Discussiones Mathematicae
General Algebra and Applications 20 (2000) 43–49

ON DUALITY OF SUBMODULE LATTICES [1]

GÁBOR CZÉDLI AND GÉZA TAKÁCH

JATE Bolyai Institute
Aradi vértanúk tere 1, H–6720 Szeged, Hungary

e-mail: czedli@math.u-szeged.hu **e-mail:** takach@math.u-szeged.hu

Dedicated to the memory of George Hutchinson

Abstract

An elementary proof is given for Hutchinson's duality theorem, which states that if a lattice identity λ holds in all submodule lattices of modules over a ring R with unit element then so does the dual of λ.

Keywords: submodule lattice, lattice identity, duality.

1991 Mathematics Subject Classification: Primary 06C05, Secondary 08B10, 16D99.

Given a ring R, always with unit element $1 = 1_R$, the class of left modules over R is denoted by R–**Mod**. Let $T(R)$ denote the set of all lattice identities that hold in the submodule lattices of all R-modules, i.e., in the class of $\{\mathrm{Sub}(M) : M \in R\text{–}\mathbf{Mod}\}$. Using the heavy machinery of abelian category theory and Theorem 4 from [3], G. Hutchinson in [2] and [3] has proved the following duality result.

Main Theorem (G. Hutchinson). *For every ring R, $T(R)$ is a selfdual set of lattice identities. In other words, a lattice identity λ holds in $\{\mathrm{Sub}(M) : M \in R\text{–}\mathbf{Mod}\}$ iff so does the dual of λ.*

The goal of the present paper is to give an easy new proof of this theorem. Our elementary approach does not resort to category theory and uses much less from [3] than the original one.

[1]This research was partially supported by the NFSR of Hungary (OTKA), grant no. T023186 and T022867, and also by the Hungarian Ministry of Education, grant no. FKFP 1259/1997 and MKM KF 402/96.

Proof of the Main Theorem. Let λ be a lattice identity. Since $\mathrm{Sub}(M) \cong \mathrm{Con}(M)$ for every $M \in R$–**Mod** and R–**Mod** is a congruence permutable variety, by results of R. Wille ([5]) or A. Pixley [4] (cf. [3] for more details) there is a strong Mal'cev condition $U(\lambda)$ such that $\lambda \in T(R)$ is equivalent to the satisfaction of $U(\lambda)$ in R–**Mod**. Using the fact that each n-ary term $f(y_1, \ldots, y_n)$ in R–**Mod** can uniquely be written in the form $r_1y_1 + \ldots + r_ny_n$ with $r_1, \ldots, r_n \in R$, $U(\lambda)$ easily turns to a system of linear equations

$$Ay = b \cdot 1_R \tag{1}$$

where A is an integer matrix, b is a column vector with integer entries, and y is the column vector of ring variables (cf. [3] for concrete examples). So we obtain that

$$\lambda \in T(R) \text{ iff } Ay = b \cdot 1_R \text{ is solvable in } R. \tag{2}$$

We can easily infer from this observation that for any rings R_i $(i \in I)$ and their direct product we have

$$T\left(\prod_{i \in I} R_i\right) = \bigcap_{i \in I} T(R_i). \tag{3}$$

A classical matrix diagonalization method, due to Frobenius ([1], cf. also [3]), asserts that for any integer matrix A there exist invertible integer matrices B and C with integer inverses such that BAC is a diagonal matrix. Choosing B and C according to this result, multiplying (1) by B from the left and introducing the notations $M := BAC$, $z := C^{-1}y$, $c := Bb$ we easily conclude that the solvability of (1) in R is equivalent to the solvability of

$$Mz = c \cdot 1_R \tag{4}$$

in R. Now, for integers $m \geq 0$ and $n \geq 1$ let $D(m, n)$ denote the "divisibility condition" $(\exists x)(mx = n \cdot 1)$ where $mx = x + \ldots + x$ (m times) and 1 stands for the ring unit. The set $\{(m, n) : m \geq 0,\ n \geq 1, \text{ and } D(m, n) \text{ holds in } R\}$ will be denoted by $D(R)$. Since M in (4) is a diagonal matrix, the solvability of (4) in R depends only on $D(R)$. Hence, combining the previous assertions and (2), we conclude that

$$D(R) \text{ determines } T(R), \tag{5}$$

i.e., $D(R_1) = D(R_2)$ implies $T(R_1) = T(R_2)$. Clearly, for arbitrary rings R_i, $i \in I$,

$$D\left(\prod_{i\in I} R_i\right) = \bigcap_{i\in I} D(R_i). \tag{6}$$

Now we claim that for arbitrary rings R and R_i $(i \in I)$

$$\text{if } D(R) = \bigcap_{i\in I} D(R_i) \text{ then } T(R) = \bigcap_{i\in I} T(R_i). \tag{7}$$

Indeed, $\bigcap_{i\in I} T(R_i) = T(\prod_{i\in I} R_i)$ by (3). Since $D(\prod_{i\in I} R_i) = D(R)$ by (6) and the premise of (7), (5) yields $T(\prod_{i\in I} R_i) = T(R)$, proving (7).

For $k > 0$ let $\boldsymbol{Z}_k$ denote the factor ring of the ring $\boldsymbol{Z}$ of integers modulo k, and let $\boldsymbol{Z}_0 = \boldsymbol{Q}$, the field of rational numbers. We claim that, for any ring R,

$$D(R) = \bigcap \{D(\boldsymbol{Z}_k) : D(R) \subseteq D(\boldsymbol{Z}_k)\} \tag{8}$$

The proof of (8) will implicitly use the fact that for any integers $m \geq 0$, $n > 0$ and $k > 0$ the following equivalence holds:

$$(m,n) \in D(\boldsymbol{Z}_k) \iff \text{g.c.d.}(m,k) \mid n. \tag{9}$$

First we deal with the case when $k := \text{char }(R) > 0$. Here char (R) denotes $\min\{i : 0 < i \in \boldsymbol{Z} \text{ and } i \cdot 1_R = 0\}$, the characteristic of R, where $\min \emptyset$ is understood as 0. We assert that

$$D(R) = D(\boldsymbol{Z}_k), \tag{10}$$

which clearly yields (8) for char $R > 0$. The embedding $\boldsymbol{Z}_k \to R$, $x \cdot 1_{\boldsymbol{Z}_k} \mapsto x \cdot 1_R$ $(x \in \boldsymbol{Z})$ ensures that $D(\boldsymbol{Z}_k) \subseteq D(R)$. Now suppose that $(a,b) \notin D(\boldsymbol{Z}_k)$, i.e., $d := \text{g.c.d.}(a,k)$ does not divide b. Let $k = k_1 d$, $a = a_1 d$ and $b = qd + r$, $0 < r < d$. If we had $ax = b \cdot 1_R$ for some $x \in R$, then $0 = k(a_1 x) = k_1 a x = k_1 b \cdot 1_R = k_1 q d \cdot 1_R + k_1 r \cdot 1_R = k(q \cdot 1_R) + (k_1 r) \cdot 1_R = (k_1 r) \cdot 1_R$ would be a contradiction, for $k_1 r < k_1 d = k = \text{char }(R)$. Hence $(a,b) \notin D(R)$. This proves $D(R) = D(\boldsymbol{Z}_k)$, and (8) follows.

Now let us assume that char $(R) = 0$. Only the $\supseteq$ part of (8) has to be verified, so suppose

$$(m,n) \notin D(R),$$

$m \geq 0$ and $n > 0$; we have to show that (m,n) does not belong to the right-hand side of (8). Two cases will be distinguished.

Case 1. $m = 0$. Then $(m,n) \notin D(\boldsymbol{Z}_0)$, and $D(R) \subseteq D(\boldsymbol{Z}_0)$ clearly follows from the implication: $(a,b) \in D(R) \Longrightarrow a \neq 0$. Hence $(m,n) = (0,n)$ does not belong to the right-hand side of (8).

Case 2. $m > 0$. First we claim that for arbitrary $0 \leq a_1, \dots, a_t \in \boldsymbol{Z}$ and $1 \leq b_1, \dots, b_t \in \boldsymbol{Z}$ we have

$$(11) \qquad (a_1,b_1), \dots, (a_t,b_t) \in D(R) \Longrightarrow (a_1 \dots a_t, b_1 \dots b_t) \in D(R).$$

Indeed, if $a_1 r_1 = b_1 \cdot 1_R$ and $a_2 r_2 = b_2 \cdot 1_R$ for $r_1, r_2 \in R$, then $(a_1 a_2)(r_1 r_2) = a_2(a_1 r_1) r_2 = a_2(b_1 \cdot 1_R) r_2 = b_1(a_2 r_2) = b_1 b_2 \cdot 1_R$. This proves (11) for $t = 2$, whence it holds for $t > 2$ as well.

Now let $m = p_1^{f_1} \dots p_t^{f_t}$ and $n = p_1^{g_1} \dots p_t^{g_t}$ with pairwise distinct primes $p_1, \dots, p_t$ and nonnegative integers $f_1, \dots, f_t$, $g_1, \dots, g_t$. We infer from (11) that $(p_i^{f_i}, p_i^{g_i}) \notin D(R)$ for some $i \in \{1, \dots, t\}$. With the notations $p := p_i$, $f := f_i$, $g := g_i$ and $k := p^{g+1}$, $(p^f, p^g) \notin D(R)$ implies $f > g$. Hence $(m,n) \notin D(\boldsymbol{Z}_k)$, for $mx = 0 \neq n \cdot 1_{\boldsymbol{Z}_k}$ holds for all $x \in \boldsymbol{Z}_k$. Now, before showing that $\boldsymbol{Z}_k$ occurs on the right hand side of (8), let us observe that if (p^{g+1}, p^g) belonged to $D(R)$, then, choosing an $r \in R$ with $p^{g+1} r = p^g \cdot 1_R$, we could obtain $p^g \cdot 1_R = p^{g+1} r = p(p^g \cdot 1_R) r = p p^{g+1} r^2 = p^{g+2} r^2 = \dots = p^f r^{f-g}$, which would contradict $(p^f, p^g) \notin D(R)$. Therefore $(p^{g+1}, p^g) \notin D(R)$.

Now, to show $D(R) \subseteq D(\boldsymbol{Z}_k)$, let $(c,d) \notin D(\boldsymbol{Z}_k)$, $0 \leq c$, and $1 \leq d$; we have to show that $(c,d) \notin D(R)$. If $c = 0$ then $(c,d) \notin D(R)$ follows from char $(R) = 0$, so $c > 0$ can be supposed. Let $c = p^u c_1$ and $d = p^v d_1$ such that p does not divide $c_1 d_1$. We infer from (9) that $u > v$ and $v \leq g$. Hence there are integers x and y with $p^v = \text{g.c.d.}(p^u, d) = x p^u + y d$. If (c,d) belonged to $D(R)$, i.e., if there was an element $r \in R$ with $cr = d \cdot 1_R$, then we would have

$$\begin{aligned} p^g \cdot 1_R &= p^{g-v}(p^v \cdot 1_R) = p^{g-v}(x p^u + y d) \cdot 1_R = \\ &= p^{g+u-v} x \cdot 1_R + p^{g-v} y d \cdot 1_R = p^{g+u-v} x \cdot 1_R + p^{g-v} y c \cdot r = \\ &= p^{g+1}((x p^{u-v-1} \cdot 1_R + p^{u-v-1} y c_1 \cdot r)), \end{aligned}$$

which would contradict $(p^{g+1}, p^g) \notin D(R)$. Thus $(c,d) \notin D(R)$, proving (8). ■

By (7) and (8), $T(R)$ is the intersection of some $T(\boldsymbol{Z}_k)$. Therefore it suffices to show that

$$(12) \qquad T(\boldsymbol{Z}_k) \quad \text{is selfdual for every} \quad k \geq 0.$$

The mentioned strong Mal'cev conditions of Wille and Pixley easily imply that, for any lattice identity λ, we have $\lambda \in T(\boldsymbol{Z}_k)$ iff λ holds in $\mathrm{Sub}(\boldsymbol{Z}_k^t)$ for all positive integers t where $\boldsymbol{Z}_k^t$ is considered a $\boldsymbol{Z}_k$-module in the natural way. (In fact, $\boldsymbol{Z}_k^t$ is the free $\boldsymbol{Z}_k$-module on t generators.) Hence (12) and the Main Theorem will prompt follow from

$$\text{for all } k \geq 0, \quad \mathrm{Sub}(\boldsymbol{Z}_k^t) \text{ is a selfdual lattice.} \tag{13}$$

Although there are deep module theoretic results implying (13), the tools we have already listed make a short elementary proof possible. The elements of $\boldsymbol{Z}_k^t$ will be row vectors, and for $\vec{x} = (x_1, \ldots, x_t) \in \boldsymbol{Z}_k^t$ the transpose of $\vec{x}$ will be denoted by $\vec{x}^*$. Standard matrix notations like $\vec{x}\vec{y}^* = x_1y_1 + \cdots + x_ty_t$ will be in effect. We claim that

$$\begin{aligned} \varphi : \mathrm{Sub}(\boldsymbol{Z}_k^t) &\to \mathrm{Sub}(\boldsymbol{Z}_k^t), \\ S &\mapsto S^\perp := \{\vec{x} \in \boldsymbol{Z}_k^t : (\forall \vec{y} \in S)(\vec{x}\vec{y}^* = 0)\} \end{aligned}$$

is a dual lattice automorphism and, in addition, an involution. All the necessary properties of φ can be checked very easily except that

$$(S^\perp)^\perp \subseteq S. \tag{14}$$

Assume that $k > 0$, and let 1_k denote the ring unit of $\boldsymbol{Z}_k$. First we prove (14) for the case when $t = 1$. Since $\boldsymbol{Z}$ is a principal ideal domain, we easily conclude that S is necessarily of the form $\{xu \cdot 1_k : x \in \boldsymbol{Z}\}$ for some positive divisor u of k in $\boldsymbol{Z}$. The same holds for the submodule $S^\perp$, so it is of the form $\{vx \cdot 1_k : x \in \boldsymbol{Z}\}$ for an appropriate positive divisor v of k in $\boldsymbol{Z}$. Since $(u \cdot 1_k)(v \cdot 1_k) = 0$, we obtain

$$k \mid uv. \tag{15}$$

On the other hand, $(k/u) \cdot 1_k$ is clearly orthogonal to all members of S, so it is in $S^\perp$, whence $(k/u) \cdot 1_k = vx \cdot 1_k = v(x \cdot 1_k)$ for some $x \in \boldsymbol{Z}$. Therefore $(v, k/u) \in D(\boldsymbol{Z}_k)$, and (9) gives $v \mid k/u$, i.e.,

$$uv \mid k. \tag{16}$$

From (15) and (16), we have $v = k/u$. Hence, giving the role of u to v we obtain $(S^\perp)^\perp = \{x(k/(k/u)) \cdot 1_k : x \in \boldsymbol{Z}\} = \{xu \cdot 1_k : x \in \boldsymbol{Z}\} = S$.

Now let $t > 1$, and let S be a submodule of $\boldsymbol{Z}_k^t$. Since S is finite, we can consider a matrix A of size $s \times t$ for some $s \geq t$ such that each vector of S

coincides with at least one row of A. Although A is a matrix over $\boldsymbol{Z}_k$, not over $\boldsymbol{Z}$, using the natural ring homomorphism $\boldsymbol{Z} \to \boldsymbol{Z}_k$ for matrix entries we can easily conclude from Frobenius' afore-mentioned result that there are square matrices B and C over $\boldsymbol{Z}_k$ with respective sizes $s \times s$ and $t \times t$ such that BAC is a diagonal matrix, and B resp. C has an inverse in the ring of $s \times s$ resp. $t \times t$ matrices over $\boldsymbol{Z}_k$. For any $\vec{y} \in \boldsymbol{Z}_k^t$ we have

$$\vec{y} \in S^{\perp} \iff A\vec{y}^* = 0.$$

Now let $\vec{v}$ be an arbitrary member of $S^{\perp\perp}$. Then

$$(\forall \vec{y} \in \boldsymbol{Z}_k^t)\ (A\vec{y}^* = 0 \Longrightarrow \vec{v}\vec{y}^* = 0).$$

Resorting to the above-mentioned B and C and multiplying by B from the left we obtain

$$(\forall \vec{y} \in \boldsymbol{Z}_k^t)\ ((BAC)(C^{-1}\vec{y}^*) = 0 \Longrightarrow (\vec{v}C)(C^{-1}\vec{y}^*) = 0).$$

Since $C^{-1}\vec{y}^*$ takes all (transposed) values from $\boldsymbol{Z}_k^t$, with the notations $M = BAC$ and $\vec{w} = \vec{v}C$ we obtain

$$(\forall \vec{z} \in \boldsymbol{Z}_k^t)\ (M\vec{z}^* = 0 \Longrightarrow \vec{w}\vec{z}^* = 0). \tag{17}$$

We know that M is a diagonal matrix, let $m_{11}, \ldots, m_{tt}$ be its diagonal entries. Choosing $\vec{z}$ such that all but one of its components are zero we obtain from (17) that

$$(\forall z_i \in \boldsymbol{Z}_k)\ (m_{ii}z_i = 0 \Longrightarrow w_i z_i = 0) \qquad (i = 1, \ldots, t). \tag{18}$$

Let $S_i = \{um_{ii} : u \in \boldsymbol{Z}_k\} \in \mathrm{Sub}(\boldsymbol{Z}_k)$; condition (18), in other words, says that $w_i \in S_i^{\perp\perp}$. Since (14) has already been proved for $t = 1$, we have $w_i \in S_i$, and we can choose an $r_i \in \boldsymbol{Z}_k$ such that

$$w_i = r_i m_{ii} \qquad (i = 1, \ldots, t). \tag{19}$$

Letting $\vec{r} = (r_1, \ldots, r_t, 0, \ldots, 0)$ (with s components) we have $\vec{r}M = \vec{w}$. Hence

$$\vec{v} = \vec{w}C^{-1} = \vec{r}MC^{-1} = \vec{r}BACC^{-1} = (\vec{r}B)A,$$

showing that $\vec{v}$ is a linear combination of the rows of A, i.e., $\vec{v} \in S$. This proves (14) for the case $k > 0$.

When $k = 0$, $\boldsymbol{Z}_0 = \boldsymbol{Q}$, and the rudiments of linear algebra yield $\dim S^{\perp} = t - \dim S$. Hence (14) follows from the evident $\supseteq$ inclusion and the fact that both sides have the same dimension. This completes the proof of the the Main Theorem. ∎

References

[1] G. Frobenius, *Theorie der linearen Formen mit ganzen Coefficienten*, J. Reine Angew. Math. **86** (1879), 146–208.

[2] G. Hutchinson, *On classes of lattices representable by modules*, p. 69–94 in: *Proceedings of the University of Houston Lattice Theory Conference*, Univ. Houston 1973.

[3] G. Hutchinson and G. Czédli, *A test for identities satisfied in submodule lattices*, Algebra Universalis **8** (1978), 269–309.

[4] A.F. Pixley, *Local Mal'cev conditions*, Canadian Math. Bull. **15** (1972), 559–568.

[5] R. Wille, *Kongruenzklassengeometrien*, Lecture Notes in Math., no. **113**, Springer-Verlag, Berlin-Heidelberg-New York 1970.

Received 23 February 1998