BIBLIOGRAPHY

- 1. K. L. Chung, Fluctuation of sums of independent random variables, Ann. of Math. vol. 51 (1950) pp. 697-706.
- 2. K. L. Chung and P. Erdös, Probability limit theorems assuming only the first moment. I, Memoirs of the American Mathematical Society, no. 6, pp. 13-19.
- 3. ——, On the lower limit of sums of independent random variables, Ann. of Math. vol. 48 (1947) pp. 1003-1013.
- 4. K. L. Chung and W. H. J. Fuchs, On the distribution of values of sums of random variables, Memoirs of the American Mathematical Society, no. 6, pp. 1-9.
- 5. H. Cramér, Random variables and probability distributions, Cambridge Tracts in Mathematics, no. 36, 1937.
- 6. C. G. Esseen, Fourier analysis of distribution functions, Acta Math. vol. 77 (1945) pp. 5-145.
- 7. G. Pólya, Über den zentralen Grenzwertsatz der Wahrscheinlichkeitsrechnung und das Momentproblem, Math. Zeit. vol. 8 (1920) pp. 171-181.
- 8. G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Oxford, 1938.

COLUMBIA UNIVERSITY

ON PROJECTIVE GEOMETRY OVER FULL MATRIX RINGS

RIMHAK REE

1. Introduction. In this note we show that projective geometry over a ring R and that over the full matrix ring R_n are essentially the same, and extend the fundamental theorem of projective geometry [1, p. 44] to the case of Φ_n -modules, where Φ is a division ring. (By a projective geometry over R we mean a lattice of all R-submodules of an R-module.) As a special case of these results we have the following: If $n \ge 3$, any lattice isomorphism of the lattice of all left ideals of Φ_n and that of Ψ_m where Φ and Ψ are division rings, is induced by an isomorphism of Φ_n and Ψ_m . We obtain also an extension of the basis theorem for vector spaces to Φ_n -modules.

Other extensions of the fundamental theorem of projective geometry have been made by Baer, for the case of R-modules, where R is a "primary ring" in his sense [2, p. 304], and the ring of rational integers [3].

2. Main theorems. In the following, by a ring we always mean an associative ring with unit element. Let R be a ring with unit

element 1. An additive group A is called an R-module if ax is defined for all a in R and all x in A such that

$$a(x + y) = ax + ay,$$

$$(a + b)x = ax + bx,$$

$$a(bx) = (ab)x,$$

$$1x = x$$

for any a, $b \in R$ and any x, $y \in A$. A subgroup B of A is called an R-submodule if $ax \in B$ for all $a \in R$ and all $x \in B$. The set of all R-submodules of A forms a modular lattice L(R, A) with respect to group-theoretical union and intersection. We will call the lattice L(R, A) a projective geometry over the ring R. (Usual projective geometry is the case when R is a division ring.)

We denote by R_n the full matrix ring of degree n over R. Our first main theorem is the following:

THEOREM 1. Let R be a ring and n be a positive integer. Then for any R_n -module M there exists an R-module A such that

$$(1) L(R_n, M) \cong L(R, A).$$

Conversely, for any R-module A there exists an R_n -module M such that (1) holds.

Now let $\mathfrak{F} = \{R, S, \cdots\}$ be a family of rings and π be a lattice theoretical condition. We shall say that the fundamental theorem of projective geometry (f.t.p.g.) holds in \mathfrak{F} under π if, for any ring R in \mathfrak{F} and R-module A such that L(R,A) satisfies the condition π , the following holds:

(2) If S is a ring in \mathfrak{F} and if B is an S-module such that $L(R, A) \cong L(S, B)$, then there exists an isomorphism σ of A to B and an isomorphism σ' of R to S such that the lattice isomorphism $A_1 \rightarrow A_1^* = B_1$, where A_1 denotes an arbitrary element in L(R, A), is induced by σ , i.e.

$$A_1^* = \{ y^{\sigma} | y \in A_1 \},$$

and such that $(ax)^{\sigma} = a^{\sigma'}x^{\sigma}$ for all a in R and all x in A. Our second main theorem is the following:

THEOREM 2. Let $\mathfrak{F} = \{R, S, \cdots\}$ be a family of rings, n a positive integer, and π be a lattice-theoretic condition. If f.t.p.g. holds in \mathfrak{F} under π then f.t.p.g. also holds in $\mathfrak{F}_n = \{R_n, S_n, \cdots\}$ under π . The isomorphism σ' of R_n to S_n needed in f.t.p.g. in \mathfrak{F}_n can always be chosen so

that σ' is of the type $(a_{ij})^{\sigma'} = (a_{ij}^{\sigma''})$, where σ'' is a suitable isomorphism of R to S.

3. Proof of Theorem 1. Let e_{ij} be the $n \times n$ matrix with 1 in the *i*th row and *j*th column and 0 elsewhere. It is easily seen that e_{ii} commutes with any diagonal matrix. Let a be an element in R. We shall denote by [a] the diagonal matrix of which all the diagonal elements are equal to a. The set of all [a] forms a subring of R_n isomorphic to R.

Let M be a given R_n -module. If we set $A = e_{11}M$, then we can consider A as an R-module, since every [a] is commutative with e_{11} . If M_1 is an R_n -submodule of M, then $A_1 = e_{11}M_1$ is an R-submodule of A. We shall show that the mapping $\phi: M_1 \rightarrow A_1 = e_{11}M_1$ gives the desired isomorphism of $L(R_n, M)$ and L(R, A). Let M_1, M_2 be two R_n -submodules of M such that $e_{11}M_1\subseteq e_{11}M_2$. We shall show that $M_1 \subseteq M_2$. For let $x \in M_1$. Then $e_{1i}x \in M_1$, and $e_{1i}x = e_{11}(e_{1i}x) \in e_{11}M_1$ $\subseteq e_{11}M_2\subseteq M_2$. Thus $e_{1i}x\in M_2$, and $e_{ii}x=e_{i1}(e_{1i}x)\in e_{i1}M_2\subseteq M_2$. Hence $e_{i,i}x \in M_2$ for $i=1, \dots, n$, and since $e_{11} + \dots + e_{nn}$ is the unit element of R_n , $x \in M_2$. Thus $M_1 \subseteq M_2$ is proved. If $e_{11}M_1 = e_{11}M_2$ then clearly $M_1 = M_2$. Hence we have proved that ϕ is univalent and preserves inclusion. Let A_1 be any R-submodule of A, and let M_1 be the set of all elements x in M such that $e_1, x \in A_1$ for all $i = 1, \dots, n$. Then M_1 is an R_n -submodule of M, for if $x \in M_1$ then $e_{ij}x \in M_1$ for $i, j=1, \dots, n$ and $[a]x \in M_1$ for all a in R, since $e_{1k}(e_{ij}x) = \delta_{ki}e_{1j}x \in A_1$, where δ_{k_i} is the Kronecker delta. Since [a] and e_{1i} permute, and A_1 is an R-submodule of A, $[a]x \in M_1$, so that M_1 is proved to be an R_n -submodule of M. We shall show that $A_1 = e_{11}M_1$. Since $e_{11}x \in A_1$ for all elements x of M_1 , we have $e_{11}M_1\subseteq A_1$. Let $x\in A_1$; then since $A_1 \subseteq A = e_{11}M$, $x = e_{11}x'$ for some $x' \in M$, and $e_{11}x = x \in A_1$, $e_{1i}x = e_{1i}(e_{11}x)$ =0 for i>1. Therefore $x\in M_1$, and $x=e_{11}x\in e_{11}M_1$. Thus $A_1=e_{11}M_1$ is proved.

To prove the second part of Theorem 1 let A be a given R-module. Let M be the totality of n-uples (x_1, \dots, x_n) of elements of A. If we define addition in M by adding component-wise, M becomes an additive group (direct sum of n copies of A). Let (a_{ij}) be an arbitrary element of R_n , and define $(a_{ij})(x_1, \dots, x_n) = (y_1, \dots, y_n)$ by $y_i = a_{i1}x_1 + \dots + a_{in}x_n$ for $i = 1, \dots, n$. Then M becomes an R_n -module, and the R-module $a_{i1}M$ is clearly isomorphic to the R-module A. That $L(R_n, M) \cong L(R, A)$ follows as in the proof of the first half of Theorem 1, so that Theorem 1 is completely proved.

4. Proof of Theorem 2. Suppose that the f.t.p.g. holds in $\mathfrak{F} = \{R, S, \cdots\}$ under π , that M is an R_n -module, and that $L(R_n, M)$

$$x^{\tau} = e_{11}(e_{11}x)^{\sigma} + e_{21}(e_{12}x)^{\sigma} + \cdots + e_{n1}(e_{1n}x)^{\sigma}.$$

Note that $(e_{1i}x)^{\sigma}$ is meaningful for $x \in M$ and $i = 1, \dots, n$, since $e_{1i}x = e_{1i}(e_{1i}x) \in e_{11}M$. We shall show that τ is an isomorphism of M and N. Since σ is an isomorphism of $e_{11}M$ to $e_{11}N$, we have easily $(x+y)^{\tau} = x^{\tau} + y^{\tau}$. If $x^{\tau} = 0$, then $e_{1i}x^{\tau} = 0$ and therefore $e_{1i}e_{1i}(e_{1i}x)^{\sigma} = e_{11}(e_{1i}x)^{\sigma} = 0$. Since $(e_{1i}x)^{\sigma} \in e_{11}N$ we have $(e_{1i}x)^{\sigma} = e_{11}(e_{1i}x)^{\sigma} = 0$. Hence $e_{1i}x = 0$, since σ is an isomorphism. Then $e_{1i}x = e_{1i}e_{1i}x = 0$ for $i = 1, \dots, n$. Therefore x = 0. Now we have to show that for any $z \in N$ there is an $x \in M$ such that $z = x^{\tau}$. Since $e_{1i}z = e_{11}(e_{1i}z) \in e_{11}N$ there exists an element x_i in $e_{11}M$ such that $e_{1i}z = x_i^{\sigma}$. Put $x = e_{11}x_1 + e_{21}x_2 + \cdots + e_{n1}x_n$. Then $e_{1i}x = e_{1i}x_i = x_i$. Hence $e_{1i}z = (e_{1i}x)^{\sigma}$, and $e_{ii}z = e_{i1}(e_{1i}x)^{\sigma}$. Therefore $z = x^{\tau}$. Thus we have proved that τ is an isomorphism of M to N. Now for any $a \in R$ and $x \in M$ we have

$$([a]x)^{\sigma} = \sum_{i=1}^{\sigma} e_{i1}(e_{1i}[a]x)^{\sigma} = \sum_{i=1}^{\sigma} e_{i1}([a]e_{1i}x)^{\sigma}$$

$$= \sum_{i=1}^{\sigma} e_{i1}[a^{\sigma'}](e_{1i}x)^{\sigma} = [a^{\sigma'}] \sum_{i=1}^{\sigma} e_{i1}(e_{1i}x)^{\sigma}$$

$$= [a^{\sigma'}]x^{\sigma},$$

and $(e_{ij}x)^{\tau} = e_{i1}(e_{1j}x)^{\sigma} = e_{ij}x^{\tau}$. Therefore for any $(a_{ij}) \in R_n$ and $x \in M$ we have $((a_{ij})x)^{\tau} = (a_{ij}^{\sigma})x^{\tau}$. Finally we have to show that M_1^* = $\{x^{\tau} | x \in M_1\}$ for an arbitrary R_n -submodule M_1 of M. We note that $y^{\tau} = y^{\sigma}$ for all $y \in e_{11}M$. Let x be in M_1 . Since we have $e_{1i}M_1^* = \{y^{\sigma} | y \in e_{11}M_1\}$, and since $e_{1i}x \in e_{11}M_1$, we have $e_{1i}x^{\tau} = (e_{1i}x)^{\tau} = (e_{1i}x)^{\sigma} \in e_{11}M_1^*$. Hence $e_{ii}x^{\tau} \in e_{i1}M_1^* \subseteq M_1^*$. Therefore $x^{\tau} \in M_1^*$. Conversely, let z be in M_1^* . Then we can find x_i in $e_{11}M_1$ such that $e_{1i}z = x_i^{\sigma} = x_i^{\tau}$. Hence $e_{ii}z = e_{i1}x_i^{\tau} = (e_{i1}x_i)^{\tau}$ and $z = \sum (e_{i1}x_i)^{\tau} = (\sum e_{i1}x_i)^{\tau}$. Clearly $x = \sum e_{i1}x_i$ is in M_1 , and $z = x^{\tau}$. Thus we have proved that the lattice isomorphism of $L(R_n, M)$ to $L(S_n, N)$ is induced by the group-isomorphism τ . Theorem 2 is completely proved.

5. Applications. Theorem 1 shows that for any division ring Φ and any Φ_n -module M the lattice $L(\Phi_n, M)$ is complementary.

To move from a projective geometry over Φ to one over Φ_n more effectively, we need lattice-theoretic definitions of a few concepts in vector spaces. Let L be a lattice with join \cup and meet \cap . We shall write $X \leq Y$ if $X \cap Y = X$. Assume that L has a smallest element 0, that is, 0 is an element such that $0 \le X$ for all $X \in L$. A finite set X_1, \dots, X_r of elements $\neq 0$ in L are said to be independent if $X_i \cap (X_1 \cup \cdots \cup X_{i-1} \cup X_{i+1} \cup \cdots \cup X_r) = 0$ for $i = 1, \cdots, r$. A set $\{X_{\alpha}\}$ of elements are said to be independent if every finite subset of $\{X_{\alpha}\}$ is independent. An element $X \neq 0$ in L is said to be minimal if $X \ge Y > 0$ implies X = Y. An independent set $\mathfrak{B} = \{X_{\alpha}\}$ of minimal elements is called a basis of L if for every minimal element X there exist finite number of elements X_1, \dots, X_n in \mathfrak{B} such that X $\leq X_1 \cup \cdots \cup X_n$. The well-known basis theorem of vector spaces [1, p. 14] can easily be seen to be equivalent to the following: If Φ is a division ring then for any Φ -module A the lattice $L(\Phi, A)$ has a basis, and any two bases of $L(\Phi, A)$ have the same (cardinal) number of elements. Now Theorem 1 shows that for any Φ_n -module M the lattice $L(\Phi_n, M)$ has a basis, and that any two bases of $L(\Phi_n, M)$ have the same number of elements. From this we may readily prove the following extension of the basis theorem of vector spaces:

Let Φ be a division ring, n be a positive integer, and M be a Φ_n -module. Then there exists a set $\mathfrak{B} = \{x_{\alpha}\}$ of elements in M such that

- (i) $\Phi_n x_\alpha$ is isomorphic to the n-dimensional vector space over Φ for any x_α in \mathfrak{B} ,
- (ii) any element x in M can be expressed as a linear combination $x = a_1x_{\alpha_1} + \cdots + a_rx_{\alpha_r}$ with $x_{\alpha_1}, \cdots, x_{\alpha_r}$ in \mathfrak{B} and a_1, \cdots, a_r in Φ_n , (iii) $a_1x_{\alpha_1} + \cdots + a_rx_{\alpha_r} = 0$ with $x_{\alpha_1}, \cdots, x_{\alpha_r}$ in \mathfrak{B} and a_1, \cdots, a_r in Φ_n implies $a_1x_{\alpha_1} = \cdots = a_rx_{\alpha_r} = 0$. Any two sets \mathfrak{B} , \mathfrak{B}' satisfying (i)-(iii) have the same number of elements.

Theorem 2 gives us at once an extension of f.t.p.g. to the case of simple rings Φ_n , since for any family $\mathfrak{F} = \{\Phi, \Psi, \cdots\}$ of division rings f.t.p.g. holds under the condition π : "there are at least three independent elements" [1, p. 44]. A similar extension when R is the ring of all integers, if we use a result of Baer [3, p. 39]: If the abelian group G contains at least two independent elements of infinite order, and if H is an abelian group such that the lattice of all subgroups of G is isomorphic to that of H, then the lattice isomorphism is induced by an isomorphism of G and G. In this case we have to consider only torsion free modules.

Now let R be a ring and $A = R \oplus \cdots \oplus R$ be a direct sum of n copies of the additive group of R. If we define $ax = (aa_1, \cdots, aa_n)$ for $a \in R$ and $x = (a_1, \cdots, a_n) \in A$, then A becomes an R-module.

We assume that R satisfies the following two conditions:

- (i) Any lattice automorphism of L(R, A) is induced by some automorphism σ of A such that $(ax)^{\sigma} = a^{\sigma'}x^{\sigma}$ for every $a \in R$, $x \in A$, where σ' is an automorphism of R.
- (ii) Let P, Q be in the full matrix ring R_n . If PQ=1 then QP=1. Q will be denoted by P^{-1} .

THEOREM 3. Let a ring R and an integer n be such that the above two conditions (i), (ii) are satisfied. Then any automorphism α of the full matrix ring R_n is of the form:

$$(a_{ij})^{\alpha} = U^{-1}(a_{ij}^{\alpha'})U$$

where α' is an automorphism of R; and U is an element of R_n for which U^{-1} exists.

PROOF. We consider R_n as an R_n -module. Then $L(R_n, R_n)$ is the lattice of all left ideals of R_n . Let I be an arbitrary left ideal of R_n . If we set $\mathfrak{l}^{\alpha} = \{(a_{ij})^{\alpha} | (a_{ij}) \in \mathfrak{l} \}$, then α becomes a lattice-automorphism of $L(R_n, R_n)$. Now in view of the proof of Theorem 1, we know that $L(R_n, R_n) \cong L(R, A)$. Therefore there is a lattice-automorphism β of L(R, A) corresponding to the automorphism α of $L(R_n, R_n)$. By our assumption β is induced by an automorphism σ of A such that $(ax)^{\sigma} = a^{\sigma'}x^{\sigma}$ for $a \in R$, $x \in A$, where σ' is an automorphism of R. Now in view of the proof of the second part of Theorem 2 there is an automorphism τ of the additive group of R_n such that τ induces the same automorphism of $L(R_n, R_n)$ as α and such that $((a_{ij})(b_{ij}))^{\tau} = (a_{ij}^{\sigma\prime})(b_{ij})^{\tau}$ for any (a_{ij}) , $(b_{ij}) \in R_n$. We set $[1]^r = V$, then for any $(a_{ij}) \in R_n$ we have $(a_{ij})^{\tau} = (a_{ij}^{\sigma \prime}) V$. Since τ is an automorphism of the additive group of R_n , there exists an element (b_{ij}) such that $(b_{ij})^{\tau} = 1$, so that if we set $W = (b_{ii}^{\sigma})$ then 1 = WV. Now by our assumption [1] = VW. Therefore if we set $(a_{ij})^{\eta} = W(a_{ij}^{\sigma'}) V$ then η is an automorphism of R_n . It is easily seen that η induces the same lattice automorphism of $L(R_n, R_n)$ as τ , and consequently, as α .

Now we set $\iota = \alpha \eta^{-1}$. Then ι is an automorphism of R_n , which induces the identity lattice automorphism of $L(R_n, R_n)$. We set

$$P = \sum_{i=1}^{n} e'_{i1}e_{1i}, \qquad Q = \sum_{i=1}^{n} e'_{i1}e_{1i}.$$

Then $PQ = \sum e_{i1}^{\iota} e_{11} e_{1i}^{\iota}$. Since the left ideal $R_n e_{11}$ is invariant under the automorphism ι , we have $e_{i1}^{\iota} = S_i e_{i1}$ for some $S_i \in R_n$. Then $e_{i1}^{\iota} e_{11} = S_i e_{i1} e_{11} = S_i e_{i1} = e_{i1}^{\iota}$. Therefore $PQ = \sum e_{i1}^{\iota} e_{i1}^{\iota} = \sum e_{i1}^{\iota} = (\sum e_{ii})^{\iota} = [1]$. Hence QP = [1]. Now we consider the automorphism γ of R_n , defined

by

$$X^{\gamma} = QX^{i}P = \sum_{i=1}^{\gamma} e_{i1}e_{1i}^{i}X^{i}e_{j1}^{i}e_{ij}.$$

Then $e_{ij}^{\gamma} = e_{i1}e_{1j} = e_{i1}e_{1j} = e_{ij}$ for any i, $j = 1, 2, \dots, n$. Now for any [a], $[a]^{\gamma}$ commutes with all $e_{ij}^{\gamma} = e_{ij}$. Hence $[a]^{\gamma} = [b]$ for some $b \in \mathbb{R}$. It is easily seen that τ induces an automorphism of the ring of all matrices of the form [a]. Therefore, there exists an automorphism γ' of R such that $[a]^{\gamma} = [a^{\gamma'}]$ for all $a \in \mathbb{R}$. Then for any $(a_{ij}) \in \mathbb{R}_n$ we have $(a_{ij})^{\gamma} = (a_{ij}^{\gamma'})$, and $(a_{ij})^{\gamma} = P(a_{ij}^{\gamma'})Q$. Therefore, from $\alpha = \iota \eta$, we have $(a_{ij})^{\alpha} = (a_{ij})^{\gamma \eta} = P^{\eta}(a_{ij}^{\gamma'})^{\eta}Q^{\eta} = P^{\eta}W(a_{ij}^{\gamma''\sigma'})VQ = U^{-1}(a_{ij}^{\alpha'})U$ where we set $U = VQ^{\eta}$, $\alpha' = \gamma'\sigma'$. Thus Theorem 3 is proved.

From Baer's Theorem [3, p. 39] we know that the ring I of all integers satisfies the above condition (i) for all n. Since I can be imbedded in a field, (ii) is also satisfied for all n. From Theorem 3, therefore, it follows that any automorphism of the full matrix ring I_n is inner.

The author wishes to express his gratitude to Professor S. A. Jennings for help and encouragement in the preparation of this work.

REFERENCES

- 1. R. Baer, Linear algebra and projective geometry, Academic Press, 1952.
- 2. ——, A unified theory of projective spaces and finite abelian groups, Trans. Amer. Math. Soc. vol. 52 (1942) pp. 283-343.
- 3. —, The significance of the system of subgroups for the structure of the group, Amer. J. Math. vol. 61 (1939) pp. 1-44.
- 4. ____, Automorphism rings of primary abelian operator groups, Ann. of Math. vol. 44 (1943) pp. 192-226.

THE UNIVERSITY OF BRITISH COLUMBIA