MATRICES OF RATIONAL INTEGERS

OLGA TAUSSKY

1. Introduction. This subject is very vast and very old. It includes all of the arithmetic theory of quadratic forms, as well as many of other classical subjects, such as latin squares and matrices with elements $+1$ or -1 which enter into Euler's, Sylvester's or Hadamard's famous conjectures. In recent years statistical research into block designs on one hand and research into finite projective geometries on the other hand have led to a large amount of progress in this area. Thirdly the possibility of help from high speed computers has raised new hopes and stimulated new research.

Under our subject comes the whole of the theory of the unimodular group in n dimensions and that of the modular group with all its ramifications into number theory and function theory including complex multiplication. The study of space groups and parts of crystallography belongs to our subject also.

Matrix theory is a natural part of algebra. However many difficult problems do not seem to yield easily to purely algebraic methods. I refer for instance to much modern research on eigen values. Either geometrical or analytical methods seem to be called to the rescue. On the other hand, much inspiration is obtained from the study of matrices with elements in a ring and not in a field. This sometimes brings out the finer nature of the theorems considered. So it seems that not only the methods of abstract algebra, but also those of analysis, geometry and number theory play an increasing role in matrix theory.

This account is divided into several chapters. Each has its own bibliography which is not intended to be complete. In particular in the chapters concerned with classical material much of the older literature is completely ignored.

BIBLIOGRAPHY

1A. COMBINATORIAL PROBLEMS

1. R. C. Bose, *Mathematical theory of the symmetrical factorial design*, Sankhyā vol. 8 (1947) pp. 106–166.

An address delivered before the Annual Meeting of the Society in Monterey, California, on April 18, 1959 by invitation of the Committee to Select Hour Speakers for Far Western Sectional Meetings; received by the editors June 5, 1959.

1a. R. C. Bose, S. S. Shrikhande and E. T. Parker, *Further results on the construction of mutually orthogonal latin squares and the falsity of Euler's conjecture*, Canad. J. Math. vol. 12 (1960) pp. 189–203 (contains further references).

2. R. H. Bruck and H. J. Ryser, *The nonexistence of certain projective planes*, Canad. J. Math. vol. 1 (1949) pp. 88–93.

3. S. Chowla and H. J. Ryser, *Combinatorial problems*, Canad. J. Math. vol. 2 (1950) pp. 93–99.

4. J. H. Curtiss, editor, *Numerical analysis*, Proceedings of the Sixth Symposium in Applied Mathematics, New York, 1956.

5. R. E. Gomory, *An algorithm for integer solutions to linear programs*, Princeton-IBM Math. Research Project, Technical Report 1, 1958.

6. J. Hadamard, *Résolution d'une question relative aux déterminants*, Bull. Sci. Math. (2) vol. 17 (1893) pp. 240–246.

7. M. Hall, *Uniqueness of the projective plane with 57 points*, Proc. Amer. Math. Soc. vol. 4 (1953) pp. 912–916.

8. ———, *Projective planes and related topics*, California Institute of Technology, 1954.

9. M. Hall, J. D. Swift and R. J. Walker, *Uniqueness of the projective plane of order eight*, Math. Tables and other Aids to Comp. vol. 10 (1956) pp. 186–194.

10. A. J. Hoffman and J. B. Kruskal, *Integral boundary points of convex polyhedra*, Annals of Mathematics Studies, no. 38, Princeton, 1956, pp. 223–246.

11. A. J. Hoffman, M. Newman, E. G. Straus and O. Taussky, *On the number of absolute points of a correlation*, Pacific J. Math. vol. 6 (1956) pp. 83–96.

12. H. W. Kuhn and A. W. Tucker, editors, Annals of Mathematics Studies, no. 38, Princeton, 1956.

13. H. B. Mann, *On orthogonal latin squares*, Bull. Amer. Math. Soc. vol. 50 (1944) pp. 249–257.

14. T. S. Motzkin, *The assignment problem*, Proceedings of the Sixth Symposium in Applied Mathematics, New York, 1956, pp. 109–125.

15. R. E. A. C. Paley, *On orthogonal matrices*, J. Math. Phys. vol. 12 (1933) pp. 311–320.

16. H. J. Ryser, *Matrices with integer elements*, Amer. J. Math. vol. 84 (1952) pp. 769–773.

17. ———, *Geometries and incidence matrices*, Amer. Math. Monthly vol. 62 (1955) pp. 25–31.

18. ———, *Combinatorial properties of matrices of zeros and ones*, Canad. J. Math. vol. 9 (1957) pp. 371–377.

19. O. Taussky, *Some computational problems concerning integral matrices*, Proceedings of the Sicily Congress, 1956.

20. C. B. Tompkins, *Machine attacks on problems whose variables are permutations*, Proceedings of the Sixth Symposium in Applied Mathematics, New York, 1956, pp. 195–211.

21. P. Turán, *On a problem in the theory of determinants*, Acta Math. Sinica vol. 5 (1955) pp. 411–423.

1B. THE MODULAR GROUP

1. H. S. M. Coxeter and W. O. J. Moser, *Generators and relations for discrete groups*, Berlin, Springer, 1957.

2. H. S. M. Coxeter, *On subgroups of the unimodular group*, J. Math. Pures Appl. (9) vol. 37 (1958) pp. 317–319.

3. E. C. Dade, *Abelian groups of unimodular matrices*, Illinois J. Math. vol. 3 (1959) pp. 11–27.

4. J. Dieudonné, *La geométrie des groupes classiques*, Berlin, Springer, 1955.

5. K. Goldberg, *Unimodular matrices of order 2 that commute*, J. Washington Acad. Sci. vol. 46 (1956) pp. 337–338.

6. K. Goldberg and M. Newman, *Pairs of matrices of order two which generate free groups*, Illinois J. Math. vol. 1 (1957) pp. 446–448.

7. L. K. Hua and I. Reiner, *On the generators of the symplectic modular group*, Trans. Amer. Math. Soc. vol. 65 (1949) pp. 415–426.

8. ———, *Automorphisms of the unimodular group*, Trans. Amer. Math. Soc. vol. 71 (1951) pp. 331–348.

9. ———, *Automorphisms of the projective unimodular group*, Trans. Amer. Math. Soc. vol. 72 (1952) pp. 467–473.

10. A. Hurwitz, *Die unimodularen Substitutionen in einem algebraischen Zahlenkörper*, Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa., 1895, pp. 332–356.

11. A. Karass and D. Solitar, *On free products*, Proc. Amer. Math. Soc. vol. 9 (1958) pp. 217–221.

12. J. Landin and I. Reiner, *Automorphisms of the general linear group over a principal ideal domain*, Ann. of Math. vol. 65 (1957) pp. 519–526.

13. ———, *Automorphisms of the two-dimensional general linear group over a euclidean ring*, Proc. Amer. Math. Soc. vol. 9 (1958) pp. 209–216.

14. ———, *Automorphisms of the Gaussian unimodular group*, Trans. Amer. Math. Soc. vol. 87 (1958) pp. 76–89.

15. M. Newman, *Structure theorems for modular subgroups*, Duke Math. J. vol. 22 (1955) pp. 25–32.

16. ———, *An alternative proof of a theorem on unimodular groups*, Proc. Amer. Math. Soc. vol. 6 (1955) pp. 998–1000.

17. ———, *The normalizer of certain modular subgroups*, Canad. J. Math. vol. 8 (1956) pp. 29–31.

18. ———, *An inclusion theorem for modular groups*, Proc. Amer. Math. Soc. vol. 8 (1957) pp. 125–127.

19. M. Newman and I. Reiner, *Inclusion theorems for congruence subgroups*, Trans. Amer. Math. Soc. vol. 91 (1959) pp. 369–379.

19a. J. Nielsen, *Die Isomorphismengruppe der freien Gruppen*, Math. Ann. vol. 91 (1924) pp. 169–209.

19b. ———, *Die Gruppe der drei-dimensionalen Gittertransformationen*, Danske-Vidensk. Selskabs. Math. Fys. vol. 5 (1924) pp. 3–29.

20. H. Rademacher, *Zur Theorie der Dedekindschen Summen*, Math. Z. vol. 63 (1955) pp. 445–463.

21. I. Reiner, *Symplectic modular complements*, Trans. Amer. Math. Soc. vol. 77 (1954) pp. 498–505.

22. ———, *Maximal sets of involutions*, Trans. Amer. Math. Soc. vol. 79 (1955) pp. 459–476.

23. ———, *Automorphisms of the symplectic modular group*, Trans. Amer. Math. Soc. vol. 80 (1955) pp. 35–50.

24. ———, *Real linear characters of the symplectic modular group*, Proc. Amer. Math. Soc. vol. 6 (1955) pp. 987–990.

25. ———, *A new type of automorphism of the general linear group over a ring*, Ann. of Math. vol. 66 (1957) pp. 461–466.

26. ———, *Normal subgroups of the unimodular group*, Illinois J. Math. vol. 2 (1958) pp. 142–144.

27. I. Reiner and J. D. Swift, *Congruence subgroups of matrix groups*, Pacific J. Math. vol. 6 (1956) pp. 529–540.

28. C. L. Siegel, *Discontinuous groups*, Ann. of Math. vol. 44 (1943) pp. 674–689.

29. O. Taussky and J. Todd, *Commuting bilinear transformations and matrices*, J. Washington Acad. Sci. vol. 46 (1956) pp. 373–375.

30. O. Taussky, Research problem 10, Bull. Amer. Math. Soc. vol. 64 (1958) pp. 124.

1c. QUADRATIC FORMS

1. H. Davenport, *Minkowski's inequality for the minimum associated with a convex body*, Quart. J. Math. Oxford Ser. vol. 10 (1939) pp. 119–121.

1a. M. Kneser, *Klassenzahlen definiter quadratischer Formen*, Arch. Math. vol. 8 (1958) pp. 241–250.

2. ———, *Klassenzahlen quadratischer Formen*, Jber. Deutsch. Math. Verein. vol. 61 (1958) pp. 76–88.

3. Chao Ko, *Determination of the class number of positive quadratic forms in nine variables with determinant unity*, J. London Math. Soc. vol. 13 (1938) pp. 102–110.

4. ———, *On the positive definite quadratic forms with determinant unity*, Acta Arith. vol. 3 (1939) pp. 79–85.

5. W. Ledermann, *An arithmetical property of quadratic forms*, Comment. Math. Helv. vol. 33 (1959) pp. 34–37.

5a. K. Mahler, *On Minkowski's theory of reduction of positive quadratic forms*, Quart. J. Math. Oxford Ser. vol. 9 (1938) pp. 259–262.

6. H. Minkowski, *Zur Theorie der positiven quadratischen Formen*, Ges. Abh., 1, Leipzig, Teubner, 1911, pp. 212–218.

6a. ———, *Diskontinuitätsbereich für arithmetische Äquivalenz*, Ges. Abh., 2, Leipzig, Teubner, 1911, pp. 53–100.

7. L. J. Mordell, *The definite quadratic forms in eight variables with determinant unity*, J. Math. Pures Appl. vol. 17 (1938) pp. 41–46.

8. M. Newman and O. Taussky, *Classes of positive definite unimodular circulants*, Canad. J. Math. vol. 9 (1956) pp. 71–73.

9. R. E. O'Connor and G. Pall, *The construction of integral quadratic forms of determinant* 1, Duke Math. J. vol. 11 (1944) pp. 319–331.

10. G. Pall, *The arithmetical invariants of quadratic forms*, Bull. Amer. Math. Soc. vol. 51 (1945) pp. 185–197.

11. ———, *Representation by quadratic forms*, Canad. J. Math. vol. 1 (1949) pp. 344–364.

12. G. Pall and O. Taussky, *Application of quaternions to the representation of a binary quadratic form as a sum of four squares*, Proc. Roy. Irish Acad. vol. 58 (1957) pp. 23–28.

12a. R. Remak, *Über die Minkowskische Reduktion der definiten quadratischen Formen*, Comp. Math. vol. 5 (1938) pp. 368–391.

13. C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Ann. of Math. vol. 36 (1935) pp. 527–606.

14. ———, *Über die analytische Theorie der quadratischen Formen.* II, Ann. of Math. vol. 37 (1936) pp. 230–263.

15. ———, *Über die analytische Theorie der quadratischen Formen.* III, Ann. of Math. vol. 38 (1937), pp. 212–291.

16. ———, *Einheiten quadratischer Formen*, Abh. Math. Sem. Univ. Hamburg vol. 13 (1939) pp. 209–239.

17. B. L. van der Waerden, *Die Reduktionstheorie der positiven quadratischen Formen*, Acta Math. vol. 96 (1956) pp. 265–309.

18. H. Weyl, *Theory of reduction for arithmetical equivalence*, Trans. Amer. Math. Soc. vol. 48 (1940) pp. 126–164.

19. ———, *Theory of reduction for arithmetical equivalence*. II, Proc. London Math. Soc. vol. 47 (1942) pp. 268–289.

1D. SPACE GROUPS AND CRYSTALLOGRAPHY

1. J. J. Burckhardt, *Die Bewegungsgruppen der Kristallographie*, Basel, Birkhäuser, 1947.

2. H. Zassenhaus, *Über einen Algorithmus zur Bestimmung der Raumgruppen*, Comment. Math. Helv. vol. 21 (1948) pp. 117–141.

2. **Elementary number theory.** The role of matrices with rational integers as elements is a double one. On one hand these matrices can be treated as a generalization of the ordinary rational integers and then we can try to see what happens to the usual number theoretical concepts and theorems. We can study common divisors, common multiples, diophantine equations, etc. New concepts can be added, e.g., instead of studying squares of numbers we can now study matrices of the form AA' where A' is the transpose of A. This is quite a famous subject. More generally we have transformations of the form ABA', so called congruent transformations and the study of the automorphs. Congruent matrices are said to belong to the same class and there is only a finite number of classes of symmetric matrices with rational integral elements and given nonzero determinants. This has been particularly studied for positive definite matrices with determinant 1.

Then there are the problems concerned with constructing normal forms of such matrices, such as the triangular Hermite normal form and the diagonal Smith normal form with the theory of elementary divisors.

Also every symmetric matrix with elements in a principal ideal ring is congruent to a triple diagonal matrix.

Bibliography

2. ELEMENTARY NUMBER THEORY FOR MATRICES

1. E. Cahen, *Theorie des nombres* I, Paris, Hermann, 1914.

2. A. Châtelet, *Groupes abéliens finis*, Paris, Gauthier-Villars, 1925.

3. L. G. du Pasquier, *Zahlentheorie der Tettarionen*, Vierteljschr. Naturf. Ges. Zürich vol. 51 (1906) pp. 55–129.

4. C. Hermite, *Sur l'introduction des variables continues dans la théorie des nombres*, J. Reine Angew. Math. vol. 41 (1851) pp. 191–216.

5. C. C. MacDuffee, *Theory of matrices*, Berlin, Springer, 1933.

6. ———, *Matrices with elements in a principal ideal ring*, Bull. Amer. Math. Soc. vol. 39 (1933) pp. 564–584.

7. G. Pall, *Representation by quadratic forms*, Canad. J. Math. vol. 1 (1949) pp. 344–364.

8. I. Reiner, *Unimodular complements*, Amer. Math. Monthly vol. 43 (1956) pp. 246–247.

9. H. J. S. Smith, *On systems of linear indeterminate equations and congruences*, Philos. Trans. Roy. Soc. London vol. 151 (1861) pp. 293–326.

10. O. Veblen and P. Franklin, *On matrices whose elements are integers*, Ann. of Math. vol. 23 (1921) pp. 1–15.

3. **Number theory in hypercomplex systems.** Deeper uses of these matrices occur in algebraic number fields and more generally in linear algebras. Here again the role is a double one. Every linear algebra can be isomorphically replaced by a ring of matrices and therefore number theory in hypercomplex systems is equivalent to number theory in certain rings of matrices. Much work has been done here. The work on number theory in the ring of integral quaternions is classical. Even integral Cayley numbers were studied, comparatively recently and independently by several people. It was found that all ideals are principal. Cayley numbers, however, do not come under the heading "matrix rings" as they are nonassociative.

Important work on number theory in general associative hypercomplex systems goes back to Artin, Brandt, Chevalley, Eichler, Hasse, K. Hey, Schilling.

Bibliography

3. Number theory in hypercomplex systems

1. E. Artin, *Zur Arithmetik hyperkomplexer Zahlen*, Abh. Math. Sem. Univ. Hamburg vol. 5 (1928) pp. 261–289.

2. H. Brandt, *Idealtheorie in Quaternionenalgebren*, Math. Ann. vol. 99 (1928) pp. 1–29.

3. ———, *Idealtheorie in einer Dedekindschen Algebra*, Jber. Deutsch. Math. Verein. vol. 37 (1928) pp. 5–7.

4. C. Chevalley, *L'arithmétique dans les algèbres de matrices*, Actualités Sci. Ind. no. 323 (1936).

5. H. S. M. Coxeter, *Integral Cayley numbers*, Duke Math. J. vol. 13 (1946) pp. 561–578.

6. M. Deuring, *Algebren*, Berlin, Springer, 1935.

7. L. E. Dickson, *Arithmetic of quaternions*, Proc. London Math. Soc. vol. 20 (1922) pp. 225–232.

8. ———, *A new simple theory of hypercomplex integers*, Bull. Amer. Math. Soc. vol. 29 (1923) p. 121.

9. ———, *Algebras and their arithmetics*, Chicago, University Press, 1923.

10. ———, *Algebren und ihre Zahlentheorie*, Zürich, Orell Füsseli, 1927.

11. M. Eichler, *Bestimmung der Idealklassenzahl in gewissen normalen einfachen Algebren*, J. Reine Angew. Math. vol. 176 (1937) pp. 192–202.

12. H. Hasse, *Über $\mathfrak{p}$-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme*, Math. Ann. vol. 104 (1931) pp. 495–534.

13. K. Hey, *Analytische Zahlentheorie in Systemen hyperkomplexer Zahlen*, Dissertation, University of Hamburg, 1929.

14. A. Hurwitz, *Über die Zahlentheorie der Quaternionen*, Ges. Abh. II, Basel, Birkhäuser, 1933, pp. 303–330.

15. C. G. Latimer, *On ideals in generalized quaternion algebras*, Trans. Amer. Math. Soc. vol. 38 (1935) p. 436.

16. R. Lipschitz, *Recherches sur les transformations, par des substitutions réelles, d'une somme de deux ou de trois carrés en elle-même*, J. Math. Pures Appl. vol. 4 (1886) pp. 373–439.

17. K. Mahler, *On ideals in the Cayley-Dickson algebra*, Proc. Roy. Irish Acad. vol. 48 (1943) pp. 123–133.

18. G. Pall, *On the arithmetic of quaternions*, Trans. Amer. Math. Soc. vol. 47 (1940) pp. 487–500.

19. ———, *On generalized quaternions*, Trans. Amer. Math. Soc. vol. 59 (1946) pp. 280–332.

20. G. Pall and O. Taussky, *Application of quaternions to the representations of a binary quadratic form as a sum of four squares*, Proc. Roy. Irish Acad. vol. 58 (1957) pp. 23–28.

21. R. A. Rankin, *A certain class of multiplicative functions*, Duke Math. J. vol. 13 (1946) pp. 281–306.

22. O. Schilling, *Über gewisse Beziehungen zwischen der Arithmetik hyperkomplexer Zahlsysteme und algebraischer Zahlkörper*, Math. Ann. vol. 111 (1935) p. 372.

23. A. Speiser, *Allgemeine Zahlentheorie*, Vierteljschr. Naturf. Ges. Zürich. vol. 71 (1926) pp. 8–41.

24. ———, *Idealtheorie in rationalen Algebren*, "Algebras and their arithmetics," Chicago, University Press, 1923, Chapter 13.

4. **Ideal theory.** On the other hand ideal theory in algebraic number fields and more general hypercomplex systems can be treated by the use of integral matrices. This was already recognized by Châtelet who set up a correspondence between ideals in an algebraic number field and matrices with rational integral elements. Poincaré's earlier theory of ideals in quadratic fields is a special case of Châtelet's. During the last decades the links between ideal theory and integral matrices were particularly emphasized, studied and enriched by MacDuffee in his book and in a number of research papers.

Bibliography

4. Ideal theory in algebraic number fields and linear algebras via matrix theory

1. A. Châtelet, *Sur certain ensembles de tableaux et leur application à la théorie des nombres*, Thèse, Annales Scientifiques de l'École Normale Supérieure vol. 28 (1911) pp. 105–202.

2. M. Deuring, *Algebren*, Berlin, Springer, 1935.

3. C. C. MacDuffee, *A method for determining the canonical basis of an ideal in an algebraic field*, Math. Ann. vol. 105 (1931) pp. 663–665.

4. ———, *Modules and ideals in a Frobenius algebra*, Monatsh. Math. vol. 48 (1939) pp. 293–313.

5. ———, *An introduction to the theory of ideals in linear associative algebras*, Trans. Amer. Math. Soc. vol. 31 (1928) pp. 71–90.

6. H. Poincaré, *Sur un mode nouveau de représentation géometrique des formes quadratiques définies ou indéfinies*, Journal de l'École Polytechnique vol. 47 (1880) pp. 177–245.

7. G. Shover and C. C. MacDuffee, *Ideal multiplication in a linear algebra*, Bull. Amer. Math. Soc. vol. 37 (1931) pp. 434–438.

8. G. Shover, *Class numbers in a linear associative algebra*, Bull. Amer. Math. Soc. vol. 39 (1933) pp. 610–614.

5. **Classes of matrices.** As a special application of ideal theory in hypercomplex systems Latimer and MacDuffee studied the ring of all polynomials $p(A)$, with integral coefficients, where A is an $n\times n$ matrix of rational integers which has as minimum polynomial $f(x)\equiv x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$ where the a_i are rational integers and $a_n\neq 0$. The zeros of $f(x)$ are further assumed all different. The aim was to show that there exists a 1-1 correspondence between the classes of integral $n\times n$ matrices which are roots of $f(x)=0$ and have $f(x)$ as minimum polynomial and the ideal classes in the ring mod $f(x)$. By the class of an integral matrix A is understood the set of all matrices $X^{-1}AX$ where X is a unimodular matrix with rational integral elements.

In the case that $f(x)$ is an irreducible polynomial this correspondence can be established particularly simply and opens up a great number of further investigations. It will now be discussed in greater detail.

Classes of matrices show particularly clearly some of the differences which occur between matrices of complex numbers and between matrices of integral numbers, or more generally, between fields and rings.

It is well known that the numbers which are roots of a polynomial equation

$$f(x) \equiv a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0, \qquad a_0 \neq 0$$

are linked up with the $n\times n$ matrices A for which $f(A)=0$. Assume the a_i and the coefficients of A to be complex numbers, and $f(x)$ to have all its zeros different. Then, if A is one matrix root, with $f(x)$ as minimum polynomial, all others are of the form $S^{-1}AS$ where S is any nonsingular $n\times n$ matrix. Since one such matrix root, the companion matrix, is well known the problem of finding matrix roots of such a polynomial appears much easier than the problem of finding number roots.

If, however, $f(x)$ is assumed to have integral numbers as coefficients, and $a_0=1$, then the problem of finding all matrix roots with

integral numbers as coefficients is considerably harder. While for S an integral matrix with $|S| = \pm 1$ every matrix of the form $S^{-1}AS$ is again a root, the converse does not hold any longer. The companion matrix remains a matrix root in the new sense too, however. All matrix roots can be divided into classes $S^{-1}AS$ where A is a fixed matrix root and S runs through all unimodular matrices. In the case where $f(x)$ is irreducible in the rational number field it can be shown that there is a 1-1 correspondence between the classes of matrix roots of $f(x)=0$ and the ideal classes in the ring $R(\alpha)$ of all polynomials with integral coefficients in α, where α is a scalar root of $f(x)=0$. The correspondence can be defined by the relation

$$A\begin{pmatrix}\alpha_1\\ \cdot\\ \cdot\\ \cdot\\ \alpha_n\end{pmatrix} = \alpha\begin{pmatrix}\alpha_1\\ \cdot\\ \cdot\\ \cdot\\ \alpha_n\end{pmatrix} \tag{1}$$

where $\alpha_1, \cdots, \alpha_n$ are the components of an eigen vector of A with respect to the eigen value α. This eigen vector is unique apart from a common multiple and its components can be chosen in $R(\alpha)$. That the set $\sum r_i\alpha_i$, with r_i integers, forms an ideal in $R(\alpha)$ follows at once from the relation (1). It is further clear that $S^{-1}AS$ which has the eigen vector $S^{-1}(\alpha_1, \cdots, \alpha_n)'$ defines the same ideal since S is unimodular. In this way, a correspondence between the classes of matrix roots and the ideal classes is set up which is 1-1. It follows immediately that the number of classes of matrix roots is finite.

The commutative composition of matrix classes thus defined is not easy to express in matrix language. It was studied by Poincaré for quadratic fields. I shall describe one way of obtaining a matrix root C which corresponds to the product of the ideals $(\alpha_1, \cdots, \alpha_n)$ and $(\beta_1, \cdots, \beta_n)$ with corresponding matrices A and B. Consider the product

$$\begin{aligned}(\alpha_1, \cdots, \alpha_n)(\beta_1, \cdots, \beta_n) &= (\alpha_1\beta_1, \alpha_2\beta_1, \cdots, \alpha_n\beta_1, \alpha_1\beta_2, \alpha_2\beta_2, \cdots, \alpha_n\beta_2, \cdots, \alpha_1\beta_n,\\ &\qquad \alpha_2\beta_n, \cdots, \alpha_n\beta_n)\end{aligned}$$

and apply a unimodular $n^2 \times n^2$ transformation S with rational integral elements which transforms this vector into

$$(\gamma_1, \cdots, \gamma_n, 0, \cdots, 0).$$

Here $(\gamma_1, \cdots, \gamma_n)$ is a modular basis for the product of the ideals considered. It is then easy to see that the $n^2 \times n^2$ matrix

$$S\begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix}S^{-1}$$

has in the upper left corner an $n\times n$ matrix C of rational integers which has α as characteristic root and $(\gamma_1, \cdots, \gamma_n)$ as corresponding characteristic vector. The lower left $(n^2-n)\times n$ block in the large matrix is zero.

The inverse of a matrix class defined by the matrix A (in the case that $1, \alpha, \cdots, \alpha^{n-1}$ form an integral basis for the integers in the field generated by α) is given by the matrix A'. (See Taussky.) This fact makes the study of matrix classes of order 2 rather easy and interesting. If A is a matrix root contained in a class of order 2 then $A' = S^{-1}AS$ for some integral unimodular S. In particular, it can happen that such a class contains a symmetric matrix. For quadratic fields $R(m^{1/2})$, where m is a square free integer, this can happen only if m is a sum of two squares. An example of a field which contains a matrix class of order 2 with a symmetric element and another matrix class of order 2 without a symmetric element is $R([410]^{1/2})$. A splitting up of the ideal classes of order 2 in quadratic fields in two types is well known, namely the ones with and the ones without an invariant ideal. The splitting up of the matrix classes of order 2 into the two types discussed above is somehow related to it (see Faddeev, Gorshkov, Taussky).

A matrix class of order 2 contains a symmetric matrix if and only if every matrix A contained in it is connected with its transposed A' by a relation

$$A' = (TT')^{-1}ATT'$$

where T is integral and unimodular. It was shown by Minkowski that for $n\leqq 7$ every positive definite unimodular matrix is a product TT' with T integral while this is not necessarily true for $n>7$. Hence the cases $n\leqq 7$ play a different role compared with $n>7$. This is also apparent in the result of Faddeev who studied polynomials with rational integers as coefficients which are characteristic polynomials of symmetric matrices of rational integers. He also linked them up with ideal classes of order 2. Gorshkov studied 3×3 symmetric matrices of rational numbers which have irreducible characteristic polynomials. He showed that an eigenvalue of such a matrix generates a cubic field in which three elements exist which are orthogonal

to their conjugates. Conversely, such a cubic field can be generated by an element which is an eigen value of a symmetric matrix.

The class of the companion matrix does not always contain a symmetric matrix. The problem is here much the same as for matrix classes of order 2. Observe also that every matrix S for which $S^{-1}AS = A'$ is symmetric.[1] For $n=2$ and for $f(x)=x^2+px+q$ the companion matrix is

$$\begin{pmatrix} 0 & 1 \\ -q & -p \end{pmatrix}$$

and the matrix S is then of the form

$$\begin{pmatrix} d & b \\ b-qd & -pb \end{pmatrix}$$

with b, d arbitrary integers. If S is unimodular then its determinant, $-(b+pd/2)^2+(p^2/4-q)d^2$, is the negative norm of a unit in the field of roots of $f(x)$. This shows that the determinant of S can be chosen as $+1$ only if $R(\alpha)$ has a unit of norm -1. For $n>2$ the determinant of S is the product of a power of -1, a norm in $R(\alpha)$ and the square of a rational number.

If $f(x)$ is any irreducible polynomial with integral coefficients and real zeros $\alpha_1, \cdots, \alpha_n$ then a symmetric matrix with $\alpha_1, \cdots, \alpha_n$ as eigen values can always be found, but not always an $n \times n$ matrix (see Krakowski).

Instead of looking for matrix classes which contain a symmetric matrix one can look for classes containing a normal matrix. For $n=2$ this leads, apart from the symmetric cases, only to the matrices corresponding to Gaussian integers. Special normal matrices with rational elements were investigated by A. A. Albert.

If the powers of α do not form an integral basis for the field generated by α then the ideal classes do not form a group since some of them have no inverses, e.g. in the ring generated by $(-35)^{1/2}$ the ideal $\mathfrak{a}=(2, 1+(-35)^{1/2})$ is equivalent to its square. The matrix

$$\begin{pmatrix} -1 & 2 \\ -18 & 1 \end{pmatrix}$$

and its transpose both correspond to $\mathfrak{a}$. The ideal class which corresponds to the transposed matrix, in the general case, is the so-called

[1] This is true in any case even if A is not a matrix of integers and even if the characteristic polynomial is reducible, as long as it coincides with the minimal polynomial (see Taussky and Zassenhaus, *On the similarity transformation between a matrix and its transpose*, Pacific J. Math. vol. 9 (1959) pp. 893–896).

complementary ideal class.[2] If $\mathfrak{a}=(\alpha_1, \cdots, \alpha_n)$ then this complementary ideal class is generated by $b=(\beta_1, \cdots, \beta_n)$ where trace $(\alpha_i\beta_k)=\delta_{ik}$. It is expected that in general the complementary ideal class is connected with[3] a "pseudo-inverse" in the semi-group of the ideal classes in $R(\alpha)$.

The classes of unimodular 2×2 matrices of integers were recently studied by Rademacher. A new set of invariants for the classes were given. Only matrices with negative trace were considered. For trace $\leqq -3$ there is a finite number of classes. For trace $=-2$ the matrix has a double characteristic root and there are infinitely many classes. If M is one matrix root then M^{-1} or $-M^{-1}$ is again a root according as $|M|=1$ or -1. The matrix M is similar (via a unimodular integral matrix) to M^{-1} (or $-M^{-1}$)—which is similar to M' via a unimodular matrix—if and only if the corresponding ideal class is equal to its conjugate class—which is equivalent to the inverse class.

This last fact is an example of the following fact: In a normal field we obtain n matrix roots from one matrix root by using the regular representation of the number roots and the polynomial relation that exists between any two of them. These matrix roots can be looked upon as "conjugate" matrices. Even if the field is not normal several of its conjugate fields could coincide so that some of the matrices could still be "conjugate." Conversely, one matrix root gives rise to an ideal class for each of its eigen vectors which lie in the same field. These are called conjugate ideal classes, anyhow.

In the irreducible case any matrix root A defines an irreducible representation for the whole $R(\alpha)$ and $S^{-1}AS$, for unimodular S, defines an equivalent representation. All irreducible representations by rational integer matrices are obtained in this way. Hence the number of irreducible inequivalent representations with integer elements is equal to the number of ideal classes in $R(\alpha)$. In this way the theory appears as a special case of a theorem of Steinitz, which was also studied by Zassenhaus, and used by Reiner for the study of integral representations of the cyclic group of prime order.

Let $\mathfrak{v}$ be a Dedekind ring which is a finitely-generated torsion free module. Then every finitely-generated torsion free $\mathfrak{v}$-module is $\mathfrak{v}$-isomorphic to a direct sum $\mathfrak{a}_1\oplus \cdots \oplus\mathfrak{a}_n$ of ideals in $\mathfrak{v}$. The number n and the product of the ideal class as of the $\mathfrak{a}_i$ are invariants and

[2] See Dedekind, *Ges. Werke* III, Braunschweig, Vieweg, 1932, p. 58.

[3] It was shown recently by Drazin, *Pseudo-inverses in associative rings and semigroups*, Amer. Math. Monthly vol. 65 (1958) pp. 506–514, that in certain semi-groups "pseudo-inverses" can be defined in a unique way. For finite semi-groups this is always possible.

determine the module up to $\mathfrak{b}$-isomorphism.

This theorem of Steinitz was also used by I. Schur to study representations of finite groups by $n \times n$ matrices in a given algebraic number field and to show that the representation can be carried out by integers in this field if n is relatively prime to the class number of the field. This generalizes a well known theorem of Burnside.

BIBLIOGRAPHY

5. MATRIX ROOTS OF POLYNOMIAL EQUATIONS

1. A. A. Albert, *Rational normal matrices satisfying the incidence relation*, Proc. Amer. Math. Soc. vol. 4 (1953) pp. 554–559.

2. R. P. Bambah and S. Chowla, *On integer roots of the unit matrix*, Proc. Nat. Inst. Sci. India vol. 13 (1937) pp. 241–246.

3. D. K. Faddeev, *On the characteristic equations of rational symmetric matrices*, Dokl. Akad. Nauk SSSR (*N.S.*) vol. 58 (1947) pp. 753–754.

4. D. S. Gorshkov, *Kubische Körper und symmetrische Matrizen*, C. R. (Doklady) Acad. Sci. SSSR vol. 31 (1941) pp. 842–844.

5. F. Krakowski, *Eigenwerte und Minimalpolynome symmetrischer Matrizen in kommutativen Körpern*, Comment. Math. Helv. vol. 32 (1958) pp. 224–240.

6. C. G. Latimer and C. C. MacDuffee, *A correspondence between classes of ideals and classes of matrices*, Ann. of Math. vol. 34 (1933) pp. 313–316.

7. H. Rademacher, *Zur Theorie der Dedekindschen Summen*, Math. Z. vol. 63 (1955) pp. 445–463.

8. I. Reiner, *Integral representations of cyclic groups of prime order*, Proc. Amer. Math. Soc. vol. 8 (1957) pp. 142–146.

9. E. Steinitz, *Rechteckige Systeme und Moduln in algebraischen Zahlkörpern.* I, Math. Ann. vol. 71 (1911) pp. 328–354.

10. ———, *Rechteckige Systeme und Moduln in algebraischen Zahlkörpern.* II, Math. Ann. vol. 72 (1912) pp. 297–345.

11. O. Taussky, *On a theorem of Latimer and MacDuffee*, Canad. J. Math. vol. 1 (1949) pp. 300–302.

12. ———, *Classes of matrices and quadratic fields*, Pacific J. Math. vol. 1 (1951) pp. 127–131.

13. ———, *Classes of matrices and quadratic fields* II, J. London Math. Soc. vol. 27 (1952) pp. 237–239.

14. ———, *On matrix classes corresponding to an ideal and its inverse*, Illinois J. Math. vol. 1 (1957) pp. 108–113.

15. O. Taussky and J. Todd, *Matrices with finite period*, Proc. Edinburgh Math. Soc. vol. 6 (1939) pp. 128–134. (This contains a list of earlier references.)

16. ———, *Matrices of finite period*, Proc. Roy. Irish Acad. vol. 46 (1940) pp. 113–121.

17. H. Zassenhaus, *Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz ganzzahliger Substitutionsgruppen*, Abh. Math. Sem. Univ. Hamburg vol. 12 (1938) pp. 276–288.

6. **Group matrices.** Representation theory is also the main source of the next chapter.

The group matrix $(x_{PQ^{-1}})$ associated with a group of order n and

elements $P, Q, \cdots$ is obtained from the regular representation. The n elements $x_P, x_Q, \cdots$ are indeterminates associated in a 1-1 correspondence with the group elements. The first row is formed by the group elements in a fixed, but arbitrary order, the other rows are then determined. If the group is cyclic the matrix is called a circulant, though sometimes this name is used for its determinant. The determinant of the general group matrix is called the group determinant. The irreducible factors of the group determinant are well known from the theory of group representations. Not much work has been done on the eigenvalues.[4] If special numerical values are substituted for the x_P then we speak about a "group matrix" or "group determinant." If the group matrix is written as a linear form in the x_P with coefficients matrices of 0's and 1's then it is a representation of the group ring of the group. For these coefficient matrices form the regular representation of the same group. This establishes a 1-1 correspondence between the elements of the abstract group ring and group matrices.

Among the group matrices with integral elements of a fixed group the unimodular ones seem of special interest. Consider such a matrix and the corresponding element of the abstract group ring with rational integers as coefficients. It can be shown that this element is a so-called unit, i.e., another element of the same group ring exists such that their product is the unit element of the group. The converse is also true. To prove this, let the first row of the group matrix be $x_P, x_Q, \cdots$. The corresponding element in the group ring is then $\sum_P x_P P$. Let $\sum_Q y_Q Q$ be any other element in the group ring for integer y's. The product of these two elements is

$$\sum_{P,Q} x_P y_Q P \cdot Q = \sum_R z_R \cdot R$$

where

$$z_R = \sum_Q x_{RQ^{-1}} y_Q.$$

This system of n equations in the n unknowns and with the unimodular matrix $(x_{RQ^{-1}})$ as coefficient matrix can be solved to give $z_R = 1$ if R is the unit element and $z_R = 0$ if R differs from the unit element.

Conversely, assume that $z_R = 1$ if R is the unit element of the group and $z_R = 0$ if R differs from the unit element. This implies that the product of the two matrices $(x_{PQ^{-1}})$ and $(y_{PQ^{-1}})$ is a permutation of the unit matrix and hence that $(x_{PQ^{-1}})$ is unimodular.

[4] See, however, E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. Reine Angew. Math. vol. 167 (1931) pp. 147–152.

Units in group rings have been discussed by G. Higman. In particular he showed that for a finite abelian group no unit of finite order exists apart from the group elements. It was further proved that units outside the group elements exist for all abelian groups unless all elements are of order 2, 3, 4 or 6.

A proof for this result for cyclic groups by means of unimodular group matrices—circulants in this case—was given recently as well by Newman and Taussky.

Both unimodular group matrices and units in the group ring form groups. It is easy to see that they are isomorphic.

Group matrices and even positive definite ones are also closed under the so-called Hadamard product for matrices

$$(a_{ik})(b_{ik}) = (a_{ik}b_{ik});$$

however unimodular group matrices are not closed under this multiplication.

To use group matrices instead of units has certain advantages. E.g., for matrices the concepts of symmetric and normal matrices exist and allow the formulation of further problems. E.g. the following theorem (Newman and Taussky) was obtained recently: *A unimodular $n\times n$ circulant of integers which is of the form AA' where A is an $n\times n$ matrix of integers is also of the form CC' where C is again an $n\times n$ circulant of integers.*

In the case of nonabelian groups units of finite order other than the group elements can occur. For the symmetric group on 3 letters consisting of the elements 1, a, a^2, b, ab, a^2b the following unit is of order 2: $-a+a^2-b+ab+ba$, (Taussky). Construct the corresponding group matrix and its transpose and multiply the corresponding units. The results are the following units:

$$(-a + a^2 - b + ab + ba)(a - a^2 - b + ab + ba)$$
$$= 5 - 2a - 2a^2 + 4ab - 4ba,$$
$$(a - a^2 - b + ab + ba)(-a + a^2 - b + ab + ba)$$
$$= 5 - 2a - 2a^2 - 4ab + 4ba.$$

These two units are of infinite order, and their corresponding group matrices have eigen values which are not roots of unity, namely $7\pm 4(3)^{1/2}$.

It is interesting to note that while the units $\pm a\mp a^2-b+ab+ba$ have no scalar part their product does have a scalar part $\neq 0$. The reason is that the group matrix corresponding to the product is positive definite and of the form AA', hence the corresponding quadratic

form represents odd and even integers. This implies that the coefficients of the squares in the form cannot all be even.

The eigenvalues of the group matrix corresponding to the unit

$$x_1 + x_2a + x_3a^2 + x_4b + x_5ab + x_6ba$$

are $[2x_1-x_2-x_3 \pm \{(2x_1-x_2-x_3)^2 \pm 4\}^{1/2}]/2$, ± 1, ± 1. This follows from representation theory, but can still be obtained by actual computation.

The elements generated by the units

$$-a + a^2 - b + ab + ba, \qquad a - a^2 - b + ab + ba$$

satisfy no other relations apart from that expressing that both units have order 2.

Another interesting unit in this group is $1+a-a^2+ab-ba$. It has the property that

$$(1 + a - a^2 + ab - ba)^n = 1 + na - na^2 + nab + nba$$

$$\text{for } n = 0, \pm 1, \pm 2, \cdots.$$

Multiplied with its "transpose" $1 - a + a^2 + ab - ba$ it gives $5-2a-2a^2-4b+4ab$ which has again infinite order.

The minors of group matrices have not received much attention. They show interesting symmetries in numerical examples, e.g. the symmetric 8×8 circulant with the first row

$$2,\ 1,\ 0,\ -1,\ -1,\ -1,\ 0,\ 1$$

has as leading principal minors

$$2,\ 3,\ 4,\ 4,\ 4,\ 3,\ 2,\ 1.$$

The symmetric 12×12 circulant with first row

$$3,\ 2,\ 1,\ 0,\ -1,\ -2,\ -2,\ -2,\ -1,\ 0,\ 1,\ 2$$

has as leading principal minors

$$3,\ 5,\ 8,\ 12,\ 16,\ 16,\ 16,\ 12,\ 8,\ 5,\ 3,\ 1.$$

Also the minors of the group matrices of the nonabelian group of order 6 show interesting symmetries.

Let us return to the theorem concerning unimodular $n\times n$ circulants of the form AA'.

It leads to a number of interesting problems which have not yet been investigated further:

(1) The corresponding question for group matrices corresponding to other groups.

(2) The following generalization suggested by Morris Newman: Let C, K be unimodular circulants of rational integers such that $C=AKA'$ where A is a unimodular matrix of rational integers. Can A be replaced by a circulant?

(3) The question as to which "classes" unimodular positive definite group matrices belong. It was shown by Minkowski that for $n \leqq 7$ every unimodular positive definite $n \times n$ matrix of rational integers is of the form AA' with A an $n \times n$ integral matrix, but that this is not the case for $n > 7$. If F is any fixed unimodular positive definite $n \times n$ matrix of rational integers then the set of matrices AFA' with A arbitrary integral and unimodular is called the class of F. For $n = 8$ there are two classes. It was shown by Newman and Taussky that a representative for each of these classes can be chosen as a circulant, the circulant with first row (2, 1, 0, -1, -1, -1, 0, 1) for the non-unit class. The corresponding question for larger n and more general groups seems of interest, in particular for the reason that group matrices are closed under multiplication while the classes of unimodular positive definite matrices do not have this property.

Postscript. The following progress concerning the questions raised in this lecture has been made, some at the Number Theory Institute at Boulder, 1959.

1. *Units of finite period in integral group rings.* Iwasawa constructed a large class of units of period 2 in the integral group ring of the S_3. By transforming a group element of order 3 by such an element of period 2 a unit of period 3 is obtained.

2. *The semi-group of ideal classes in $R(\alpha)$.* The author raised the question of studying the possible structures of the semi-group formed by the ideal classes in the ring $R(\alpha)$ formed by all polynomials in some algebraic integer α with rational integral coefficients, in particular the question of when this semi-group is the union of groups. Dade and Zassenhaus showed that this is true for all quadratic fields, but not, in general, for others. In the quadratic case every element has as its pseudo-inverse its inverse in the group in which it lies. This result is already contained in Gauss' work on quadratic forms. It is this pseudo-inverse which corresponds to the transposed matrix class.

3. *Symmetry of principal minors in special circulants.* The circulant with first row 2, 1, 0, -1, -1, -1, 0, 1 has as leading principal minors 2, 3, 4, 4, 4, 3, 2. It was pointed out by Davenport that this symmetry holds for any symmetric unimodular matrix (a_{rs}) which has the additional property

(1) symmetry in the nonprincipal diagonal, i.e.

$$a_{rs} = a_{n+1-s},\ n+1-r,$$

$$(2) \qquad (a_{rs})^{-1} = (a_{rs}) \quad \text{or} \quad (a_{rs})^{-1} = ((-1)^{r+s}a_{rs}).$$

For let $\Delta(u, v)$ denote the principal minor formed with the rows from u to v inclusive, and let $\Delta'(u, v)$ have the same meaning for the matrix $(a_{rs})^{-1}$. Then for any unimodular matrix it is known that

$$\Delta(1, r) = \Delta'(r+1, n).$$

By (2) above, $\Delta'(r+1, n) = \Delta(r+1, n)$ and by (1) above $\Delta(r+1, n) = \Delta(1, n-r)$. Hence

$$\Delta(1, r) = \Delta(1, n-r).$$

The 8×8 circulant in question has the property that $(a_{rs})^{-1} = ((-1)^{r+s}a_{rs})$. However, not all unimodular circulants have this property, e.g. the circulant with the first row $(3, -2, 1, 1, -2)$ does not.

Bibliography

6A. Integral group matrices

1. G. Higman, *The units of group rings*, Proc. London Math. Soc. vol. 46 (1940) pp. 231–248.
2. M. Newman and O. Taussky, *On a generalization of the normal basis in abelian algebraic number fields*, Comm. Pure Appl. Math. vol. 9 (1956) pp. 85–91.
3. ———, *Classes of positive definite unimodular circulants*, Canad. J. Math. vol. 9 (1956) pp. 71–73.
4. O. Taussky, *Normal matrices in algebraic number theory*, Proceedings of the International Congress of Mathematicians, Amsterdam, 1956.
5. ———, *Unimodular integral circulants*, Math. Z. vol. 63 (1955) pp. 286–289.

6B. Integral group representations

1. W. Burnside, *On the arithmetical nature of the coefficients in a group of linear substitutions*, Proc. London Math. Soc. (2) 7 (1908) pp. 8–13.
2. F. E. Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz*, Abh. Math. Sem. Univ. Hamburg vol. 14 (1938) pp. 357–412.
3. W. Gaschütz, *Über den Fundamentalsatz von Maschke zur Darstellungstheorie der endlichen gruppen*, Math. Z. vol. 56 (1952) pp. 376–387.
4. J. M. Maranda, *On the equivalence of representations of finite groups by groups of automorphisms of modules over Dedekind rings*, Canad. J. Math. vol. 7 (1955) pp. 516–526.
5. ———, *On $\mathfrak{y}$-adic integral representations of finite groups*, Canad. J. Math. vol. 5 (1953) pp. 344–355.
6. I. Kaplansky, *Modules over Dedekind rings and valuation rings*, Trans. Amer. Math. Soc. vol. 72 (1952) pp. 327–340.
7. I. Reiner, *Maschke modules over Dedekind rings*, Canad. J. Math. vol. 8 (1956) pp. 329–334.

8. ———, *Integral representations of cyclic groups of prime order*, Proc. Amer. Math. Soc. vol. 8 (1957) pp. 142–146.

9. I. Schur, *Arithmetische Untersuchungen über endliche Gruppen linearer Substitutionen*, S.-B. Preuss. Akad. Wiss. Berlin (1906) pp. 164–184.

10. ———, *Über Gruppen linearer Substitutionen mit Koeffizienten aus einem algebraischen Zahlkörper*, Math. Ann. vol. 71 (1911) pp. 355–367.

11. H. Zassenhaus, *Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz*, Abh. Math. Sem. Univ. Hamburg vol. 12 (1938) pp. 276–288.

CALIFORNIA INSTITUTE OF TECHNOLOGY