[P] R. Palais, *Seminar on the Atiyah-Singer index theorem*, Ann. of Math. Study no. 57, Princeton Univ. Press, Princeton, N. J., 1965.

[Pt] V. K. Patodi, *Curvature and the eigenforms of the Laplace operator*, J. Differential Geom. **5** (1971), 233–249.

[R1] J. Roe, *An index theorem on open manifolds*, J. Differential Geom. **27** (1988), 87–113.

[R2] ——, *Finite propagation speed and Connes' foliation algebra*, Proc. Cambridge Philos. Soc. **102** (1987), 459–466.

[S] R. T. Seeley, *Complex powers of an elliptic operator*, Proc. Sympos. Pure Math., vol. 10, Amer. Math. Soc., Providence, R. I., 1967, pp. 288–307.

JAMES L. HEITSCH
UNIVERSITY OF ILLINOIS

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 20, Number 1, January 1989

0273-0979/89 $1.00 + $.25 per page

Elliptic functions and rings of integers, by Ph. Cassou-Noguès and M. J. Taylor. Progress in Mathematics, vol. 66, Birkhäuser, Boston, Basel and Stuttgart, 1987, xvi + 198 pp., $29.50. ISBN 0-8176-3350-2

The idea of constructing prescribed algebraic number fields by means of the values of real or complex functions is usually referred to as the 'Jugendtraum,' a word used by Kronecker in an 1880 letter to Dedekind [8]. Hilbert made the realization of this idea the twelfth problem of his 1900 address [7], adding that he considered "... this problem as one of the most profound and far-reaching in the theory of numbers and of functions." In the present book, Cassou-Noguès and Taylor give an exposition of Taylor's recent work on an "integral Jugendtraum" for the rings of integers of ray class fields of imaginary quadratic fields. The object of this work is to construct by means of elliptic functions explicit generators of such rings of integers either as algebras or as Galois modules.

The two examples which motivated the Jugendtraum were provided by the finite abelian extensions of either the rational numbers $\mathbf{Q}$ or of an imaginary quadratic field. By the Kronecker-Weber Theorem, every abelian extension of $\mathbf{Q}$ is contained in a cyclotomic field of the form $\mathbf{Q}(\zeta_n)$, where $\zeta_n = \exp(2\pi i/n)$ is a primitive nth root of unity for some positive integer n. Thus the values of the function $e(z) = \exp(2\pi iz)$ at rational z generate all abelian extensions of $\mathbf{Q}$. One can view these z as the points of finite order on the one-dimensional real torus $\mathbf{R}/\mathbf{Z}$. Suppose now that $\mathbf{Q}$ is replaced by an imaginary quadratic field K. In this case the torus $\mathbf{R}/\mathbf{Z}$ may be replaced by a two-dimensional torus $\mathbf{C}/\Omega$, where Ω is a nonzero ideal of $\mathcal{O}_K$ and we view K as a fixed subfield of $\mathbf{C}$. An elliptic function for $\mathbf{C}/\Omega$ is a meromorphic function of $z \in \mathbf{C}$ whose value at z depends only on $z \bmod \Omega$. A division point of $\mathbf{C}/\Omega$ is a point of finite order on $\mathbf{C}/\Omega$. By work of Weber, Feuter and Hasse, there are elliptic functions for $\mathbf{C}/\Omega$ such that every abelian extension of K is contained in a ray class field generated over K by the values of these functions at suitable division points. There are different combinations of elliptic functions which generate the

abelian extensions of K in this way. For a precise statement of results of this kind, as well as the connection of these results to elliptic curves, see ξ III and ξ IX of the book under review, as well as [**14**].

Suppose now that L is an arbitrary number field, and that N is finite extension of L. Let $\mathcal{O}_N$ and $\mathcal{O}_L$ be the rings of integers of N and of L, respectively. Given the idea of constructing N by adjoining to L the values of certain functions, it is natural to ask how one can construct $\mathcal{O}_N$ by adjoining the values of such functions to $\mathcal{O}_L$. Here are some results concerning this integral form of Kronecker's Jugendtraum in the two cases we have discussed.

Suppose first that $N = \mathbf{Q}(\zeta_n)$ is a cyclotomic extension of $\mathbf{Q}$, where $\zeta_n = \exp(2\pi i/n)$ as before. A discriminant calculation shows that $\mathcal{O}_N$ is the ring $\mathbf{Z}[\zeta_n]$ obtained by adjoining ζ_n to $\mathbf{Z}$. Thus if L is any subfield of N, one has $\mathcal{O}_N = \mathcal{O}_L[\zeta_n]$. In a similar way, the subfield $N^+ = \mathbf{Q}(\zeta_n + \zeta_n^{-1})$ of N has ring of integers $\mathbf{Z}[\zeta_n + \zeta_n^{-1}] = \mathcal{O}_{L^+}[\zeta_n + \zeta_n^{-1}]$ when $L^+ = L \cap N^+$. A remarkable result of M. N. Gras [**6**] is that the only abelian extensions $N'/\mathbf{Q}$ of prime degree $l \geq 5$ for which $\mathcal{O}_{N'} = \mathbf{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_{N'}$ are the real cyclotomic extensions $N' = \mathbf{Q}(\zeta_n + \zeta_n^{-1})$, where $n = 2l + 1$.

A similar pattern occurs for the abelian extensions N of an imaginary quadratic field K. Suppose $\mathcal{A}$ is a nonzero integral ideal of $\mathcal{O}_K$. The counterpart of the field $\mathbf{Q}(\zeta_n)$ is the ray class classfield $K(\mathcal{A})$ of K of conductor $\mathcal{A}$. The fact that $\mathcal{O}_{\mathbf{Q}(\zeta_n)} = \mathbf{Z}[\zeta_n]$ suggests the problem of finding small subfields L of $K(\mathcal{A})$ such that $\mathcal{O}_{K(\mathcal{A})}$ is monogenic over $\mathcal{O}_L$, i.e., for which there is an α in $\mathcal{O}_{K(\mathcal{A})}$ for which $\mathcal{O}_{K(\mathcal{A})} = \mathcal{O}_L[\alpha]$. One would also like to give such an α explicitly as the division value of an elliptic function.

In the book under review, Taylor and Cassou-Noguès construct an α for which $\mathcal{O}_{K(\mathcal{A})} = \mathcal{O}_L[\alpha]$ when $\mathcal{A} = 4f$ for some odd ideal f and when L is the ray class field $K(4)$ of conductor $4\mathcal{O}_K$. They also prove that in this case, the ring of integers $\mathcal{O}_{N^+}$ of the compositum $N^+ = LK(f)$ is generated by a single element β over $\mathcal{O}_L$. The problem of descending L further towards K is a delicate one. In [**3**] Taylor and Cassou-Noguès conjecture that for all $\mathcal{A}$, $\mathcal{O}_{K(\mathcal{A})}$ is generated over $\mathcal{O}_{K(1)}$ by a single element, and they prove this if $\mathcal{A}$ is prime to 6. Complementing these positive results, J. Cougnard has recently shown (cf. [**4**]) an elliptic counterpart to the above Theorem of M. N. Gras.

Let us now return to the general situation of a finite Galois extension N/L of number fields. Let $G = \mathrm{Gal}(N/L)$, and let $L[G]$ be the group ring of G with coefficients in L. Thus far we have considered the problem of finding algebra generators for N over L, or of $\mathcal{O}_N$ over $\mathcal{O}_L$. A second natural problem is to find generators for N as a module for $L[G]$, or for $\mathcal{O}_N$ as a module for various subrings of $L[G]$. The largest subring Λ_L of $L[G]$ which acts on $\mathcal{O}_N$ is called the associated order of $\mathcal{O}_N$ in $L[G]$. Thus Λ_L is the ring of $\gamma \in L[G]$ such that $\gamma\beta \in \mathcal{O}_N$ for all $\beta \in \mathcal{O}_N$. Clearly $\mathcal{O}_L[G] \subseteq \Lambda_L$, and it is a theorem of E. Noether that $\mathcal{O}_L[G] = \Lambda_L$ if N/L is at most tamely ramified.

The normal basis theorem states that N always has a single generator as an $L[G]$ module. The structure of $\mathcal{O}_N$ as a module for various subrings of the associated order Λ_L is a subject with a lively history of its own. A

comprehensive account of this up through 1983 is given by Fröhlich in [5]. The two results which have most closely motivated the book of Taylor and Cassou-Noguès concern abelian extensions N of $L = \mathbf{Q}$. If $N/\mathbf{Q}$ is abelian and at most tamely ramified, Hilbert and Speiser showed that $\mathcal{O}_N$ is a free rank one module over $\Lambda_{\mathbf{Q}} = \mathbf{Z}[G]$, with a generator being given by the trace to N of a primitive root of unity in the minimal cyclotomic field which contains N. This was generalized by Leopoldt [11], who showed that for all abelian $N/\mathbf{Q}$, $\mathcal{O}_N$ is a free rank one module for the associated order $\Lambda_{\mathbf{Q}}$. Leopoldt in fact determined $\Lambda_{\mathbf{Q}}$ explicitly in terms of the ramification of $N/\mathbf{Q}$, and he constructed a generator for $\mathcal{O}_N$ as a $\Lambda_{\mathbf{Q}}$ module by means of Gauss sums.

Suppose now that K is an imaginary quadratic field, and that $\mathbf{P} = \lambda\mathcal{O}_K$ is an unramified principal prime ideal of K for which $\lambda \equiv \pm 1 \bmod 4\mathcal{O}_K$. Cassou-Noguès and Taylor study the counterpart of Leopoldt's Theorem when N is the ray classfield $K(4\mathbf{P}^{m+r})$ and L is the ray classfield $K(4\mathbf{P}^r)$, where m and r are integers for which $r \geq m \geq 1$. In this case they explicitly determine the associated order Λ_L of $\mathcal{O}_N$ in $L[G]$, and they show $\mathcal{O}_N$ is a locally free Λ_L module. If 2 splits in K, they show that $\mathcal{O}_N$ is a free rank one Λ_L module on a particular element α of $\mathcal{O}_N$ which is constructed via elliptic functions. (A somewhat more general form of these results was originally shown by Taylor in [19 and 21].) In a forthcoming paper, A. Srivastav shows that the condition that 2 splits in K can be removed.

A notable feature of the above results is that since $r \geq m \geq 1$, the extension N/L is wildly ramified at each place where it ramifies, these being the places of L over $\mathbf{P}$. Thus far there has been relatively little success in using explicit elliptic and modular function techniques to analyze in a comparable way tamely ramified extensions in which the top field is abelian over an imaginary quadratic field. This is one of the central open problems in the theory; for some related results, see [5, 12, 1, 2]. While on the topic of open problems, the Jugendtraum has been cited in connection with the theory of Shimura varieties (see [10],and also [9, 13]) and with Stark's conjectures [15–18]. The application of these ideas to integral versions of Jugendtraum of the kind we have discussed remains to be considered.

I will now discuss the chapters and organization of the book of Cassou-Noguès and Taylor. Chapter I motivates the elliptic results to come by means of the analogous results for abelian extensions of $\mathbf{Q}$. Chapters II and III contain general background material concerning classfield theory, elliptic functions, CM elliptic curves over $\mathbf{C}$, and a very brief discussion of the reduction of elliptic curves defined over number fields. In Chapters IV and V the authors study Feuter's elliptic functions $T(z)$ and $T_1(z)$ for a given period lattice $\Omega \subseteq \mathbf{C}$. These functions are simple expressions in the Weierstrass $\wp$-function $\wp(z)$ and its derivative. From now on we will assume that Ω is a nonzero ideal of $\mathcal{O}_K$ for some imaginary quadratic field K. The advantage of the Feuter functions is that in this case, they give rise to a model for the elliptic curve $\mathbf{C}/\Omega$ which is defined over $K(4)$, and which has good reduction outside of 2. This leads to considerable control over the ideals generated by the values of $T(z)$ and of $T_1(z)$ at division points ∂ of $\mathbf{C}/\Omega$. The guiding analogy used in Chapters IV and V is that the division

values $T(\partial)$ of $T(z)$ are the elliptic counterparts of $1-\zeta$ when ζ is a root of unity. Using work of Feuter, the authors develop the counterparts for these $T(\partial)$ of various results from the theory of cyclotomic fields. For example, they find the elliptic counterparts of cyclotomic polynomials. I wish that the authors had expanded some of their motivational remarks in Chapters IV and V concerning the arithmetic of elliptic curves. Alternately, it would have been useful to have an appendix outlining algebraic proofs of some of the results proved via complex function theory.

To consider the Galois module structure of $\mathcal{O}_N$ the authors introduce several further ideas. The first, in Chapter VI, is the notion of an Abel resolvent function. This is a linear combination $R(z)$ of translates by division points of the elliptic function $D(z) = T_1(z)/T(z)$. As in other Galois module structure problems, one wishes to reduce questions about the Galois structure of a ring of integers to questions about the ideals generated by the values of resolvents. In Chapters VII and VIII the authors apply the theory of the modular function to this problem. The first step is to relate the value of a resolvent $R(z)$ at a division point ∂ of $\mathbf{C}/\Omega$ to the value of a particular modular function $G_\partial(\gamma)$ at the point $\gamma = \gamma_0$ in the upper half plane $\mathcal{H}$ which corresponds to the lattice Ω. The authors then apply the q-expansion principle to $G_\partial(\gamma_0)$, which in this setting states that if f is a modular function, the singular values of f (i.e., the values of f at complex multiplication points $\gamma_0 \in \mathcal{H}$) are algebraic integers provided that the Fourier coefficients of f at every cusp are abelian algebraic integers. An analysis of the Fourier expansions of $G_\partial(\gamma)$ and $G_\partial(\gamma)^{-1}$ then leads to the desired results concerning $R(\partial)$. In Chapter IX, the authors use the q-expansion principle, coupled with congruences between various polynomials whose roots are singular values of modular functions, to prove various instances of the main Theorem of complex multiplication concerning the action of $\mathrm{Gal}(\overline{K}/K)$ on the division values of elliptic functions for $\mathbf{C}/\Omega$.

The last ingredient needed to study the structure of $\mathcal{O}_N$ as a module for its associated order Λ_L in $L[G]$ is contained in Chapter X. This is the explicit determination of Λ_L for the N/L in question, and a proof that $\mathcal{O}_N$ is locally free over Λ_L. These purely local results are proved using formal groups and an interesting integral version of Lubin-Tate theory for the integers of the abelian extensions of local fields.

The proofs of the main theorems are completed in Chapter X. In an appendix the Feuter functions $T(z)$ and $T_1(z)$ are compared to the standard theta functions for $\mathbf{C}/\Omega$, and their division values are compared to the elliptic units of Robert and Ramachandra.

This book is well written, and it should be useful both to specialists and students. One suspects that Kronecker himself would have felt at home with it, since the use complex function theory is emphasized rather than that of modern algebraic geometry over the integers. There are several chapters devoted to the needed background material, so the book could serve as an advanced graduate course text, though it would be useful to discuss concurrently some other texts on the arithmetic of elliptic curves. The authors' approach of minimizing the use of algebraic geometry will be

popular with many readers but not with everyone. Taylor's more recent paper [20] on the rings of integers of *CM* fields illustrates more fully how algebraic geometry can enter into this subject.

References

1. J. Brinkhuis, *Galois modules and embedding problems*, J. Reine Angew. Math. **346** (1984), 141–165.

2. ——, *Normal integral bases and complex conjugation*, J. Reine Angew. Math. **375/376** (1987), 157–166.

3. Ph. Cassou-Noguès and M. J. Taylor, *A note on elliptic curves and the monogeneity of rings of integers*, J. London Math. Soc. (2) **37** (1988), 63–72.

4. J. Cougnard, *Conditions nécessaires de monogénéité, application aux extensions cycliques de degré premier $l \geq 5$ d'un corps quadratique imaginaire*, J. London Math. Soc. (2) **37** (1988), 73–87.

5. A. Fröhlich, *Galois module structure of algebraic integers*, Ergebnisse 3 Folge Band I, Springer-Verlag, Berlin and New York, 1983.

6. M. N. Gras, *Non-monogénéite de l'anneau des entiers des extensions cycliques de* **Q** *de degré premier $l \geq 5$*, J. Number Theory **23** (1986), 347–353.

7. D. Hilbert, *Mathematical problems*, Lecture delivered at the International Congress of Mathematicians in Paris in 1900, Bull. Amer. Math. Soc. **8** (1902), 437–479.

8. L. Kronecker, Werke, Band V, (K. Hensel ed.), Teubner, Leipzig and Berlin, 1930.

9. R. Langlands, *Automorphic representations, Shimura varieties and motives. Ein Märchen*, Proc. Sympos. Pure Math., vol. **33**, Amer. Math. Soc., Providence, R.I., 1979, pp. 205–246.

10. ——, *Some contemporary problems with origins in the Jugendtraum*, Proc. Sympos. Pure Math., vol. **28**, Amer. Math. Soc., Providence, R.I., 1976, pp. 401–418.

11. H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. **201** (1959), 119–149.

12. L. McCulloh, *Galois module structure of abelian extensions*, J. Reine Angew. Math. **375/376** (1987), 259–306.

13. J. Milne, *Automorphic bundles on connected Shimura varieties*, Invent. Math. **92** (1988), 91–128.

14. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten and Princeton Univ. Press, Princeton, N.J., 1971.

15. H. M. Stark, *Hilbert's twelfth problem and L-series*, Bull. Amer. Math. Soc. **83** (1977), 1072–1074.

16. ——, *L-functions at $s = 1$. III. Totally real fields and Hilbert's Twelfth Problem*, Adv. in Math. **22** (1976), 64–84.

17. ——, *L-functions at $s = 1$. IV. First derivatives at $s = 0$*, Adv. in Math. **35** (1980), 197–235.

18. J. Tate, *Les Conjectures de Stark sur les fonctions L d'Artin en $s = 0$, Notes d'un cours à Orsay rédigées par D. Bernardi et N. Schappacher*, Birkhäuser, Boston, Basel, Stuttgart, 1984.

19. M. J. Taylor, *Formal groups and the Galois module structure of local rings of integers*, J. Reine Angew. Math. **358** (1985), 97–103.

20. ——, *Mordell-Weil groups and the Galois module structure of rings of integers*, Illinois J. Math. (to appear).

21. ——, *Relative Galois module structure of rings of integers and elliptic functions*, Math. Proc. Cambridge Philos. Soc. **94** (1983), 389–397; II, Ann. of Math. (2) **121** (1985), 519–535; III, Proc. London Math. Soc. (3) **51** (1985), 415–431.

TED CHINBURG
COLUMBIA UNIVERSITY