Canad. Math. Bull. Vol. 15 (2), 1972

ON $GL_2(R)$ WHERE R IS A BOOLEAN RING

BY
JOSEPH G. ROSENSTEIN

In this paper we characterize the 2×2 invertible matrices over a Boolean ring, and, using this characterization, show that every invertible matrix has order dividing 6. This suggests that GL_2 of a Boolean ring is built up out of copies of the symmetric group S_3. Indeed, if B is a finite Boolean ring, then $GL_2(B)$ turns out to be a direct sum of copies of S_3. If B is infinite, then $GL_2(B)$ is more difficult to calculate; we present here descriptions of $GL_2(B)$ for the "extreme" cases of countable Boolean rings—namely, the Boolean ring which is generated by its atoms and the atomless Boolean ring. The former provides a negative answer to the question of whether the functor $GL_2(\cdot)$ preserves inverse limits; the latter is a corollary of a theorem which states that, under certain circumstances, $GL_2(\cdot)$ preserves direct limits. It turns out, in addition, that every invertible matrix is a product of elementary ones, as is the case for matrices over a Euclidean domain.

My interest in this topic was generated during a study of groups whose theories are $\aleph_0$-categorical—i.e. which can be characterized up to isomorphism, within the class of countable groups, by their first-order properties. One can show that such a group must be one of bounded order in which finitely generated subgroups are (uniformly) finite. The search for examples of such groups led me to study the GL_2 of a Boolean ring. It turns out that the GL_2 of an atomless Boolean ring is $\aleph_0$-categorical, whereas the GL_2 of the Boolean ring generated by its atoms is not (although it satisfies the conditions above).

We adopt the following convention: by "ring" we shall always mean "commutative ring with unit."

The structure of $GL_2(R)$ has been studied extensively for many years; initially R was assumed to be a field, but subsequently this requirement was relaxed so that R was assumed to belong to certain classes of integral domains. (Cf. [1] and the references given there.) Boolean rings are of course far from integral domains; for, in a Boolean ring, $a+a=0$ and $a^2=a$ hold for all elements a of the ring.

THEOREM 1. *A matrix* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *over a Boolean ring is invertible if and only if it can be written as*

$$\begin{pmatrix} a & 1+a+x \\ 1+a+x' & a+w+xx' \end{pmatrix}$$

where $ax=x$, $ax'=x'$, *and* $aw=0$.

Received by the editors November 4, 1970 and, in revised form, May 11, 1971.

Proof. We first note that for any ring R a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ over R is invertible if and only if $ad-bc$ is a unit of R, in which case its inverse is

$$\begin{pmatrix} d/ad-bc & -b/ad-bc \\ -c/ad-bc & a/ad-bc \end{pmatrix}.$$

Now in a Boolean ring if $xy=1$ then $x=x(xy)=x^2y=xy=1$, so that 1 is the only unit in a Boolean ring. Thus, since in addition $a=-a$ for each element a of a Boolean ring, we can write the inverse of the original matrix as $\begin{pmatrix} d & b \\ c & a \end{pmatrix}$, the matrix having an inverse if and only if $ad+bc=1$.

Now set $y=b+ab$. Then $ay=0$. Hence $b=x+y$ where $ax=a(ab)=ab=x$ and $ay=0$.

Similarly, set $y'=c+ac$. Then $ay'=0$. Hence $c=x'+y'$ where $ax'=a(ac)=ac=x'$ and $ay'=0$.

Note that $xy=(ax)y=x(ay)=0$ and similarly $x'y=xy'=x'y'=0$. In particular,

$$bc = (x+y)(x'+y') = xx'+yy'.$$

Thus $1=ad+bc=ad+xx'+yy'$ so that

$$a = ad+a(xx')+a(yy') = ad+xx'.$$

Hence if we set $z=d+xx'$, then $az=ad+axx'=a$. Thus $d=xx'+z$ where $az=a$. If we set $w=z+a$, then $d=xx'+a+w$ and $aw=az+a=0$.

Hence $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ can be written in the form

$$\begin{pmatrix} a & x+y \\ x'+y' & xx'+w+a \end{pmatrix},$$

where $ax=x$, $ax'=x'$, $ay=0$, $ay'=0$, and $aw=0$. Now write $g=y+1+a$ and $g'=y'+1+a$; note that $ag=ag'=0$. Hence,

$$yy' = (1+a+g)(1+a+g') = 1+a+g+g'+gg'$$

so that $1+a+yy'=g+g'+gg'$. But on the other hand, since $ad+bc=1$, we get

$$a(xx'+w+a)+(x+y)(x'+y') = 1$$

and therefore $xx'+a+xx'+yy'=1$. Thus $1+a+yy'=0$. Hence $g+g'+gg'=0$. But then $g=g(g+g'+gg')=0$ and, similarly, $g'=0$. So $y=1+a$ and $y'=1+a$. Therefore $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is of the form

$$\begin{pmatrix} a & 1+a+x \\ 1+a+x' & a+w+xx' \end{pmatrix},$$

https://doi.org/10.4153/CMB-1972-048-6 Published online by Cambridge University Press

where $ax=x$, $ax'=x'$, and $aw=0$. Note also that $xw=(ax)w=x(aw)=0$ and, similarly, $x'w=0$.

It is a simple matter to verify that a matrix of the form arrived at in the last paragraph is indeed invertible, and this proves the theorem.

The representation given in Theorem 1 is unique, as can easily be verified.

THEOREM 2. *Let $M \in GL_2(B)$. Then*

(i) $M^6=I$ $\left(\text{notation for } \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right)$,

(ii) $M^2=I$ *if and only if*

$$M = \begin{pmatrix} a & 1+x+a \\ 1+x'+a & a \end{pmatrix},$$

where $ax=x$, $ax'=x'$ and $xx'=0$.

(iii) $M^3=I$ *if and only if*

$$M = \begin{pmatrix} a & 1+x+a \\ 1+x+a & 1+x \end{pmatrix},$$

where $ax=x$.

Proof. Since $M \in GL_2(B)$, we can write M as

$$\begin{pmatrix} a & 1+a+x \\ 1+a+x' & a+w+xx' \end{pmatrix},$$

where $ax=x$, $ax'=x'$, and $aw=0$. Then

$$M^2 = \begin{pmatrix} 1+xx' & xx'+w \\ xx'+w & 1+w \end{pmatrix}$$

and

$$M^3 = \begin{pmatrix} a+w & 1+a+x+w+xx' \\ 1+a+x'+w+xx' & a+w \end{pmatrix}.$$

But $M^3 \in GL_2(B)$ and so $(M^3)^{-1}=M^3$. Hence $M^6=I$, proving (i). (An alternative proof, suggested by the referee, is obtained by first observing, via Cayley's theorem, that if $M \in GL_2(B)$ then $M^2=I+MT$, where T is the trace of M, and then verifying that $(I+MT)^3=I$.)

If $M^2=I$, then $xx'=0$ and $w=0$. So

$$M = \begin{pmatrix} a & 1+a+x \\ 1+a+x' & a \end{pmatrix}.$$

Conversely, if M is of this form, where $ax=x$, $ax'=x'$, and $xx'=0$, then $M^2=I$. This proves (ii).

https://doi.org/10.4153/CMB-1972-048-6 Published online by Cambridge University Press

Finally, if $M^3=I$, then

$$\begin{aligned} a+w &= 1, \\ 1+a+x+w+xx' &= 0, \end{aligned}$$

and

$$1+a+x'+w+xx' = 0.$$

Hence $x+xx'=0$ and $x'+xx'=0$ so $x=xx'=x'$. Hence, making the appropriate substitutions, we see that M can be written in the prescribed form. Conversely, if M is of this form then $M^3=I$. This proves (iii).

THEOREM 3. *Let* $\mathscr{M}_3=\{M \mid M^3=I\}$. *Then* $\mathscr{M}_3 \lhd GL_2(B)$, *and is Abelian.*

Proof. By direct computation.

THEOREM 4. *Every element of* $GL_2(B)$ *is a product of elementary matrices—i.e. matrices of the form* $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ *and* $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ *for* $a \in B$.

Proof. If $M \in GL_2(B)$, then $M=M^4 \cdot M^3$, $(M^4)^3=I$, and $(M^3)^2=I$, so it is sufficient to prove the claim for matrices of order 2 and order 3.

If $M^2=I$, then by Theorem 2 we can write

$$M = \begin{pmatrix} a & 1+x+a \\ 1+x'+a & a \end{pmatrix},$$

where $xx'=0$, $ax=x$, and $ax'=x'$. But then

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & x' \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

If $M^3=I$, then by Theorem 2 we can write

$$M = \begin{pmatrix} a & 1+x+a \\ 1+x+a & 1+x \end{pmatrix},$$

where $ax=x$. But then

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

The verifications we leave for the reader.

Let B be a finite Boolean ring. Then, as is well known, $B \simeq \sum_{0 \le i \le n-1} \oplus B_i$ where, for each i, B_i is the field with two elements; conversely, each such direct sum is a Boolean ring. Thus for each $n \ge 1$ there is a unique Boolean ring with 2^n elements. Furthermore, if B is as above, each element $b \in B$ can be described by an n-tuple $\langle b_0, b_1, \ldots, b_{n-1} \rangle$ of 0's and 1's. Let $n_b=\{i \mid b_i=1\}$. Then $n_{bc}=n_b \cap n_c$ so that $n_{bc}=n_b$ iff $n_b \subseteq n_c$, and $n_{bc}=\varnothing$ iff $n_b \cap n_c=\varnothing$.

https://doi.org/10.4153/CMB-1972-048-6 Published online by Cambridge University Press

THEOREM 5. *If B has 2^n elements then $GL_2(B)$ has 6^n elements; of these, 3^n have order 3 and 4^n have order 2.*

Proof. There is a 1–1 correspondence between $GL_2(B)$ and the set of all quadruples $\langle a, x, x', w\rangle$ of elements of B for which $ax=x$, $ax'=x'$, and $aw=0$. This is true since

$$\begin{pmatrix} a & 1+a+x \\ 1+a+x' & w+a+xx' \end{pmatrix} = \begin{pmatrix} b & 1+b+y \\ 1+b+y' & v+b+yy' \end{pmatrix}$$

if and only if $a=b$, $x=y$, $x'=y'$, and $w=v$.

Suppose that $a \in B$ and $n_a=k$. We can then choose x in 2^k different ways (since $n_x \subseteq n_a$), we can choose x' in 2^k different ways, and we can choose w in 2^{n-k} different ways (since $n_w \cap n_a=\varnothing$). Hence the number of elements of $GL_2(B)$ which have a in the upper left-hand corner is exactly $2^k \cdot 2^k \cdot 2^{n-k}$. The total number of $a \in B$ for which $n_a=k$ is precisely $\binom{n}{k}$. Thus the number of elements in $GL_2(B)$ is

$$\sum_{0 \le k \le n} \binom{n}{k} \cdot 2^k \cdot 2^k \cdot 2^{n-k} = 2^n \sum_{0 \le k \le n} \binom{n}{k} \cdot 2^k = 2^n \cdot 3^n = 6^n.$$

By Theorem 2, an element of $GL_2(B)$ has order 3 iff it has the form

$$\begin{pmatrix} a & 1+x+a \\ 1+x+a & 1+x \end{pmatrix},$$

where $ax=x$, so that the number of elements of order 3 is

$$\sum_{0 \le k \le n} \binom{n}{k} \cdot 2^k = 3^n.$$

Similarly, an element of $GL_2(B)$ has order 2 iff it has the form

$$\begin{pmatrix} a & 1+a+x \\ 1+a+x' & a \end{pmatrix},$$

where $xx'=0$, $ax=x$, and $ax'=x'$, so that the number of elements of order 2 is

$$\sum_{0 \le k \le n} \binom{n}{k} \cdot \left(\sum_{0 \le i \le k} \binom{k}{i} \cdot 2^{k-i} \right) = \sum_{0 \le k \le n} \binom{n}{k} \cdot 3^k = 4^n.$$

Theorem 5 suggests the possibility that $GL_2(B)$ is a direct sum of n six-element groups. One can see immediately that $GL_2(B)$ is not a direct sum of cyclic groups of order six, since such a direct sum would have to be commutative, which $GL_2(B)$ is not. The only other group with six elements is the group S_3, the symmetric group on three letters. This group is generated by two elements c and d satisfying $c^2=1$, $d^3=1$, and $cd=d^2c$.

THEOREM 6. *If B has 2^n elements, then $GL_2(B) \simeq \sum_{0 \le i < n} \oplus G_i$, where $G_i \simeq S_3$ for each i.*

https://doi.org/10.4153/CMB-1972-048-6 Published online by Cambridge University Press

Proof. For each i, $0 \leq i < n$, define b^i to be the unique element of B satisfying

$$b^i_j = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j. \end{cases}$$

Define G_i to consist of the following six elements of $GL_2(B)$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & b^i \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ b^i & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1+b^i & b^i \\ b^i & 1+b^i \end{pmatrix}, \quad \begin{pmatrix} 1+b^i & b^i \\ b^i & 1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 1 & b^i \\ b^i & 1+b^i \end{pmatrix}.$$

One can easily verify that G_i is a group isomorphic to S_3; one can further verify, although the calculations are tedious, that $G_i \lhd GL_2(B)$. (The verification is simplified if one first observes, as in Theorem 4, that we need only show that if M has order 2 and $A \in G_i$ then $MAM \in G_i$ and that if M has order 3 and $A \in G_i$ then $MAM^2 \in G_i$.) One can also verify straightforwardly that if $A \in G_i$ and $B \in G_j$, where $i \neq j$, then $AB = BA$. In all of these verifications one must lean heavily on the fact that for every $a \in B$ either $ab^i = b^i$ or $ab^i = 0$, with the former taking place if and only if $a_i = 1$.

To show that $G_0 + \cdots + G_{n-1} = G_0 \oplus \cdots \oplus G_{n-1}$ we need only show that if $A_i \in G_i$ for each i and $A_0 A_1 \cdot \ldots \cdot A_{n-1} = I$ then $A_i = I$ for each i. (This is sufficient because we already know that elements of different G_i's commute.)

Partition $\{0, 1, \ldots, n-1\}$ into six sets $P_1, \ldots, P_6$ putting

$$i \text{ into } P_1 \quad \text{iff} \quad A_i = \begin{pmatrix} 1 & b^i \\ 0 & 1 \end{pmatrix},$$

$$i \text{ into } P_2 \quad \text{iff} \quad A_i = \begin{pmatrix} 1 & 0 \\ b^i & 1 \end{pmatrix},$$

$$i \text{ into } P_3 \quad \text{iff} \quad A_i = \begin{pmatrix} 1+b^i & b^i \\ b^i & 1+b^i \end{pmatrix},$$

$$i \text{ into } P_4 \quad \text{iff} \quad A_i = \begin{pmatrix} 1 & b^i \\ b^i & 1+b^i \end{pmatrix},$$

$$i \text{ into } P_5 \quad \text{iff} \quad A_i = \begin{pmatrix} 1+b^i & b^i \\ b^i & 1 \end{pmatrix},$$

and

$$i \text{ into } P_6 \quad \text{iff} \quad A_i = I.$$

Now let $B_j = \prod_{i \in P_j} A_i$ for $1 \leq j \leq 6$. (This is well defined since the A_i's commute.) Thus $B_1 B_2 B_3 B_4 B_5 = I$. One can verify that

$$B_1 = \begin{pmatrix} 1 & a^1 \\ 0 & 1 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 & 0 \\ a^2 & 1 \end{pmatrix}, \quad B_3 = \begin{pmatrix} 1+a^3 & a^3 \\ a^3 & 1+a^3 \end{pmatrix},$$

$$B_4 = \begin{pmatrix} 1 & a^4 \\ a^4 & 1+a^4 \end{pmatrix}, \quad \text{and} \quad B_5 = \begin{pmatrix} 1+a^5 & a^5 \\ a^5 & 1 \end{pmatrix},$$

where $a^j_i = 1$ iff $i \in P_j$. This, of course, implies that $a^j a^k = 0$ if $j \neq k$.

https://doi.org/10.4153/CMB-1972-048-6 Published online by Cambridge University Press

But then

$$B_1B_2B_3B_4B_5 = \begin{pmatrix} 1+a^3+a^5 & a^1+a^3+a^4+a^5 \\ a^2+a^3+a^4+a^5 & 1+a^3+a^4 \end{pmatrix}.$$

If this equals the identity, then it follows easily that $a^1=a^2=a^3=a^4=a^5=0$ and hence that $P_1=P_2=P_3=P_4=P_5=\varnothing$ and therefore $A_i=I$ for all i.

Hence

$$G_0+G_1+\cdots+G_{n-1}=G_0\oplus G_1\oplus\cdots\oplus G_{n-1}.$$

But the direct sum has 6^n elements, hence must be all of $GL_2(B)$. Therefore

$$GL_2(B) \simeq \sum_{0<i\leq n} \oplus G_i,$$

where each $G_i \simeq S_3$.

An element b of a Boolean ring B is said to be atomic if whenever $ab\neq 0$ then $ab=b$. We define G_b to be

$$\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&b\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\b&1\end{pmatrix}, \begin{pmatrix}1+b&b\\b&1+b\end{pmatrix}, \begin{pmatrix}1&b\\b&1+b\end{pmatrix}, \begin{pmatrix}1+b&b\\b&1\end{pmatrix}\right\}.$$

THEOREM 6A. *Let B be a Boolean ring and let $\{b_i \mid i\in I\}$ be the set of atomic elements of B. Then $\sum_{i\in I} G_{b_i}=\sum_{i\in I}\oplus G_{b_i}$ and is a normal subgroup of $GL_2(B)$.*

Proof. The same as Theorem 6.

The difference between Theorem 6 and Theorem 6A is that in the former we are able to conclude that $GL_2(B)=\sum_{i\in I}\oplus G_{b_i}$ since the latter has the same number of elements as the former. This conclusion is not possible in Theorem 6A. In cases where I is small (e.g. if B is atomless) then $GL_2(B)$ will clearly be a proper superset of $\sum_{i\in I}\oplus G_{b_i}$; we shall see that even if I is large, i.e. even if B is generated by its atomic elements, as long as it is infinite we still may not have $GL_2(B)=\sum_{i\in I}\oplus G_{b_i}$.

We first note that homomorphisms behave properly.

LEMMA. *Let $h: B\to B'$ be a ring homomorphism between Boolean rings. Define $h^*: GL_2(B)\to GL_2(B')$ by*

$$h^*\begin{pmatrix}a&b\\c&d\end{pmatrix} = \begin{pmatrix}h(a)&h(b)\\h(c)&h(d)\end{pmatrix}.$$

Then h^* is a group homomorphism. Furthermore, h^* is 1–1 iff h is 1–1, and h^* is onto iff h is onto.

Proof. All but one of the claims are easily proved for any homomorphism h in the category of rings. The assumption that B' is a Boolean ring is needed only to invoke Theorem 4 to show that if h is onto then so is h^*. Note that in general this is false—e.g. $h: Z\to Z_5$ does not induce an onto map h^*.

Let B_I be the ring of all finite and cofinite subsets of I. Then B_I can be represented

as a particular subring of $\prod_{i \in I} R_i$ where each $R_i \simeq Z_2$. This subring consists of all $f \in Z_2^I$ such that either $\{i \mid f(i)=0\}$ is finite or $\{i \mid f(i)=1\}$ is finite. Thus the structure of B_I is completely determined by the cardinality of I.

THEOREM 6B. *$GL_2(B_N) \neq \sum_{i \in N} \oplus G_{b_i}$; in fact, $\sum_{i \in N} \oplus G_{b_i}$ is not a direct summand of $GL_2(B_N)$.*

Proof. Define a function $h: B_N \to \{0, 1\}$ by

$$h(f) = \begin{cases} 1 & \text{if } \{i \mid f(i) = 0\} \text{ is finite} \\ 0 & \text{if } \{i \mid f(i) = 1\} \text{ is finite.} \end{cases}$$

One must verify that h is a homomorphism and that $h^*(M)=I$ if and only if $M \in \sum_{i \in N} \oplus G_{b_i}$. Since h is onto so is h^*; but $GL_2(\{0, 1\})$ has six elements, hence $h^*(\sum_{i \in N} \oplus G_{b_i}) \neq GL_2(\{0, 1\})$. Therefore $GL_2(B_N) \neq \sum_{i \in N} \oplus G_{b_i}$ for in fact

$$GL_2(B_N) \Big/ \sum_{i \in N} \oplus G_{b_i} \simeq S_3.$$

It remains a possibility that there is a subgroup $H \lhd GL_2(B_N)$ such that $GL_2(B_N) = H \oplus \sum_{i \in I} \oplus G_{b_i}$. To see that this does not happen it suffices to show that if $R \in GL_2(B_N) - \sum_{i \in N} \oplus G_{b_i}$ then the normal subgroup H generated by R contains more than six elements.

There are three cases:

Case 1. $h^*(R) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ or $h^*(R) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Let $R = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then, for each $x \in B$,

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in H.$$

But this equals $\begin{pmatrix} a+cx & \cdots \\ \cdots & \cdots \end{pmatrix}$. Since $h(a)=h(c)=1$ we know that $h(ac)=1$ so that there are infinitely many $x \in B$ for which $ax=cx=x$. Each of these gives a different element of H, so that H has many more than six elements.

Case 2. $h^*(R) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $h^*(R) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Then for each $x \in B$,

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \in H.$$

But this equals $\begin{pmatrix} \cdots & \cdots \\ \cdots & bx+d \end{pmatrix}$ and we can proceed as in Case 1.

Case 3. $h^*(R) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. We proceed as in Case 2 but note that since $h(d)=0$ and $h(b)=1$ we can find infinitely many $x \in B$ for which $bx=x$ and $dx=0$.

https://doi.org/10.4153/CMB-1972-048-6 Published online by Cambridge University Press

Thus $\sum_{i\in N}\oplus G_{b_i}$ is not a direct summand of $GL_2(B_N)$. It is easy to see however that $\sum_{i\in N}\oplus G_{b_i}$ together with

$$\left\{\begin{pmatrix}0&1\\1&0\end{pmatrix},\ \begin{pmatrix}1&1\\1&0\end{pmatrix},\ \begin{pmatrix}0&1\\1&1\end{pmatrix},\ \begin{pmatrix}1&1\\0&1\end{pmatrix},\ \begin{pmatrix}1&0\\1&1\end{pmatrix}\right\}$$

generates $GL_2(B_N)$.

THEOREM 7. *The group $GL_2(B_N)$ is isomorphic to the group generated by the elements $\{x_i \mid i\in N\}\cup\{y_i \mid i\in N\}$ subject to the following relations:*

(i) $x_i^2=1,\quad y_i^3=1$ *for each* $i\geq 0$
(ii) $x_ix_j=x_jx_i$ *for each* $i, j\geq 0$
(iii) $x_iy_j=y_jx_i$ *for each* $i, j\geq 1$ *where* $i\neq j$
(iv) $y_iy_j=y_jy_i$ *for each* $i, j\geq 0$
(v) $x_iy_i=y_i^2x_i$ *for each* $i\geq 0$
(vi) $y_ix_0=x_0y_i^2$ *for each* $i\geq 1$
(vii) $x_iy_0=y_0x_iy_i$ *for each* $i\geq 1$

Proof. Define a homomorphism from the free group on the generators above to $GL_2(B_N)$ as follows:

$$f(x_0)=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad f(x_i)=\begin{pmatrix}1+b^i&b^i\\b^i&1+b^i\end{pmatrix}\quad \text{for } i>0,$$

$$f(y_0)=\begin{pmatrix}1&1\\1&0\end{pmatrix},\quad f(y_i)=\begin{pmatrix}1+b^i&b^i\\b^i&1\end{pmatrix}\quad \text{for } i>0.$$

It suffices to show that $w\in\ker f$ if and only if $w=1$ is a consequence of (i)–(vii) above.

The "if" part requires a direct verification that certain words, obtained from (i)–(vii) above, are actually in the kernel of f. On the other hand, let w be any word. Then using (ii), (iv), (vi), and (vii) we can write it in a form where all x_0's and y_0's are to the left of all x_i's and y_i's for $i>0$. Furthermore, using (i), (iii), and (v) we can write w in the form $w_0w_1w_2\ldots w_k$ where for each j, $0\leq j\leq k$, w_j is one of

$$\{1, x_j, y_j, y_j^2, x_jy_j, x_jy_j^2\}.$$

If now $f(w)=I$, then we can show, as in the proof of Theorem 6, that $f(w_j)=I$ for each j, and hence that $w_j=1$ for each j. Hence $w=1$ is a consequence of (i)–(vii) above, and the theorem is proven.

We now wish to look at $GL_2(\cdot)$ as a functor from the category of rings to the category of groups, and interpret Theorem 6B from this point of view.

For each $n\in N$ let B_n be the Boolean ring generated by the atoms $\{b_i^n \mid i<n\}$. If $m\leq n$ we define $f_{mn}\ B_n\to B_m$ by stipulating that $f_{mn}(b_i^n)=b_i^m$ if $i<m$ and $f_{mn}(b_i^n)=0$ if $i\geq m$. Thus $\{B_n \mid n\in N\}$ together with $\{f_{mn} \mid m\leq n\}$ is an inverse system of rings. It is easy to see that B_N, generated by the atoms $\{b_i \mid i\in N\}$, is its inverse

https://doi.org/10.4153/CMB-1972-048-6 Published online by Cambridge University Press

limit, where $f_n: B_N \to B_n$ is defined by stipulating that $f_n(b_i)=b_i^n$ if $i<n$ and $f_n(b_i)=0$ if $i \geq n$.

Also $\{GL_2(B_n) \mid n \in N\}$ together with $\{f_{mn}^* \mid m \leq n\}$ forms an inverse system of groups; and since $GL_2(B_n)=\sum_{i<n} \oplus G_i^n$, where $G_i^n \simeq S_3$ for each n and i, and since f_{mn}^* maps $GL_2(B_n)$ to $GL_2(B_m)$ by sending G_i^n to G_i^m for $i<m$ and G_i^m to 0 for $i \geq m$, it is clear that the inverse limit of this sytem is $\sum_{i \in N} \oplus G_i$, where each $G_i \simeq S_3$ and where f_n maps $\sum_{i \in N} \oplus G_i$ to $\sum_{i<n} \oplus G_i^n$ by sending G_i to G_i^n if $i<n$ and otherwise to 0.

Thus from a categorical point of view, Theorem 6B may be interpreted as

COROLLARY. *The functor $GL_2(\cdot)$ does not preserve inverse limits; more strongly, $GL_2(\cdot)$ does not preserve inverse limits even if in the inverse system the morphisms f_{mn} are all surjections and all induce surjections f_{mn}^*. (I do not know whether there already are examples of this in the literature.)*

The following theorem provides the usual contrast between inverse and direct limits.

THEOREM 8. *Let $\{R_i \mid i \in I\}$ and $\{f_{ij} \mid i \leq j\}$ form a direct system of rings. Let $\{GL_2(R_i) \mid i \in I\}$ and $\{f_{ij}^* \mid i \leq j\}$ be the corresponding direct system of groups. Let R and G be the direct limits of these systems. Assume that all f_{ij} are injective. Then $G \simeq GL_2(R)$.*

Proof. Let $f_i: R_i \to R$ and $g_i: GL_2(R_i) \to G$ be the maps required by the definition of direct limit. Thus for each $i \leq j$ we have $f_i=f_jf_{ij}$ and $g_i=g_jg_{ij}$. Since $f_i: R_i \to R$, $f_i^*: GL_2(R_i) \to GL_2(R)$ for each i. Hence there is a (unique) isomorphism $\rho: G \to GL_2(R)$ such that $\rho g_i=f_i^*$.

We wish to find an isomorphism $\tau: GL_2(R) \to G$ so that $\rho\tau=\mathrm{id}_{GL_2(R)}$ and $\tau\rho=\mathrm{id}_G$; for then $G \simeq GL_2(R)$. First of all, we note that, using the fact that R is the direct limit, if $x \in R$ then for some i there is an element $y \in R$ such that $f_i(y)=x$. Secondly, we note that if $A \in GL_2(R)$ then, since I is a directed partial ordering, there is an $i \in I$ and a matrix $B_i \in GL_2(R_1)$ such that $f_i^*(B_i)=A$. We would like to define $\tau(A)=g_i(B_i)$—but in order to do that we must first show that the value of $\tau(A)$ does not depend on i. So suppose that $B_i \in GL_2(R_i)$, $B_j \in GL_2(R_j)$, $f_i^*(B_i)=A$, and $f_j^*(B_j)=A$. Find a $k \in I$ such that $i \leq k$ and $j \leq k$. Then $f_i=f_kf_{ik}$ and $f_j=f_kf_{jk}$ so that $f_i^*=f_k^*f_{ik}^*$ and $f_j^*=f_k^*f_{jk}^*$. Now since each f_{ij} is an injection so is each f_k, and, by the lemma, the same is true for each f_k^*; therefore, $f_{ik}^*(B_i)=f_{jk}^*(B_j)$ so that $g_i(B_i)=g_kf_{ik}^*(B_i)=g_kf_{jk}^*(B_j)=g_j(B_j)$. Hence $\tau(A)$ is well defined. It is a simple matter to verify that τ is a homomorphism, that τ is 1–1, and that $\rho\tau$ and $\tau\rho$ are both identity maps. Therefore, $G \simeq GL_2(R)$.

We now turn to the situation where the Boolean ring in question is an atomless Boolean ring. In this case B contains a set $\{p_i \mid i \in I\}$ of elements which freely generate it; that is, every element of B can be written *uniquely* (modulo commutativity

https://doi.org/10.4153/CMB-1972-048-6 Published online by Cambridge University Press

of the generators) in the form $\prod_{1 \le j \le k} q_{i_j}$ where for $j \neq j'$ we have $i_j \neq i_{j'}$ and where for each j, $1 \le j \le k$, q_{i_j} is either p_{i_j} or is $1+p_{i_j}$.

Let p and q be two of the free generators of B, and let B_0 be the subring of B generated by p and q. One can easily verify that B_0 has sixteen elements and that its atoms are pq, $p(1+q)$, $(1+p)q$, and $(1+p)(1+q)$. Thus from Theorem 5 we know that $GL_2(B_0)$ has 6^4 elements and can be decomposed into a direct sum of four subgroups each of which is isomorphic to S_3. More generally, if B is freely generated by the set $\{p_i \mid i \in N\}$ then the subring B_k of B generated by $\{p_1, p_2, \ldots, p_k\}$ has 2^k atoms and therefore has $2^{(2^k)}$ elements. Hence Theorem 5 implies that $GL_2(B_k)$ has $6^{(2^k)}$ elements, and can be decomposed into a direct sum of 2^k subgroups each of which is isomorphic to S_3.

Thus locally $GL_2(B)$ behaves like the groups of $GL_2(B_I)$ discussed earlier—in the sense that if a given element of $GL_2(B)$ has entries which involve the generators $p_{i_1}, p_{i_2}, \ldots, p_{i_r}$ then it can be viewed as an element of a subgroup of $GL_2(B)$ which is isomorphic to a direct sum of 2^r copies of S_3.

But these subgroups of $GL_2(B)$ do not fit together nicely to form $GL_2(B)$—in the way that the corresponding subgroups of $GL_2(B_I)$ fit together to form $GL_2(B_I)$. This is so because $GL_2(B_k)$ is not, in the case where B is atomless, a simple projection of $GL_2(B_{k+1})$; this results from the fact that the atoms of B_k are no longer atoms in B_{k+1}—for example, $p_1p_2 \ldots p_k$ decomposes into $p_1p_2 \ldots p_kp_{k+1}$ and $p_1p_2 \ldots p_k(1+p_{k+1})$. Thus if one tried to present $GL_2(B)$ as in Theorem 7 by taking as generators for $GL_2(B)$ the union of the generators of the $GL_2(B_k)$ then one would have the unhappy situation that each generator, e.g.

$$\begin{pmatrix} 1+p_1 & p_1 \\ p_1 & 1+p_1 \end{pmatrix}$$

could be decomposed into a product of two generators

$$\begin{pmatrix} 1+p_1p_2 & p_1p_2 \\ p_1p_2 & 1+p_1p_2 \end{pmatrix} \cdot \begin{pmatrix} 1+p_1(1+p_2) & p_1(1+p_2) \\ p_1(1+p_2) & 1+p_1(1+p_2) \end{pmatrix}.$$

Such a presentation is not at all satisfactory. But one could not hope to do much better; for trying to find an acceptable presentation of $GL_2(B)$ is tantamount to finding atoms for an atomless Boolean ring.

So instead of trying to describe $GL_2(B)$ in terms of generators and relations we shall describe it categorically.

Let B_k be as above the subring of B freely generated by $\{p_1, p_2, \ldots, p_k\}$ and for each k let $f_k: B_k \to B_{k+1}$ be the identity map on B_k. Using the notation of the lemma stated earlier, the ring isomorphisms f_k give rise to group isomorphisms f_k^*: $GL_2(B_k) \to GL_2(B_{k+1})$ for each k. The sequence of groups $\{GL_2(B_k) \mid k \in N\}$, together with the isomorphisms $\{f_k^* \mid k \in N\}$, forms a direct system of groups. Let G be the direct limit of this direct system.

https://doi.org/10.4153/CMB-1972-048-6 Published online by Cambridge University Press

THEOREM 9. $G \simeq GL_2(B)$.

Proof. This conclusion is just a corollary of Theorem 8.

From these two extreme cases, the atomic and atomless Boolean rings, it should be possible to specify the structure of $GL_2(B)$ where B is any particular Boolean ring. We leave that to the reader. He may also want to generalize the conclusions here in several other directions. If he is interested in applying these techniques to other rings, he should be aware that the early theorems of this paper depend heavily on the fact that, in a Boolean ring, 1 is the only invertible element. On the other hand, if he is interested in finding $GL_n(B)$ for $n>2$, he should be aware that the basic building block $GL_n(\{0, 1\})$, which for $n=2$ is S_3, is in general a group which has $(2^n-1)(2^n-2)(2^n-4)\ldots(2^n-2^{n-1})$ elements—and for $n=3$ this is already 168 elements. (See [2, p. 77].) This difficulty, however, does not appear to be insurmountable.

As I pointed out in the opening paragraphs of this paper my investigations here arose during a search for $\aleph_0$-categorical groups. Since any further examples that I might find by looking in this direction are probably limits of finite groups, it seems that my purposes would best be served by studying such limits in general rather than by pursuing further examples.

Appendix. It seems appropriate to include at this point proofs of the claims mentioned earlier concerning the $\aleph_0$-categoricity of the groups of Theorems 7 and 9. These proofs rest on a theorem of Engeler, Svenonius, and Ryll-Nardzewski (cf. [3]) which can be described as follows: Let L be the first-order predicate calculus which contains symbols for the group operations, and let $F_n(L)$ be the set of well-formed formulas (wffs) of L whose free variables are among $v_1, v_2, \ldots, v_n$. We say that two n-tuples of elements of the group G are first-order equivalent$_G$ if they satisfy in G precisely the same wffs of $F_n(L)$. Then G is $\aleph_0$-categorical iff for each n the number of first-order equivalence$_G$ classes of n-tuples of elements of G is finite. Let us call two n-tuples $\langle a_1, a_2, \ldots, a_n\rangle$ and $\langle b_1, b_2, \ldots, b_n\rangle$ of elements of G automorphically equivalent$_G$ if there is an automorphism τ of G such that $\tau(a_i)=b_i$ for each i. If two n-tuples are automorphically equivalent$_G$, they are also first-order equivalent$_G$.

Thus in order to show that a group G is not $\aleph_0$-categorical it is necessary and sufficient to display, for some n, an infinite list of pairwise first-order inequivalent$_G$ n-tuples of elements of G. On the other hand, to show that G is $\aleph_0$-categorical it is sufficient (though not necessary) to display enough automorphisms of G so that for each n the number of automorphism equivalence$_G$ classes of n-tuples of elements of B is finite—since that implies the same is true for the number of first-order equivalence$_G$ classes.

We first show that the group $G=GL_2(B_N)$ of Theorem 7 is not $\aleph_0$-categorical. For each t let $d_t=x_1x_2\ldots x_t$; we shall show that the 1-tuples $\{\langle d_t\rangle \mid t\geq 1\}$ are pairwise first-order inequivalent$_G$. For each t let $\varphi_t(v)$ be the wff $(\exists^{!3^t}u)(\exists w)(w^{-1}vw=u)$

https://doi.org/10.4153/CMB-1972-048-6 Published online by Cambridge University Press

which says that v has precisely 3^t distinct conjugates in G. It is a simple matter to verify, using the proof of Theorem 7, that $\langle d_t \rangle$ satisfies the wff $\varphi_t(v)$ in G for each t. On the other hand it is clear from the definition of the $\varphi_t(v)$ that $\langle d_t \rangle$ does not satisfy the wff $\varphi_s(v)$ in G if $s \neq t$. Hence the 1-tuples $\{\langle d_t \rangle \mid t \geq 1\}$ are pairwise first-order inequivalent$_G$ so that $GL_2(B_N)$ is not $\aleph_0$-categorical.

We now show that the group G of Theorem 9 is $\aleph_0$-categorical. First some information about Boolean rings. An r-tuple $\langle b_1, b_2, \ldots, b_r \rangle$ of elements of a Boolean ring B is said to be independent if no product of the form $q_1 q_2 \ldots q_r$, where each q_i is either b_i or $1+b_i$, is zero. If B and B' are countable atomless Boolean rings, then B and B' are isomorphic (so that such a ring is $\aleph_0$-categorical); furthermore, if $\langle b_1, b_2, \ldots, b_r \rangle$ and $\langle b'_1, b'_2, \ldots, b'_r \rangle$ are independent r-tuples of elements of B and B', then we can find an isomorphism α so that $\alpha(b_i) = b'_i$ for each i. (This result, although apparently unpublished, is well known.)

Now let $\langle M_1, M_2, \ldots, M_n \rangle$ be an n-tuple of elements of G. We shall construct an automorphism ρ of G so that $\rho(M_i) \in g_{4n}(GL_2(B_{4n}))$ for each i, where g_{4n}: $GL_2(B_{4n}) \to G$ is the canonical map. This implies that the n-tuple $\langle M_1, M_2, \ldots, M_n \rangle$ is automorphically equivalent$_G$ to one of the $(6^{2^{4n}})^n$ n-tuples of elements of $g_{4n}(GL_2(B_{4n}))$. Hence we will be able to conclude that G is $\aleph_0$-categorical.

Since $M_1, M_2, \ldots, M_n$ have altogether at most $4n$ different entries there is an $r \leq 4n$ and there is an r-tuple $\langle b_1, b_2, \ldots, b_r \rangle$ of independent elements of B which generate a subring of B which includes all entries of $M_1, M_2, \ldots, M_n$. Let h_r be the canonical map from B_r to B (recall that B_r is generated by the r-tuple $\langle p_1, p_2, \ldots, p_r \rangle$ of independent elements) so that $\langle h_r(p_1), \ldots, h_r(p_r) \rangle$ is an r-tuple of independent elements of B. Then, by the above, there is an automorphism α of B such that $\alpha(b_i) = h_r(p_i)$ for each i. By the lemma α^* is an automorphism of G such that $\alpha^*(M_i) \in g_r(GL_2(B_r))$ and hence of $g_{4n}(GL_2(B_{4n}))$ for each i. This completes the proof.

References

1. P. M. Cohn, *On the structure of the GL_2 of a ring*, Publ. Dép. Math. No. 30, Inst. Hautes Etudes Sci., 1966.

2. L. E. Dickson, *Linear groups*, reprinted by Dover, New York, 1958.

3. E. Engeler, *A characterization of theories with isomorphic denumerable models*, Notices, Amer. Math. Soc. **6** (1959), p. 161.

Rutgers University,
New Brunswick, New Jersey