are distinct, since dgr_R may not be a recursive function even if $dgr_R(p) \leq k$ is a recursive predicate.

9.12. Example. Define a recursive function β on the nonnegative integers such that the set of primes in Im β is not recursive. Let $f(p) = k$ for p prime if k is the smallest integer such that $\beta(k) = p$, with $f(p) = \infty$ if there is no such k, and let $R = S(I,f)$. Then $dgr_R(p) \leq k$ is decidable, since it is true iff one or more of $\beta(1),\beta(2),\ldots,\beta(k)$ is equal to p. However, dgr_R is not a recursive function because the inverse image of $\{\infty\}$ contains p iff it is in the complement of the image of β, and this set of primes is not recursively enumerable by hypothesis.

There are two special classes of rings of some interest.

9.13. Corollary. Suppose R is a von Neumann regular ring of characteristic zero. Then $Div_R(m,n)$ is a recursively computable predicate iff the set of primes p such that $p\cdot 1$ is invertible in R is recursive.

Proof: For each prime p, there exists t in R such that $(p\cdot 1)t(p\cdot 1) = p\cdot 1$, by hypothesis. So, $dgr_R(p) \in \{0,1\}$ for all primes p by 9.1a,b, and the result then follows from 9.4d and 9.11. ■

9.14. Corollary. Suppose R is a torsion-free ring. Then $Div_R(m,n)$ is a recursively computable predicate iff the set of primes p such that $p\cdot 1$ is invertible in R is recursive.

Proof: If $k = dgr_R(p)$ and $0 < k < \infty$, then $Div_R(p^{k+1},p^k)$ implies that $p^k\cdot(p\cdot t - 1) = 0$ for some t in R, and $p\cdot t - 1 \neq 0$ because $Div_R(p^1,p^0)$ is false. So, $dgr_R(p) \in \{0,\infty\}$ if R is torsion-free, and the result again follows from 9.4d and 9.11. ■

Observe that $S(x,f)$ is a (possibly trivial) regular ring iff $f(p) \in \{0,1\}$ for all primes p. Similarly, $S(x,f)$ is a (nontrivial) torsion-free ring iff $x = \mathbf{I}$ and $f(p) \in \{0,\infty\}$ for all primes p.

From previous analysis, we can show that a conjunction of finitely many **Z**-image divisibility conditions is always equivalent to a single **Z**-image divisibility condition. This reduction is recursively computable, and does not depend upon the choice of the ring.

9.15. Proposition. Suppose $m_1,m_2,\ldots,m_k$ and $n_1,n_2,\ldots,n_k$ are integers. Then there exist $m \geq 0$ and $n \geq 1$, recursively computable from $m_1,m_2,\ldots,m_k$ and $n_1,n_2,\ldots,n_k$, such that for all rings R,

$\mathrm{Div}_R(m,n)$ is true iff $\mathrm{Div}_R(m_j,n_j)$ is true for $j = 1,2,\ldots,k$.

Proof: Let $h_j = \mathrm{div}_{m_j,n_j}$ for $j = 1,2,\ldots,k$, and let $h = h_1 \wedge h_2 \wedge \ldots \wedge h_k$ in $\mathbf{N}[0,\infty]^{Pr}$. Suppose $m_i = 0$ and $n_i \neq 0$ for some $i \leq k$. By 9.6b, h_i has finite height, so h has finite height since $h \leq h_i$, so $h = \mathrm{expt}_n$ for some $n \geq 1$. If R has characteristic d, it follows from 9.7b that $\mathrm{Div}_R(0,n)$ is true iff ($\mathrm{dgr}_R \leq h$ and $d \neq 0$) iff ($\mathrm{dgr}_R \leq h_j$ for $j \leq k$ and $d \neq 0$) iff $\mathrm{Div}_R(m_j,n_j)$ is true for $j \leq k$.

Suppose there is no such $i \leq k$. By 9.6c, h_i is ∞-cofinite for all $i \leq k$, so h is ∞-cofinite, and so $h = \mathrm{div}_{m,n}$ for some $m,n \geq 1$. By 9.7b again, $\mathrm{Div}_R(m,n)$ holds iff $\mathrm{dgr}_R \leq h$ iff $\mathrm{dgr}_R \leq h_j$ for $j \leq k$ iff $\mathrm{Div}_R(m_j,n_j)$ is true for $j \leq k$.

In Appendix F, we give an algorithm for computing such an m and n from $m_1,m_2,\ldots,m_k$ and $n_1,n_2,\ldots,n_k$, based on 9.6b,c and 9.7b. ■

Now consider nonhomogeneous systems of linear equations with **Z**-image coefficients in a ring R. That is, given integers a_{ij} and v_i for $i = 1,2,\ldots,s$ and $j = 1,2,\ldots,t$, we ask whether there exist elements (not necessarily **Z**-images) $r_1,r_2,\ldots,r_t$ in R satisfying the equations:

$$\begin{aligned} a_{11}\cdot r_1 + a_{12}\cdot r_2 + \cdots + a_{1t}\cdot r_t &= v_1\cdot 1,\\ a_{21}\cdot r_1 + a_{22}\cdot r_2 + \cdots + a_{2t}\cdot r_t &= v_2\cdot 1,\\ \vdots \qquad\quad \vdots \qquad\quad & \qquad\quad \vdots \qquad\quad \vdots\\ a_{s1}\cdot r_1 + a_{s2}\cdot r_2 + \cdots + a_{st}\cdot r_t &= v_s\cdot 1, \end{aligned}$$

(Recall that $a_{ij}\cdot r_j = \zeta_R(a_{ij})r_j$ and $v_i\cdot 1 = \zeta_R(v_i)$.) Now, the solvability of a 1 by 1 system is just a **Z**-image divisibility condition $\mathrm{Div}_R(a_{11},v_1)$. If $A = [a_{ij}]$ is an $s\times t$ *diagonal* matrix and $k = \min\{s,t\}$, then the solvability of the system is a conjunction of terms $\mathrm{Div}_R(a_{ii},v_i)$ for $i \le k$ and $\mathrm{Div}_R(0,v_i)$ for $k < i \le s$. Using standard techniques of integer matrix diagonalization and 9.15, we can reduce any nonhomogeneous system of linear equations of the form displayed above to an equivalent single **Z**-image divisibility condition $\mathrm{Div}_R(m,n)$. We will see that m and n can be recursively computed from the integers a_{ij} and v_i, independently of the choice of the ring R.

9.16. Definitions and Properties. For R a ring with unit and positive integers s and t, $\mathfrak{M}_{s,t}(R)$ denotes the set of $s\times t$ matrices with coefficients in R. The set of $s\times s$ matrices on R is denoted by $\mathfrak{M}_s(R)$ also.

If $A = [a_{ij}]$ is an $s\times t$ integer matrix (in $\mathfrak{M}_{s,t}(\mathbf{Z})$), let $A_R = [\zeta_R(a_{ij})]$ in $\mathfrak{M}_{s,t}(R)$, an $s\times t$ matrix of **Z**-images in R.

9.16a. For any ring R with unit, $\mathfrak{M}_s(R)$ is a ring with unit $I_s = [\delta_{ij}]$ (Kronecker delta) under the usual matrix sum and product. Also, $\mathfrak{M}_{s,t}(R)$ is a left-$\mathfrak{M}_s(R)$, right-$\mathfrak{M}_t(R)$ bimodule under matrix sum and product.

9.16b. If A and B are in $\mathfrak{M}_{s,t}(\mathbf{Z})$ and C is in $\mathfrak{M}_{t,u}(\mathbf{Z})$, then $(A+B)_R = A_R + B_R$ and $(BC)_R = B_RC_R$. Also, $(I_s)_R$ is the ring unit of $\mathfrak{M}_s(R)$, so that $A \mapsto A_R$ determines a ring homomorphism $\mathfrak{M}_s(\mathbf{Z})\longrightarrow\mathfrak{M}_s(R)$ preserving the ring unit. If B is an invertible element of $\mathfrak{M}_s(\mathbf{Z})$, then B_R is invertible in $\mathfrak{M}_s(R)$ with $(B_R)^{-1} = (B^{-1})_R$.

The following matrix diagonalization result was given at least as early as 1879 by Frobenius, and perhaps even earlier in a form like the one below.

9.17. Proposition. Given an $s\times t$ integer matrix A, there exist an $s\times s$ integer matrix B and a $t\times t$ integer matrix C such that B^{-1} exists in $\mathfrak{M}_s(\mathbf{Z})$,

C^{-1} exists in $\mathfrak{M}_t(\mathbf{Z})$, and $D = [d_{ij}] = BAC$ is an $s \times t$ diagonal matrix (that is, $d_{ij} = 0$ if $i \neq j$). Furthermore, such B, C and D are recursively computable from A.

The reduction of each nonhomogeneous system of linear equations to a single **Z**-image divisibility condition can now be verified.

9.18. Proposition. Suppose $A = [a_{ij}]$ in $\mathfrak{M}_{s,t}(\mathbf{Z})$ and $V = [v_i]$ in $\mathfrak{M}_{s,1}(\mathbf{Z})$, for $s,t \geq 1$. Then there exist integers $m \geq 0$ and $n \geq 1$, which are recursively computable from A and V, such that for all rings R, 9.18a is equivalent to $\mathrm{Div}_R(m,n)$.

9.18a. There exists Y in $\mathfrak{M}_{t,1}(R)$ such that $A_R Y = V_R$.

Proof: By 9.17, there exist B invertible in $\mathfrak{M}_s(\mathbf{Z})$ and C invertible in $\mathfrak{M}_t(\mathbf{Z})$ such that $BAC = D = [d_{ij}]$ is a diagonal matrix in $\mathfrak{M}_{s,t}(\mathbf{Z})$. Also, B and C are computable from A. Let $U = [u_i] = BV$ in $\mathfrak{M}_{s,1}(\mathbf{Z})$. For any ring R, consider the condition:

(*) There exists Y_0 in $\mathfrak{M}_{t,1}(R)$ such that $D_R Y_0 = U_R = B_R V_R$.

Since D is diagonal, (*) is true iff $\mathrm{Div}_R(d_{ii},u_i)$ holds for $i = 1,2,\ldots,s$, defining d_{ii} to be 0 if $t < i \leq s$. By 9.15, there exist $m \geq 0$ and $n \geq 1$ such that (*) is true iff $\mathrm{Div}_R(m,n)$ holds. Since d_{ii} and u_i for $i \leq s$ are recursively computable from A and V, so are m and n.

Assuming (*), let $Y = C_R Y_0$. Then $A_R Y = B_R^{-1} B_R A_R C_R Y_0 = B_R^{-1} D_R Y_0 = B_R^{-1} B_R V_R = V_R$, proving 9.18a. Conversely, assume 9.18a and let $Y_0 = C_R^{-1} Y$. Then $D_R Y_0 = B_R A_R C_R C_R^{-1} Y = B_R A_R Y = B_R V_R$, proving (*). Therefore, (*), 9.18a and $\mathrm{Div}_R(m,n)$ are all equivalent. ■

In Appendix F, computer programs are described for the recursively computable operations discussed here. There is a reasonably efficient polynomial-time computation of m and n from A and V as in 9.18, which is feasible if the dimensions s and t are not too large.