Norms of ideals in direct sums of number fields and applications to the circulants problem of Olga Taussky-Todd

submitted for the Degree of

MASTER OF SCIENCE

of the

UNIVERSITY OF GLASGOW

by

Paul Joseph Trafford

April 1992

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

M.Sc. Thesis Summary

This thesis, *'Norms of Ideals in direct sums of number fields and applications to the circulants problem of Olga Taussky-Todd,'* presents wide-ranging material in the Mathematical areas of Algebraic and Analytic Number Theory. The work, which is substantially original, is set out in three chapters which are supported by appendices.

As the title suggests, the main aim is to tackle a problem which was originally posed by Olga Taussky-Todd who asked what values can be taken by the determinant of a certain type of $n \times n$ matrix with integer entries — the circulant (see [15]).

Hitherto fragmentary algebraic results have been proved by M.Newman, using matrix manipulation ([5],[6]). However, for a given circulant, he gave no indication as to what proportion of integers are values. The thesis solves this problem by utilising a well-known relationship between determinants of matrix transformations and "absolute" norms of fractional ideals in a direct sum of number fields. By working appropriately in the latter structure, asymptotic methods are made available to complete the solution. A sketch of the mathematical strategy is given in the preface.

The overall approach is to start at the level of great generality in Chapter 1 where, by slight modification, there is a generalisation of some extensive results published by R.W.K.Odoni in recent mathematical journals (see e.g. [12]). Subsequently there is successive specialisation down to the case of the circulant. In Chapter 2, by using standard techniques of group characters and the arithmetic of cyclotomic fields there are proved a few new results for abelian group determinants. In the final chapter there are given new elementary proofs of results for particular circulants, first presented by Newman in [5,6]. Then the methodology of the first chapter is reprised to establish the most important original result of this thesis — that "almost all" integers with appropriate 'critical' exponents are values of a given circulant.

I declare that this thesis, submitted for the Degree of Master of Science at the University of Glasgow, has been duly composed by myself.

1992

Preface

This thesis, presented for the degree of M.Sc. (Research in Mathematics), consists substantially of new work undertaken with the supervision of Professor R.W.K.Odoni, to whom I am immensely grateful for his patience, good humour and most of all a seemingly boundless enthusiasm for mathematics; I wish him all the best for the future. I would also like to thank the staff and research students in the Mathematics Department at Glasgow University. Finally, I am indebted to the Science and Engineering Research Council for financial support during my studies.

The main task is to tackle a problem, originally posed by Olga Taussky-Todd, which asks, "What are the integer values which may be taken by a circulant with integer entries?" We present here a detailed quantitative solution; it seems that at present a complete characterisation of values cannot be given: during the course of our work we construct quite an elaborate extension of $\mathbf{Q}$, the field of rational numbers, by forming the Galois hull, H, of *ray-classes* (see Chapter 1 for a definition); if a characterisation existed, then there would need to be some suitable congruence relations on the primes in H, which is unlikely. We can, however, measure densities; by using the very general machinery of ray-classes in Chapter 1, we show in Chapter 3 that almost all integers with appropriate 'critical' exponents are values of circulants.

In addition to the work directed specifically at the circulants problem, we look at values of group determinants (for which the circulant is an example). We consider in some detail the case of elementary abelian p-groups. This material is presented in Chapter 2, where various methods are employed; in particular, we use group characters and the arithmetic of cyclotomic fields.

The results for general group determinants are, however, somewhat fragmen-

tary; the circulant is a very special case, for which the strategy for determining a quantitative solution is outlined below.

Definition The *circulant* of order n is given by

$$\Delta_n(\underline{x}) := \begin{vmatrix} x_0 & x_1 & \dots & x_{n-1} \\ x_{n-1} & x_0 & \dots & x_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \dots & x_0 \end{vmatrix}, \text{ where } x_0, \dots, x_{n-1} \in \mathbf{Z}.$$

It is easy to show that $\Delta_n(\mathbf{Z}^n)$ contains all r with $(r,n) = 1$ (see (L2) in Chapter 2). Thus it remains to determine, given a prime $p \mid n$, what m with $p \mid m$ are values of the circulant?

Relationship between group determinants and norms of ideals in algebras

Let G be any abelian group, $\#G = n$; then take $\mathbf{Q}G$, the group algebra of G over $\mathbf{Q}$; $\dim_{\mathbf{Q}} \mathbf{Q}G = n$. For any $\alpha \in \mathbf{Q}G$, we define $L_\alpha : \mathbf{Q}G \to \mathbf{Q}G$ by $x \mapsto \alpha x \ \forall x \in \mathbf{Q}G$. Then L_α is a $\mathbf{Q}$-linear map.

Definition The *group determinant* (denoted by $N(\alpha)$) := *det* L_α.

If we take $G = C_n$, $\alpha \in \mathbf{Z}G$, then the group determinant is a circulant of order n.

Let $A := \bigoplus_{j \in J} K_j$, where K_j are algebraic number fields, and let $S := \bigoplus_{j \in J} \mathbf{Z}_j$, the integral closure of $\mathbf{Z}$ in A. Integral ideals $\boldsymbol{a}$ in S (denoted by $\boldsymbol{a} \triangleleft S$) are those of the form $\bigoplus_{j \in J} \boldsymbol{a}_j$ where $0 \neq \boldsymbol{a}_j \triangleleft \mathbf{Z}_j$.

It is established in Theorem 9 for suitable A, that $A \cong_{\mathbf{Q}} \mathbf{Q}G$, while S contains the image of $\mathbf{Z}G$. For such A and S, we have also (Lemma A11): suppose $r \in \mathbf{Z}G$, $L_r : \mathbf{Q}G \to \mathbf{Q}G$ is $\mathbf{Q}$-linear, then $|det\ L_r| = N(rS)$.

These two relations prompt us to use the ideal theory of orders in direct sums of number fields.

For A and S determined in Theorem 9, let $\mathcal{O} = \mathbf{Z}G$; then $\mathcal{O}$ is an order in S. If $f = \#G$, then $fS \subseteq \mathcal{O}$. Owing to the poor ideal theory in S we work

mod fS and introduce ray-classes – a generalisation of ideal classes, with certain conditions imposed. We proceed to examine principal ideals $\boldsymbol{a}$ with generators in $\mathcal{O}$. So we look for a suitable characterisation of ideals $rS; r \in \mathcal{O}$, bearing in mind the need for relative ease in handling the quantitative analysis. This is achieved by expressing ideals as $\boldsymbol{a} = \boldsymbol{bg}$, where $\boldsymbol{b}$ consists only of prime ideal factors of fS and where $(\boldsymbol{g}, fS) = 1$. A key lemma (Lemma 1) enables us to generate plenty of partners $\boldsymbol{g}$ 'compatible' with $\boldsymbol{b}$ (which give rise to ideals of the form $\boldsymbol{a} = rS$ with suitable prime exponents), subsequently yielding enough for our purposes.

For the asymptotic analysis of the number of positive integers $\leq x$ which are norms of elements of $\mathcal{O}$, we introduce *ranges* which have the important property of being Frobenian multiplicative. Hence we are able to utilise the Chebotarev Density Theorem to reach the desired result, following the method of Odoni in [11] and [12].

P.Trafford

March 1992.

Contents

CHAPTER 1

Ideal Theory of Orders in a Direct Sum of Number Fields with Asymptotic Expansion for Ranges

0.Introduction

Let $K_1, K_2, \ldots, K_k$ be arbitrary number fields (i.e. finite extensions of the rational field $\mathbf{Q}$). Let $\mathbf{Z}_j$ be the corresponding ring of integers ($j = 1, \ldots, k$), i.e. the maximal orders of K_j. Let $A = \bigoplus_{j=1}^{k} K_j$, $S = \bigoplus_{j=1}^{k} \mathbf{Z}_j$. Then the integral ideals $\boldsymbol{a}$ in S (denoted by $\boldsymbol{a} \lhd S$) are those ideals $\boldsymbol{a} := \bigoplus_{j=1}^{k} \boldsymbol{a}_j; 0 \neq \boldsymbol{a}_j \lhd \mathbf{Z}_j$. Necessarily, if $\boldsymbol{a} \lhd S$ then $S/\boldsymbol{a}$ is a finite ring. Multiplication of these ideals is done componentwise as for ordinary integral ideals, and hence the term 'integral ideal' is appropriate; throughout Chapter 1 "ideal" will mean 'integral ideal'.

Suppose we have a ring $\mathcal{O}$, containing an identity element 1, such that $\mathcal{O} \subseteq S$ with finite index. Then $\mathcal{O}$ is an order of the direct sum of number fields. For $\boldsymbol{a} \lhd S$, denote by $N(\boldsymbol{a})$ the norm of $\boldsymbol{a}$ (thus $\#(S/\boldsymbol{a})$). In Chapter 1, we are interested in norms for principal ideals with generators in $\mathcal{O}$, i.e. for ideals of the form rS; $r \in \mathcal{O}$. Due to the poor ideal theory in $\mathcal{O}$, we work in the bigger ring S by introducing a 'conductor', $f \in \mathbf{N}$ (the set of natural numbers) such that $fS \subseteq \mathcal{O}$. The next two sections describe an appropriate characterisation for ideals ($mod^{\times} fS$) by introducing *ray-classes* and *ranges*. Certain properties of these enables us to determine a general analysis of asymptotic expansions for ranges, bringing the first chapter to a close.

1. Ray-Classes

We choose a conductor $f \in \mathbf{N}$ such that $fS \subseteq \mathcal{O}$: (letting $f = [S : \mathcal{O}]$ will do). Let $\boldsymbol{a}_1$,$\boldsymbol{a}_2$ be ideals in S. Then we define $\boldsymbol{a}_1$ to be *equivalent* to $\boldsymbol{a}_2$ (write $\boldsymbol{a}_1 \sim \boldsymbol{a}_2$) if and only if there exist $\lambda, \mu \in S$ such that $\lambda \boldsymbol{a}_1 = \mu \boldsymbol{a}_2$, with $\lambda \equiv \mu \equiv 1 \ (mod^{\times} fS)$; and with λ and μ having the same signature in the

Minkowski map (write $\lambda/\mu \gg 0$). The details of the Minkowski map are to be found in Appendix A.

Let $[\boldsymbol{a}] := \{x; x \sim \boldsymbol{a}\}$. As with ray-classes for solitary number fields, multiplication is defined for $\boldsymbol{a}_1, \boldsymbol{a}_2 \triangleleft S$ by $[\boldsymbol{a}_1]\cdot[\boldsymbol{a}_2] := [\boldsymbol{a}_1\,\boldsymbol{a}_2]$, and hence is well-defined. To impose a group structure we introduce the restriction $\boldsymbol{a}_1 + fS = \boldsymbol{a}_2 + fS = S$. Now let I be the set of equivalence classes satisfying all the conditions above. Then it is easy to show that $(I, \cdot)$ is a finite group under $\sim$ (see Appendix - LEMMA A1). As these equivalence classes are obviously extensions of ray-classes for the one summand case, we call them also 'ray-classes' – of S $(mod^{\times} fS)$. Note that if $\lambda, \mu \in S$ satisfy $\lambda - 1 \equiv \mu - 1 \equiv 0\ (mod^{\times} fS)$, then $\lambda - 1$ and $\mu - 1 \in \mathcal{O}$, hence $\lambda, \mu \in \mathcal{O}$; we include this in the definition of $\sim$. Having defined ray-classes, we look for systematic ways of handling principal ideals in S with generator in $\mathcal{O}$. We say an ideal $\boldsymbol{g}$ is 'good' if $(\boldsymbol{g}, fS) = S$, and $\boldsymbol{b}$ is 'bad' if $\boldsymbol{b}$ is composed only of prime ideal factors of fS.Thus $\forall \boldsymbol{a} \triangleleft S$, $\boldsymbol{a} = \boldsymbol{b}\boldsymbol{g}$ for some unique such $\boldsymbol{b}$,$\boldsymbol{g}$. The following Lemma utilises this decomposition, where $A^{\star}$ denotes the units of A.

LEMMA 1 *Suppose* $0 \neq r \in \mathcal{O}$ *and* $rS = \boldsymbol{b}\boldsymbol{g}$. *If* $\boldsymbol{g}' \sim \boldsymbol{g}$, *then* $\boldsymbol{b}\boldsymbol{g}' = r'S$, *where* $0 \neq r' \in \mathcal{O} \cap A^{\star}, r'/r \gg 0$.

Proof This is almost identical to the one summand case (see [7]). We have $\lambda \boldsymbol{g}' = \mu \boldsymbol{g}$, with $\lambda \equiv \mu \equiv 1\ (mod^{\times} fS), \lambda/\mu \gg 0$. So $\lambda(\boldsymbol{b}\boldsymbol{g}') = \mu \boldsymbol{b}\boldsymbol{g} = \mu r S$, a principal ideal. Since $(\lambda, fS) = (\mu, fS) = S$, it is clear that $\boldsymbol{b}\boldsymbol{g}'$ is principal, i.e. $\boldsymbol{b}\boldsymbol{g}' = \nu S$, for some $\nu \in S$. Then $\lambda\nu S = \mu r S$; hence $\lambda\nu = \mu r \epsilon$, where $\epsilon \in S^{\star}$, the units of S. $[S^{\star} := \bigoplus_{j=1}^{k} \mathbf{Z}_j^{\star}$, so $\epsilon = [\epsilon_1, \ldots, \epsilon_k]$ where $\epsilon_j \in \mathbf{Z}_j^{\star}, j = 1, \ldots, k]$. So $\lambda\nu\epsilon^{-1} = \mu r$, and we then have $\nu\epsilon^{-1} \equiv r\ (mod^{\times} fS)$. Hence $\nu\epsilon^{-1} \in \mathcal{O}$. Put $\nu\epsilon^{-1} = r'$ say. Thus $\lambda r' = \mu r$; on taking signatures, we have $r'/r = \mu/\lambda \gg 0$, while $\boldsymbol{b}\boldsymbol{g}' = r'S$ $\square$

In order to find asymptotics for the number of positive integers $\leq x$ which are norms of elements of $\mathcal{O}$, we first introduce ranges.

2.Ranges

Definition Suppose we are given a fixed signature $\underline{\sigma}$ and a fixed bad ideal $\boldsymbol{b}$. Then if $(rS) = (\boldsymbol{b})(\boldsymbol{g})$, with some $r \in \mathcal{O}$, sgn r=$\underline{\sigma}$, then $\boldsymbol{b}$ is said to be 'compatible with $\boldsymbol{g}$.'

Suppose $n \in \mathbf{N}$ and that $n = N(rS)$ is soluble for some $r \in \mathcal{O}$ with sgn $r = \underline{\sigma}$. We have $n = (N\boldsymbol{b})(N\boldsymbol{g}) = bg$, with $b, g \in \mathbf{N}$; b composed only of primes $p \mid f$, and g composed only of $p \nmid f$. We define $g \in \mathbf{N}$ to be 'good' if and only if $p \nmid g \ \forall p \mid f$, and let $b \in \mathbf{N}$ be 'bad' if and only if $p \mid b \Rightarrow p \mid f$. By unique factorisation in $\mathbf{N}$, every $n \in \mathbf{N}$ is uniquely expressible as bg; b bad, and g good.

Definition The 'Range of g', $\mathcal{R}(g) := \{[\boldsymbol{g}]; N\boldsymbol{g} = g\}$.

Hence $\mathcal{R}(g) \in 2^I = \{$ subsets of the ray-class group $(mod^{\times} fS)\}$, and $\mathcal{R}(g) = \emptyset$ if no $N\boldsymbol{g} = g$. By Lemma 1, if $\boldsymbol{b}$ is compatible with $\boldsymbol{g}$, $N\boldsymbol{b} = b$, $N\boldsymbol{g} = g$, $rS = \boldsymbol{bg}$, sgn $r' = \underline{\sigma}$, and if $\boldsymbol{g} \sim \boldsymbol{g'}$, where $N\boldsymbol{g'} = g'$, then $\boldsymbol{b}$ is compatible with $\boldsymbol{g'}$, and so $\exists r' \in \mathcal{O}$, sgn $r' = \underline{\sigma}$ such that $N(r'S) = bg'$.

Now let $s \in \mathbf{C}, Re\ s > 1$. We can express the last result analytically in the form:

$$F(s) = \sum_{n \in U} n^{-s} = \sum_{\mathcal{S} \in 2^I} \left(\sum_{g \in V} g^{-s} \right) \left(\sum_{b \in W} b^{-s} \right)$$

$$U = \{n \in \mathbf{N}; \exists r \in \mathcal{O} \text{ with } N(rS) = n \text{ and } sgn\ r = \underline{\sigma}\};$$

where $V = \{g \in \mathbf{N}; g \text{ good}, g = N\boldsymbol{g} \text{ for some } \boldsymbol{g} \text{ with } \mathcal{R}(g) = \mathcal{S}\};$

$$W = \{b \in \mathbf{N}; b \text{ bad}, b = N\boldsymbol{b}, \text{ compatible with some } \boldsymbol{g} \text{ with } [\boldsymbol{g}] \in \mathcal{S}\}.$$

Now $\sum_{b \in W} b^{-s}$ is analytic and bounded in every closed half plane of the type $Re\ s \geq \delta > 0$; thus, to a large extent, the singularities of $F(s)$ are governed by those of the various $\sum_{g \in V} g^{-s}$; to determine the behaviour of the latter, we need to find some properties of ranges.

If $A, B \in 2^I$, then define $A \circ B := \{ab; a \in A, b \in B\}$. (By convention, $A \circ \emptyset = \emptyset \circ A = \emptyset$, $\forall A \in 2^I$). Thus 2^I becomes a finite commutative monoid, partially ordered by inclusion (see Lemma 2 below) with identity being the singleton $\{\underline{1}\}$ where $\underline{1}$ is the principal class. Note that 2^I may be regarded as the power set of $\rho_1 \times \rho_2 \ldots \times \rho_k$; ρ_j = ray-class group $(mod^{\times} f\mathbf{Z}_j)$ of $K_j (j = 1, \ldots, k)$.

Notation $\mathbf{N}_m := \{n \in \mathbf{N}; (m, n) = 1\}$; in particular $\mathbf{N}_f = \{$ good g in $\mathbf{N}\}$.

LEMMA 2 *For* $g_1, g_2 \in \mathbf{N}_f$, $\mathcal{R}(g_1 g_2) \supseteq \mathcal{R}(g_1) \circ \mathcal{R}(g_2)$ *with equality if* g_1 *and* g_2 *are coprime; in particular* $\mathcal{R} : \mathbf{N}_f \to 2^I$ *is multiplicative.*

Proof This is easy (see Appendix A), following directly from analogy with the one summand case.

From this Lemma, we note that the range $\mathcal{R}(n)$ depends only on the prime factorisation of n. A lot of further information may be derived, all of which is analogous with the one summand case; we restrict our attention to those facts which are needed to calculate asymptotics.

Maximal Ranges and their characterisation

Consider the set of all ranges $\mathcal{R}(n); n \in \mathbf{N}$. Since 2^I is finite, the image $\mathcal{R}(\mathbf{N}_f)$ is finite, and so there exist ranges which are maximal with respect to inclusion in 2^I. We call these 'maximal ranges.' Let $\mathbf{1} := \{\underline{1}\}, \underline{1}$ = identity ray-class.

LEMMA 3 *There exists a unique maximal range which contains* $\mathbf{1}$*; it is a subgroup of* I.

Proof Let M be a maximal range containing $\mathbf{1}$. Let $M = \mathcal{R}(g_1)$. Then, by Lemma 2, $M^2 \subseteq \mathcal{R}(g_1^2)$. As $\mathbf{1} \in M$, we have $M \subseteq M^2 \subseteq \mathcal{R}(g_1^2)$. Thus $\mathcal{R}(g_1^2)$ is a range containing $\mathbf{1}$, while the maximality of M implies $M = M^2$, and so M is a subgroup of I because I is finite. Suppose now that M_1, M_2 are maximal ranges containing $\mathbf{1}$, and let $\mathcal{R}(g_1) = M_1, \mathcal{R}(g_2) = M_2$. Then $\mathcal{R}(g_1 g_2) \supseteq M_1 M_2 \supseteq M_1$

and also $M_1M_2 \supseteq M_2$; but $\mathbf{1} \in M_1 \cap M_2 \Rightarrow M_1M_2 = M_1 = M_2$ (as M_1, M_2 are maximal) $\square$

LEMMA 4 *The maximal ranges are precisely the cosets of H in I, where H is the unique maximal range containing* **1**.

Proof Let M be any maximal range. Suppose $\mathcal{R}(g) = M$, $\mathcal{R}(h) = H$. Then $\mathcal{R}(gh) \supseteq MH \supseteq M$. Hence $MH = M$ (while $M^nH = M^n \ \forall n \geq 1$). From this it is clear that M is a union of cosets of H. We show first that M is a single coset of H. Let $\mu_1, \mu_2 \in M$ and let $n = \#I$. Then $\mathbf{1} \in M^n$, and $M^n = HM^n \supseteq H$, i.e. $M^n \supseteq H$, while $\mathcal{R}(g^n) \supseteq M^n \supseteq H$. By the maximality of H, $M^n = H$. Now $\mathbf{1} = \mu_1^n$ and $\mu_1^{n-1}\mu_2 \in M^n = H$, hence $\mu_1^{-1}\mu_2 \in H$. So $\mu_1 H = \mu_2 H$, $\forall \mu_1, \mu_2 \in M$ and this implies $M = \mu_1 H = \mu_2 H$.

Now we show that each coset of H is a maximal range.

Given any class $\mathbf{x} \in I$, $\exists g \in \mathbf{N}_f$ with $\mathbf{x} \in \mathcal{R}(g) = M$ (maximal). Then $M = \mathbf{x}H \subseteq \mathcal{R}(g)H = \mathcal{R}(g)\mathcal{R}(h) \subseteq \mathcal{R}(gh)$, where $\mathcal{R}(h) = H$. This implies $\mathcal{R}(gh) = M$ and hence $\mathbf{x}H = \mathcal{R}(gh) = M$ is a maximal range $\square$

3. Frobenian Property of Ranges

Using the notation above, we have arbitrary number fields $K_1, \ldots, K_k$, with corresponding rings of integers $\mathbf{Z}_1, \ldots, \mathbf{Z}_k$. We have also $fS \subseteq \mathcal{O}$ for some $f \in \mathbf{N}$. Let ρ_j be the ray-class group of $K_j(mod^{\times} f\mathbf{Z}_j)$, $(j = 1, \ldots, k)$. Then denote by $\mathcal{M}$ the finite monoid consisting of all subsets of $\rho_1 \times \ldots \times \rho_k$, which is determined by letting $\mathcal{R}(n) := \{(\mathcal{C}_1, \ldots, \mathcal{C}_k \in \rho_1 \times \ldots \times \rho_k\}$such that for $j = 1, \ldots, k \ \exists 0 \neq \boldsymbol{a}_j \triangleleft \mathbf{Z}_j$ with $\prod_{j=1}^{n} N(\boldsymbol{a}_j) = n$ and $[\boldsymbol{a}_j] = \mathcal{C}_j\}$. We wish to characterise the ranges $\mathcal{R}(p^n)$ of $p \in \mathbf{N}_f$ in terms of prime ideals in a suitable extension of $\mathcal{R}$. In particular, we find appropriate conditions on primes $p \neq q \in \mathbf{N}_f$ such that $\mathcal{R}(p^n) = \mathcal{R}(q^n)$ $\forall n \in \mathbf{N}$, so that we may invoke the Chebotarev density theorem to obtain qualitative results on the distribution of norms 'of the right type.' The

following Lemma yields the desired conditions. First we recall the definition of a Frobenian multiplicative function.

Definition Suppose $\theta : \mathbf{N}_d \to \mathcal{M}$ is multiplicative, where $\mathcal{M}$ is a commutative monoid. Suppose $\exists$ a number field L such that

(i) $L/\mathbf{Q}$ is Galois;

(ii) No prime in $\mathbf{N}_d$ ramifies in $L/\mathbf{Q}$;

(iii) Whenever p,q are primes in $\mathbf{N}_d$, with $Frob(p, L/\mathbf{Q}) = Frob(q, L/\mathbf{Q})$, then $\forall n \geq 1$, $\theta(p^n) = \theta(q^n)$, where $Frob(p, L/\mathbf{Q})$ denotes the conjugacy class of p relative to L over $\mathbf{Q}$.

Then we say that θ is 'Frobenian multiplicative relative to $L/\mathbf{Q}$.'

LEMMA 5 *The range function is Frobenian multiplicative relative to $L/\mathbf{Q}$, for some L (defined below).*

Proof From Lemma 1, to prove $\mathcal{R}(p^n) = \mathcal{R}(q^n)$ $\forall n \in \mathbf{N}$, it will suffice to show in each $\mathbf{Z}_i$, that $p\mathbf{Z}_i$ and $q\mathbf{Z}_i$ have the same number of prime ideal factors of given residual degree and ray-class $(mod^{\times} f\mathbf{Z}_i)$, (for $i = 1, \ldots, k$). We construct a sufficiently large (finite) Galois extension L of $\mathbf{Q}$ so that this holds whenever we have distinct primes $p, q \in \mathbf{N}_f$, unramified in L, with $Frob(p, L/\mathbf{Q}) = Frob(q, L/\mathbf{Q})$. We choose L to be the Galois hull over $\mathbf{Q}$ of the compositum $\prod_{i=1}^{k} \mathcal{R}_i$; here $\mathcal{R}_i$ is the ray-class field of $K_i(mod^{\times} f\mathbf{Z}_i)$. This gives us the following tower of fields:

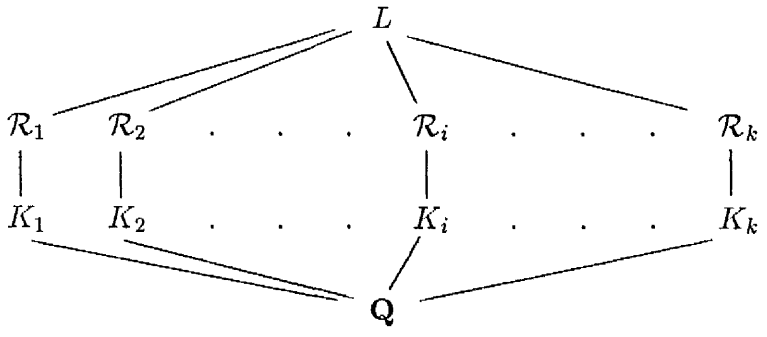

Fig. 1

Consider now the consequences of $Frob(p, L/\mathbf{Q}) = Frob(q, L/\mathbf{Q})$ for distinct primes p, q unramified in $L/\mathbf{Q}$. Hence, $p\mathbf{Z}_L = \wp_1 \dots \wp_g$, with $N\wp_i = p^{\mathrm{f}_0}$ and $q\mathbf{Z}_L = \boldsymbol{q}_1 \dots \boldsymbol{q}_g$, with $N\boldsymbol{q}_i = q^{\mathrm{f}_0}$, where f_0 is the order of any Frobenius element, $Frob(\wp_i, L/\mathbf{Q})$ or $Frob(\boldsymbol{q}_i, L/\mathbf{Q})$. WLOG, we may take $\sigma_j := Frob(\wp_j, L/\mathbf{Q}) = Frob(\boldsymbol{q}_j, L/\mathbf{Q})$, for $j = 1, \dots, g$.

Now $Frob(\wp_j, L/K_i)$ is the smallest power of σ_j which lies in $Gal(L/K_i)$ (see Lemma A2 in Appendix A). Hence $Frob(\wp_j, L/K_i) = Frob(\boldsymbol{q}_j, L/K_i)$ in $Gal(L/K_i)$. Now R_i/K_i is Galois and there exists a natural projection $\pi : Gal(L/K_i) \to Gal(R_i/K_i)$ defined by $\sigma \mapsto \sigma \mid_{R_i}$ (see Lemma A3 in Appendix A). Under π, $Frob(\wp_j, L/K_i)$ maps to $Frob(\wp_j \cap \mathcal{R}_j, R_i/K_i)$.

Thus $\forall i, j$, $Frob(\wp_j \cap R_i, R_i/K_i) = Frob(\boldsymbol{q}_j \cap R_i, R_i/K_i) = \left(\frac{R_i/K_i}{\wp_j \cap K_i}\right)$, the Artin symbol, since R_i/K_i is abelian. Thus, by Artin's reciprocity theorem, $\wp_j \cap K_i$ and $\boldsymbol{q}_j \cap K_i$ lie in the same ray-class $(mod^{\times} f\mathbf{Z}_i)$ $\forall i, j$. Also the residual degree of $\wp_j \cap K_i$ equals the residual degree of $\boldsymbol{q}_j \cap K_i$ $\forall i, j$. It follows that $\mathcal{R}(p^n) = \mathcal{R}(q^n)$ $\forall n \in \mathbf{N}$ as required$\square$

The next section utilises the Frobenian multiplicative property of ranges.

4. Asymptotic expansions for ranges of arbitrary orders in a direct sum of number fields

Our analysis starts from the following general theorem which describes qualitatively the type of expansions which arise in studying the asymptotics of $\#\{n \leq x; \theta(n) = \alpha\}$; here θ is any Frobenian multiplicative function with values in a finite commmutative monoid $\mathcal{M}$, and $\alpha \in \mathcal{M}$. We are particularly interested in $\#\{n \leq x; \theta(n) \neq \emptyset\}$, where θ is the range function defined above. Details of the proof of the theorem are to be found in [11].

THEOREM 6 *Let $\alpha \in \mathcal{M}$, a finite commmutative monoid. Let θ be a Frobenian multiplicative function with values in $\mathcal{M}$. Then $\#\{n \leq x; \theta(n) = \alpha\}$ has an*

asymptotic expansion consisting of a finite sum of asymptotic series of the type

$$x^{\kappa^{-1}}(log\ x))^{\beta-1}\sum_{r=0}^{h}\sum_{n=0}^{\infty}a_{r,n}(loglog\ x)^{r}(log\ x)^{-n}\ \ +O(x^{\kappa^{-1}}e^{-c\sqrt{log\ x}}),\quad(4.1)$$

where $\beta\in\mathbf{Q},\ ,0\leq\beta\leq 1,\ 0\leq h\in\mathbf{Z},\ \kappa\in\mathbf{N}.$

We now apply this to ranges. For d divisible by all primes ramified in $L/\mathbf{Q}$, let $\mathcal{P}=\{p\in\mathbf{N}_d$ such that p splits completely in $L\}$; then we have:

LEMMA 7 *Let* $\alpha\in\mathcal{M}$, *let* θ *be the range function, and suppose* $\theta(n)=\alpha$ *is soluble. Then the dominant term of (4.1) has* $\kappa=1$, *and* $\beta=$ *the Dirichlet density of the set of primes* $p\in\mathcal{P}$.

Proof This may be deduced from the following:

LEMMA 8 *Let* $\psi:\mathbf{N}_d\to\{0,1\}$ *be Frobenian multiplicative. Then* $\#\{n\in\mathbf{N}_d; n\leq x,\ \psi(n)=1\}$ *has an asymptotic expansion of the type*

$$x(log\ x)^{\gamma-1}\left\{\sum_{j=0}^{\infty}c_j(log\ x)^{-j}\right\},$$

where $\gamma\in\mathbf{Q}$ *is the Dirichlet density of the set of primes* p *with* $\psi(p)=1$, *and* $c_0>0$ *if* $\gamma>0$.

Proof

$$Let\ F(s)=\sum_{\substack{n\in\mathbf{N}_d\\ \psi(n)=1}}n^{-s},\quad\text{where } s=\sigma+\imath t;\ \sigma,t\in\mathbf{R}.\qquad(4.2)$$

Then

$$F(s)=\prod_{p\nmid d}\left(1+\sum_{\substack{k=1\\ \psi(p^k)=1}}p^{-k}\right).$$

And so

$$log\ F(s)=\sum_{\psi(p)=1}p^{-s}\ \ +H(s),$$

where $H(s)$ is analytic for $\sigma>\frac{1}{2}$.

Let $\Gamma_p = \{\mathcal{C}$ such that $Frob(p, L/\mathbf{Q}) = \mathcal{C}, \psi(p) = 1\}$. Let $\gamma = \frac{\#\Gamma_p}{\#G}$, the Dirichlet density of the set of primes p with $\psi(p) = 1$. Then

$$F(s) = (s-1)^{-\gamma} D(s),$$

where $D(1) \neq 0$, $D(s)$ is analytic for $\sigma \geq 1$, with moderate vertical growth. Applying the Mellin transform, we find that: $\#\{n \in \mathbf{N}_d; n \leq x, \psi(n) = 1\}$ has an asymptotic expansion of the type $\sum_{j=1}^{\infty} A_j x (log\ x)^{\gamma - j}$, with $A_1 > 0$ and this is easily seen to be of the required form$\square$ *Lemma 8.*

We have $\forall p \in \mathcal{P}$, $\forall n \in \mathbf{N}$, $\mathcal{R}(p^n) = \underline{1}$, i.e. consists only of the principal ray-class. So if we let $\theta_1 : \mathbf{N}_d \to \mathcal{M}$ be given by

$$\theta_1(n) := \begin{cases} 1 & \text{iff } p \mid n \Rightarrow p \in \mathcal{P} \\ 0 & \text{otherwise} \end{cases},$$

then θ_1 is clearly Frobenian multiplicative. Let $\mathcal{E} := \{n \in \mathbf{N}_d; p \mid n \Rightarrow p \in \mathcal{P}\}$. We deduce from Lemma 8 that $\#(\mathcal{E} \cap [1, x]) = \#\{n \in \mathbf{N}_d; n \leq x,\ \theta_1(n) = 1\}$ has an asymptotic expansion of the type $\sum_{j=1}^{\infty} A_j x (log\ x)^{\gamma_p - j}$, where $A_1 > 0$, γ_p is the Dirichlet density of the set of primes p with $\theta_1(p) = 1$. Clearly this number is a lower bound for $\#\{n \in \mathbf{N}_d; n \leq x, \mathcal{R}(n) = \underline{1}\}$. Now suppose $\alpha \in 2^I$ with $\mathcal{R}(n_0) = \alpha$, for some n_0. Consider all numbers $n := n_0 e \leq x$, where $e \in \mathcal{E}$ and $(e, n_0) = 1$. Clearly all of these have $\mathcal{R}(n) = \alpha$. Their number is given by $\#\{e \in \mathcal{E}; e \leq \frac{x}{n_0}, (e, n_0) = 1\}$. In (4.2), with $\psi = \theta_1$, we just remove those p which divide n_0 (a finite number). It follows that

$$\#\{e \in \mathcal{E}; e \leq \frac{x}{n_0}, (e, n_0) = 1\} \sim (\frac{x}{n_0})(log\ \frac{x}{n_0})^{\gamma_p - 1} \sum_{j=0}^{\infty} a_j (log\ \frac{x}{n_0})^{-j},$$

with $a_0 > 0$.

Comparing this with the statement of the theorem, we see that at least one of the expansions (4.1) must have $\kappa = 1$. As all $a_j's \geq 0$, the dominant term has a term (4.1) with $\beta = \gamma_p$ $\square$

If we define $\theta_2 : \mathbf{N}_d \to \mathcal{M}$ by

$$\theta_2(n) := \begin{cases} 1 & \mathcal{R}(n) \neq \emptyset \\ 0 & \text{otherwise} \end{cases},$$

then $\theta_2(n)$ is clearly Frobenian multiplicative and we deduce immediately from Lemma 8 that $\#\{n \in \mathbf{N}_d; \mathcal{R}(n) \neq \emptyset\}$ has an asymptotic expansion consisting of a finite sum of asymptotic series of the type (4.1), with the leading term having $\kappa = 1$, $\beta =$ the Dirichlet density of the set of primes p with $\theta_2(p) = 1$.

CHAPTER 2
Norms and Abelian Group Determinants

0. Introduction

In this chapter we seek primarily more information on the nature of norms of ideals in algebras, by considering the special case $K = \mathbf{Q}$. In particular, for a given prime p, we are interested in 'allowable' exponents k such that there exist norms n, with $p^k \parallel n$, and the 'critical' exponent – the l, say, such that $p \mid n \Rightarrow p^l \mid n$. The chapter ends with a simple demonstration that almost all norms have non-empty range.

1. Group Determinants

Let R be a commutative ring with 1, G a finite group, $\#G = n$, $G = \{g_1, \ldots, g_n\}$ say. Let RG be the group algebra of G over R ; so RG is free as an $R-$ module of rank n. For $\alpha \in RG$, let L_α be the $R-$ module morphism $t \mapsto \alpha t$ (for $t \in RG$). The determinant of L_α is called the 'norm' of α, denoted by $N(\alpha)$; clearly $N(\alpha\beta) = N(\alpha)N(\beta)$ as $L_{\alpha\beta} = L_\alpha \circ L_\beta$, and $N(\alpha) = 0$ if and only if α is a zero divisor in RG. Now adjoin independent indeterminates $x_1, \ldots, x_n$ to R and consider the "generic" element $\lambda := \sum_{i=1}^n x_i g_i$ in $R[x]G$. The determinant of L_λ (regarded as an $R[x]-$ module morphism) will be called the 'group determinant' of G, denoted by $det(RG)$. It is a homogeneous polynomial of degree n in $x_1, \ldots, x_n$, with coefficients in the prime subring of R; taking $R = \mathbf{Z}$, $G = C_n$ gives a circulant - we shall study this in detail in Chapter 3.

Structure of $\mathbf{Q}G$; *Construction of a* $\mathbf{Q}-$*algebra isomorphism*

First we need some information on characters and group algebras. Let G be any finite abelian group, and let $\hat{G}$ denote its dual – the group of characters of G (i.e. $\hat{G} = Hom(G, \mathbf{C})$). Let $\chi \in \hat{G}$; then $\chi(G)$ is cyclic, and $G/ker\ \chi$ is cyclic; clearly these D are precisely the kernels of characters of G. Consider all $D \triangleleft G$

such that G/D is cyclic. Label them $\{D_j\}_j \in J$. Choose $\forall j \in J$, $\chi_j \in \hat{G}$ such that $ker\ \chi_j = D_j$. Suppose $ker\ \psi = D_j$, some $\psi \in \hat{G}$. Let $< \bar{\gamma} >= G/D_j$, where $\gamma \in G$. Then $\psi(\gamma) = \chi_j(\gamma^r)$ with $(r, [G : D_j]) = 1$. Hence $\psi(\gamma) = \chi_j^r(\gamma)$ and it follows that $\psi = \chi_j^r$, since γ and D_j together generate G. Thus for each D_j there is at least one character χ_j such that $\forall r$ with $(r, [G : D_j]) = 1$, $ker\ \chi_j^r = D_j$, and these χ_j^r are all the characters of G whose kernels are D_j; from now onwards we take an arbitrary but fixed choice of the χ_j.

Now define the following:

$$\text{Let } K_j = \mathbf{Q}(\text{primitive } [G : D_j]^{th}\text{root of 1});$$

$$\mathbf{Z}_j = \text{integers of } K_j;$$

$$N_j = \text{norm } K_j/\mathbf{Q};$$

$$T_j = \text{trace } K_j/\mathbf{Q}.$$

THEOREM 9 *Let* $\mathcal{L} : \mathbf{Q}G \to \bigoplus_{j\in J} K_j$ *be defined by*

$$\sum_{g\in G} q_g g \mapsto \left(\sum_{g\in G} q_g \chi_j(g) \right)_{j\in J}$$

Then $\mathcal{L}$ *is a* $\mathbf{Q}$ *- algebra isomorphism.*

Proof We have that $\mathbf{Q}G$ and $\bigoplus_{j\in J} K_j$ are $\mathbf{Q}$ - algebras. $\mathcal{L}$ is clearly a homomorphism, so it suffices to show that

$$\begin{cases} (i)\ \forall \underline{\alpha} \in \bigoplus_{j\in J} K_j\ \exists \underline{y} \in \mathbf{Q}G\ ;\ \mathcal{L}(\underline{y}) = \underline{\alpha}; \\ (ii)\ \mathcal{L} \text{ is an injection.} \end{cases}$$

(i): We construct a preimage for $\underline{\alpha}$ as follows. Let $\underline{\alpha} = \{\alpha_j\}_{j\in J} \in \bigoplus_{j\in J} K_j$. We need to find $q_g \in \mathbf{Q}$ such that $\alpha_j = \sum_g q_g \chi_j(g)$,$\forall j \in J$.

Suppose, then, that

$$\alpha_j = \sum_g q_g \chi_j(g),$$

where $\chi_j \in (\hat{G} : D_j)^{th}$ roots of 1.

Let $\sigma \in \mathrm{Gal}(K_j/\mathbf{Q}) = \Gamma_j$, say. Denoting (after Hilbert) $\sigma(\chi(g))$ by $\chi^\sigma(g)$, we have $\alpha_j^\sigma = \sum_g q_g \chi_j^\sigma(g)$. Multiplying through by $\chi_j^\sigma(h^{-1})$, where $h \in G$, we obtain

$$\alpha_j^\sigma \chi_j^\sigma(h^{-1}) = \sum_g q_g \chi_j^\sigma(gh^{-1}).$$

Now summing over all σ's $\in \Gamma_j$ implies

$$\sum_\sigma \sigma(\chi(g')) = \sum_{\chi; ker\ \chi = D_j} \chi(g') \quad (\text{any } g' \in G).$$

Thus,

$$\begin{aligned}\sum_g q_g \sum_{\substack{\chi \\ ker \chi = D_j}} \chi(gh^{-1}) &= \sum_\sigma \alpha_j^\sigma \chi_j^\sigma(h^{-1}) \\ &= T_j(\alpha_j \chi_j(h^{-1})).\end{aligned}$$

Now summing over all $j \in J$ yields,

$$\sum q_g \sum_{\chi \in \hat{G}} \chi(gh^{-1}) = \sum_{j \in J} T_j(\alpha_j \chi_j(h^{-1})).$$

Then

$$q_h = \frac{1}{\#G} \sum_{j \in J} T_j(\alpha_j \chi_j(h^{-1}))$$

since we have the orthogonality relation

$$\sum_{\chi \in \hat{G}} \chi(a) = \begin{cases} \#G & \text{if } a = 1_G \\ 0 & \text{otherwise} \end{cases}.$$

Finally, noting that $\underline{\alpha} \mapsto \mathcal{M}(\underline{\alpha})$ is a $\mathbf{Q}$-linear map $\bigoplus K_j \to \mathbf{Q}G$, we see that if $\mathcal{M}(\underline{\alpha}) = \sum_g \left(\frac{1}{\#G} \sum_{j \in J} T_j \left(\alpha_j \chi_j(g^{-1}) \right) \right) g$ then, from the orthogonality relations, $\mathcal{L}(\mathcal{M}(\underline{\alpha})) = \underline{\alpha}$.

(ii) It is enough to show that $\mathbf{Q}G$ and $\bigoplus_{j \in J} K_j$ have the same dimension over $\mathbf{Q}$. The dimension of $\mathbf{Q}G$ is clearly $\#G$, while that of K_j is $\phi((G : D_j))$, (ϕ = Euler's totient function). But $\phi((G : D_j))$ is also $\#\{\chi \in \hat{G};\ ker\ \chi = D_j\}$. Hence

$dim\ \bigoplus_{j\in J} K_j = \sum_{j\in J} \phi((G:D_j)) = \sum_{j\in J} \#\{\chi \in \hat{G};\ ker\ \chi = D_j\} = \#\hat{G} = \#G$, as required.□

Summarising, we have:

$$\begin{aligned} &(i)\ \mathbf{Q}G \underset{\mathbf{Q}}{\cong} \bigoplus_{j\in J} K_j \text{ while} \\ &(ii)\ \alpha \in \mathcal{L}(\mathbf{Z}G) \Leftrightarrow \sum_{j\in J} T_j(\alpha_j \overline{\chi_j}(g)) \ \in \#G\mathbf{Z}\ \ \forall g \in G. \end{aligned} \tag{1.1}$$

LEMMA 10 *At least one of the summands on the RHS. in (1.1) (i) is* $\mathbf{Q}$ *(WLOG the first, say), then* det $\mathbf{Z}G \supseteq n^n\mathbf{Z}$.

Proof We have from (1.1)(ii) that $nS \subseteq \mathbf{Z}G$. Let $z \in \mathbf{Z}$ and $\alpha = n(z, 1, 1, \ldots, 1)$; then $N(\alpha) = n^n z$ as required□

2. Critical and Allowable Exponents for Finite Abelian Groups

Most of our discussion will apply to elementary abelian p-groups, but first we may establish a few properties for more general cases.

$\mathbf{Z}$ – order of a direct sum of arbitrary number fields

Suppose R is a $\mathbf{Z}$-order such that $R \subset K_1 \bigoplus \ldots \bigoplus K_r := A$, where the K_i $(i = 1, \ldots, r)$ are number fields. Choose a $\mathbf{Z}$-basis $\omega_1, \ldots, \omega_n$ of R and consider now the $K/\mathbf{Q}$ norm of $N(\sum_{j=1}^n x_j\omega_j)$ for $\underline{x} := (x_1, \ldots, x_n) \in \mathbf{Z}^n$; such $N(r)$ have norms of the form $N(\sum_{j=1}^n x_j\omega_j)$. It is clear that this is a polynomial $F(\underline{x}) \in \mathbf{Z}[\underline{x}]$. Now $p^k \parallel N(\sum_{j=1}^n x_j\omega_j)$ is soluble iff $\exists \underline{x} \in \mathbf{Z}^n$ such that $p^k \parallel F(\underline{x})$. This indicates that, for any $\mathbf{Z}$-order R, when examining allowable/critical exponents of primes p which divide norms, we may apply the Chinese Remainder Theorem to a set of simultaneous congruences, and thus we need only treat each p separately.

Group Rings

Let G be an arbitrary finite abelian group of order n. . Consider the values $k \in \mathbf{N}$ such that $p^k \parallel N(r)$, some $r \in \mathbf{Z}G$ and prime $p \mid n$. The following theorem

shows that the allowable/critical exponents may be obtained by considering only group rings for groups of prime power order. Recall that since G is finite abelian, it has a unique Sylow p-subgroup S, say.

THEOREM 11

(i) If $\alpha \in \mathbf{Z}S$ *such that* $p^k \parallel det_S\alpha$ *then* $\exists \beta \in \mathbf{Z}G$ *such that* $p^k \parallel det_G\beta$.

(ii) If $\beta \in \mathbf{Z}G$ *such that* $p^k \parallel det_G\beta$ *then* $\exists \alpha \in \mathbf{Z}S$ *such that* $p^k \parallel det_S\alpha$.

Proof We give constructions for β in (i) and α in (ii).

We have $G = ST$ (an internal direct product) such that $S \cap T = (1)$.

(i) Suppose $\alpha \in \mathbf{Z}S$ such that $p^k \parallel det_S\alpha$. Then consider

$$\beta = \alpha \sum_{t \in T} t + \#T.1_G - \sum_{t \in T} t$$

β is clearly in $\mathbf{Z}G$. Let $\chi \in \hat{G} = Hom(G, \mathbf{C}^*)$. Then we may extend χ to a $\mathbf{Q}$-algebra homomorphism $\mathbf{Q}G \mapsto \mathbf{C}$ by defining $\chi(\sum_{g \in G} q_g g) = \sum_{g \in G} q_g \chi(g)$. Hence,

$$\chi(\beta) = \chi(\alpha) \sum_{t \in T} \chi(t) + \#T - \sum_{t \in T} \chi(t) \tag{2.1}$$

In (2.1), $\chi|_T$ is trivial iff χ is a character of S only if $\chi(\beta) = \chi(\alpha)\#T$, whereas if $\chi|_T$ is non-trivial then $\chi(\beta) = \#T$ (since $\sum_{t \in T} \chi(t) = 0$). Hence,

$$det_G\beta = \prod_{\chi \in \hat{G}} \chi(\beta) = \prod_{\chi \in \hat{S}} \prod_{\chi \in \hat{T}} \chi(\beta)\psi(\beta) = (\#T)^n \prod_{\chi \in \hat{S}} \chi(\alpha) = (\#T)^n det_S\alpha.$$

As $p \not| (\#T)$ then $p^k \parallel det_S\alpha$ as required$\square$

(ii) Suppose $\beta \in \mathbf{Z}G$ such that $p^k \parallel det_G\beta$. We may write

$$\beta = \sum_{\sigma \in S} \sum_{t \in T} n(\sigma, \tau)\sigma\tau, \text{ where } n(\sigma, \tau) \in \mathbf{Z}.$$

Now consider

$$\alpha = \prod_{\phi \in \hat{T}} \sum_{\sigma \in S} \sum_{t \in T} n(\sigma, \tau)\phi(\tau)\sigma \quad \in \mathbf{Z}[\zeta]S, \text{ where } \zeta \text{ is some root of unity.}$$

In fact $\alpha \in \mathbf{Z}S$ since for a given σ, the net coefficient of σ in this expression of α is a symmetric function of the $\phi(\tau)$. Also we have

$$det_S\alpha = \prod_{\chi\in\hat{S}} \chi(a) = \prod_{\chi\in\hat{S}} \prod_{\phi\in\hat{T}} \chi(\beta) = det_G\beta \square$$

3. Some Results on the Group Determinants of Elementary Abelian p-Groups

Let G be an elementary abelian p - group of order p^n ($n \in \mathbf{N}$). Then we have the following (see Odoni [10]):

THEOREM 12 *Let $p \geq 2$ be prime and let G be elementary abelian of order p^n ($n \geq 1$). If $m \in \mathbf{Z}$ and $p \not| m$ then a necessary and sufficient condition for $m \in det(\mathbf{Z}G)$ is that $m^{p-1} \equiv 1 \ (mod\ p^n)$.*

We examine now critical exponents for G. The methods will continue to utilise group characters and the arithmetic of cyclotomic fields.

Lower Bounds for Critical Exponents of $G = {C_p}^n$

Notation Given a Dedekind domain, for a ring R, and principal prime ideal λR, $V_\lambda(\alpha) := k;\ \lambda^k \parallel \alpha, (\alpha \in R)$.

(3.(i)) Suppose $p \,|\, m$ and $m \in det(\mathbf{Z}G)$, i.e. $m = det\ \gamma$, for some $\gamma \in \mathbf{Z}G$. If $\gamma = \sum_{g\in G} a_g g$ ($a_g \in \mathbf{Z}$) then

$$(m =)\ det\ \gamma = \prod_{\chi\in\hat{G}} \chi(\gamma) = \prod_{\chi\in\hat{G}} \sum_{g\in G} a_g\chi(g)$$

(lifting up χ as on page 14). We have $\forall\chi \in \hat{G}$, $\sum_{g\in G} a_g\chi(g) \in \mathbf{Z}[\zeta]$ where ζ is some primitive p^{th} root of unity; and also $\exists\chi' \in \hat{G}; \lambda := 1-\zeta \mid \sum_{g\in G} a_g\chi'(g)$ since $det\ \gamma \in p\mathbf{Z}$. As $\forall\chi \in \hat{G}$, $\chi(g)$ is a power of ζ, $\chi(g) \equiv 1\ (mod\ \lambda)$. Hence $\lambda \mid \sum_{g\in G} a_g$, and so

$$\sum_{g\in G} a_g \in p\mathbf{Z}. \tag{3.1}$$

If $\psi \in \hat{G}$, then $\psi(g) \equiv 1 \ (mod\ \lambda)$, giving $\sum_{g\in G} a_g(\psi(g)-1) \equiv 0 \ (mod\ \lambda)$ and hence

$$\sum_{g\in G} a_g\psi(g) \equiv 0 \ (mod\ \lambda). \tag{3.2}$$

From (3.1) and (3.2) we deduce $V_\lambda(det\ \gamma) \geq (p-1)V_p(\sum_{g\in G} a_g) + p^n - 1$ (since $p\mathbf{Z}[\zeta] = \lambda^{p-1}$ and $\#G = p^n$). Thus a trivial lower bound is

$$V_p(det\ \gamma) \geq V_p(\sum_{g\in G} a_g) + \frac{p^n-1}{p-1} \tag{3.3}$$

(3.(ii)) We may find a tighter lower bound by regarding G as a vector space $\mathbf{F}_p^n = \{(x_1, x_2, \ldots, x_n);\ x_i \in \mathbf{F}_p\ (i = 1, \ldots, n)\}$. We proceed now to handle first odd primes p and then the case $p = 2$.

Suppose $p > 2$. Let $\lambda = 1 - \zeta$ where ζ is a primitive p^{th} root of unity. A typical character $\chi \in \hat{G}$ may be defined by $\chi_{\underline{y}}(\underline{x}) = \zeta^{(\underline{x}.\underline{y})}\ \forall \underline{x} \in G$, where $\underline{y}$ running through G gives the complete set of characters. Then

$$det\ \gamma = \prod_{\chi\in\hat{G}} \sum_{g\in G} a_g\chi(g) = \prod_{\underline{y}\in G} \left\{ \sum_{\underline{x}\in G} a(\underline{x})(\zeta^{(\underline{x}.\underline{y})} - 1) + T \right\},$$

where $T = \sum_{\underline{x}\in G} a(\underline{x})$. So

$$V_\lambda(det\ \gamma) = \sum_{\underline{y}\in G} V_\lambda \left(T + \sum_{\underline{x}\in G} a(\underline{x})(\zeta^{(\underline{x}.\underline{y})} - 1) \right).$$

Now $\lambda = 1 - \zeta$ gives

$$\zeta^{(\underline{x}.\underline{y})} - 1 = (1-\lambda)^{\underline{x}.\underline{y}} - 1 = \left(1 - (\underline{x}.\underline{y})\lambda + \binom{\underline{x}.\underline{y}}{2}\lambda^2 + \ldots\right) - 1.$$

Hence we obtain,

$$V_\lambda(det\ \gamma) = \sum_{\underline{y}\in G} V_\lambda \left(T + \sum_{\underline{x}\in G} a(\underline{x}) \left\{ -\lambda(\underline{x}.\underline{y}) + \lambda^2 \binom{\underline{x}.\underline{y}}{2} - \ldots \right\} \right). \tag{3.4}$$

Regarding the inner sum as a polynomial in $\underline{y}$, $f(\underline{y})$ say, we define:

$$\mathcal{V}_1 := \left\{ \underline{y} \in G;\ \sum_{\underline{x} \in G} a(\underline{x})(\underline{x}.\underline{y}) \equiv 0\ (mod\ p) \right\}$$

$$\mathcal{V}_2 := \left\{ \underline{y} \in \mathcal{V}_1;\ \sum_{\underline{x} \in G} a(\underline{x})(\underline{x}.\underline{y})^2 \equiv 0\ (mod\ p) \right\}$$

$$\vdots$$

$$\mathcal{V}_n := \left\{ \underline{y} \in \mathcal{V}_{n-1};\ \sum_{\underline{x} \in G} a(\underline{x})(\underline{x}.\underline{y})^n \equiv 0\ (mod\ p) \right\}$$

where $\mathcal{V}_r \neq \{\underline{0}\} = \mathcal{V}_{r+1}$ for some $r < n$, with necessarily $r < p$.

The $\mathcal{V}_i$'s represent varieties in $\underline{y}$. Now we obtain

$$\begin{aligned} V_\lambda(det\ \gamma) &= V_\lambda(T) + \#(G \setminus \mathcal{V}_1) + 2\#(\mathcal{V}_1 \setminus \mathcal{V}_2) + \ldots + (r+1)\#(\mathcal{V}_r \setminus \mathcal{V}_{r+1}) \\ &= V_\lambda(T) + (p^n - \#\mathcal{V}_1) + 2(\#\mathcal{V}_1 - \#\mathcal{V}_2) + \ldots (r+1)\#(\mathcal{V}_r - 1) \\ &= V_\lambda(T) + \sum_{j=1}^{r} (\#\mathcal{V}_j - 1) + p^n - 1 \end{aligned}$$

Hence, under the assumption that p is sufficiently large compared with n,

$$V_p(det\ \gamma) = V_p(T) + \frac{p^n - 1}{p-1} + \sum_{j=1}^{r} \frac{\#\mathcal{V}_j - 1}{p-1} \tag{3.5}$$

where $V_p(T) \geq 1$.

It is a fact that $\mathcal{V}_i$, the set of projective points, satisfies $\#\mathcal{V}_i - 1 \equiv 0\ (mod\ p-1)$. (See e.g. Ireland & Rosen [2].)

(3.(iii)) We are now faced with the problem of minimising (3.5) by an appropriate choice of $a(\underline{x})$ satisfying $T = \sum_{\underline{x} \in G} a(\underline{x}) \in p\mathbf{Z}$. For $\mathcal{V}_1$, this is equivalent to determining the number of co-dimension 1 subspaces of $\mathbf{F}_p^n$. The minimum number possible is thus p^{n-1} which is attainable by the following argument. For

$l = 1, 2, \ldots, n$ let $\underline{e}_l = (0, \ldots, 1, \ldots, 0)$ with the '1' in the l^{th} position). Hence $\{\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n\}$ is a basis for $\mathbf{F}_p^n$. Then any $\underline{x}$, and fixed candidate $\underline{y}$ is given by:

$$\underline{x} = \mu_1\underline{e}_1 + \mu_2\underline{e}_2 + \ldots + \mu_n\underline{e}_n, \text{ where } \mu_l \in \mathbf{F}_p \ (l = 1, 2, \ldots, n),$$

$$\text{and } \underline{y} = \lambda_1\underline{e}_1 + \lambda_2\underline{e}_2 + \ldots + \lambda_n\underline{e}_n, \text{ where } \lambda_l \in \mathbf{F}_p \ (l = 1, 2, \ldots, n).$$

Hence we need for $\mathcal{V}_1$ ($a(\underline{x})$ being denoted by $a_{(\mu_1, \mu_2, \ldots, \mu_n)}$):

$$\sum_{\mu_1=0}^{p-1} \sum_{\mu_2=0}^{p-1} \cdots \sum_{\mu_n=0}^{p-1} a_{(\mu_1, \mu_2, \ldots, \mu_n)}[\lambda_1\mu_1 + \lambda_2\mu_2 + \ldots + \lambda_n\mu_n] \equiv 0 \ (mod\ p) \quad (3.6)$$

Put $a_{(1,0,\ldots,0)} = p^k - 1$, $a_{(1,0,\ldots,0)} = 1$ and all other $a_{(\mu_1, \mu_2, \ldots, \mu_n)} = 0$. Then (3.6) becomes

$$(p^k - 1)\lambda_1 + \lambda_n \equiv 0 \ (mod\ p).$$

Thus (3.6) clearly has p^{n-1} solutions $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ with $\lambda_1 \equiv \lambda_n \ (mod\ p)$ and λ_l any $\in \mathbf{F}_p$ $(1 < l < n)$, and so $\underline{y}$ has p^n choices□

For $\mathcal{V}_2, \mathcal{V}_3$ and upwards, the minimum number is not generally obvious. We do have however:

LEMMA 13 *Let $G = {C_p}^2$, where p is an odd prime. Then in (3.5), $V_p(det\ \gamma) \geq$*

$\geq V_p(T) + p + 2$. Further, by a suitable choice of $a(\underline{x})$ (to be determined) $\exists\gamma:$ *$V_p(det\ \gamma) = k + p + 2$, where $k \in \mathbf{N}$ is arbitrary.*

[The case $p = 2$ is dealt with later]

Proof Consider $\mathcal{V}_1$ represented by (3.6) above ; here this becomes

$$\sum_{\mu_1=0}^{p-1} \sum_{\mu_2=0}^{p-1} a_{\mu_1, \mu_2}(\lambda_1\mu_1 + \lambda_2\mu_2) \equiv 0 \ (mod\ p). \quad (3.7)$$

As above $\#\mathcal{V}_1 \geq p$. Using the same notation, the number of solutions $\underline{y}$ to $\mathcal{V}_2$ is given by the number of solutions (λ_1, λ_2) to

$$\sum_{\mu_1=0}^{p-1} \sum_{\mu_2=0}^{p-1} a_{\mu_1, \mu_2}(\lambda_1\mu_1 + \lambda_2\mu_2)^2 \equiv 0 \ (mod\ p). \quad (3.8)$$

In general, this has at least one solution in common with (3.7), viz $(\lambda_1, \lambda_2) = \underline{0}$. Hence $\#\mathcal{V}_2 \geq 1$ so in (3.5) $V_p(det\ \gamma) \geq V_p(T) + p + 2$. In fact, putting $a_{1,0} = p^k - 2$, $a_{0,1} = a_{0,2} = 1$, and $a_{i,j} = 0$ (for all other i, j) yields in (3.6):

$$\begin{aligned} (p^k - 2)\lambda_1 + 3\lambda_2 &\equiv 0\ (mod\ p) \\ \Rightarrow 2\lambda_1 &\equiv 3\lambda_2\ (mod\ p) \\ \Rightarrow \lambda_1 &\equiv \frac{3}{2}\lambda_2\ (mod\ p) \end{aligned} \tag{3.9}$$

The congruence (3.9) has p solutions $mod\ p$. In (3.8) we have: $(p^k - 2)\lambda_1^2 + 5\lambda_2^2 \equiv 0\ (mod\ p)$ and substituting in the value of λ_1 from (3.6) gives $\lambda_2^2 \equiv 0\ (mod\ p)$. Hence $(\lambda_1, \lambda_2) = \underline{0}$ is the unique solution. Thus in (3.5) $V_p(det\ \gamma) = k + p + 2$, where $\sum_{i=0}^{p-1} \sum_{j=0}^{p-1} a_{i,j} = p^k$, as required $\square$

3.(iv) For $p = 2$ we use a different approach which manipulates matrices. This method helps give a complete solution for the particular case $p = 2$, $n = 2$ but cannot be applied so effectively to more general cases.

PROPOSITION 14 *Let $G = {C_2}^2$. Then $det(\mathbf{Z}G)$ is given by $(4\mathbf{Z} + 1) \dot{\cup} 16\mathbf{Z}$.*

Proof It follows directly from Theorem 12 that if $2 \not| m$ then $m \in det(\mathbf{Z}G)$ iff $m \equiv 1\ (mod\ 4)$. Hence the only odd numbers in $det(\mathbf{Z}G)$ are precisely those given by $4\mathbf{Z} + 1$. We show now that the only even numbers in $det(\mathbf{Z}G)$ are given by $16(\mathbf{Z})$. First we consider $G = {C_2}^n$ for arbitrary $n \in \mathbf{N}$. Let $\gamma := \sum_{g \in G} a_g$. Then

$$det\ \gamma = \prod_{\chi \in \hat{G}} \sum_{g \in G} a_g \chi(g).$$

Let $b_\chi := \sum_{g \in G} a_g \chi(g)$, so $det\ \gamma = \prod_{\chi \in \hat{G}} b_\chi$. In matrix form we have:

$$\begin{pmatrix} b_{\chi_1} \\ b_{\chi_2} \\ \vdots \\ b_{\chi_{2^n}} \end{pmatrix} = \begin{pmatrix} \chi_1(g_1) & \chi_1(g_2) & \cdots & \chi_1(g_{2^n}) \\ \chi_2(g_1) & \chi_2(g_2) & \cdots & \chi_2(g_{2^n}) \\ \vdots & \vdots & & \vdots \\ \chi_{2^n}(g_1) & \chi_{2^n}(g_2) & \cdots & \chi_{2^n}(g_{2^n}) \end{pmatrix} \begin{pmatrix} a_{g_1} \\ a_{g_2} \\ \vdots \\ a_{g_{2^n}} \end{pmatrix},$$

where $G = \{g_1, \ldots, g_{2^n}\}$ and $\hat{G} = \{\chi_1, \ldots, \chi_{2^n}\}$.

Let $\underline{\underline{A}} = (\chi_i(g_j))$ $i, j = 1, \ldots, 2^n$. The following Lemma yields much information.

LEMMA 15 $\underline{\underline{A}}^2 = 2^n \underline{\underline{I}}_{2^n}$, *where* $\underline{\underline{I}}_k$ *is the* $k \times k$ *identity matrix for* $k \in \mathbf{N}$.

Proof As in (3.(ii)) we regard G as ${F_2}^n$ and since -1 is the primitive second root of unity, $\forall \underline{x} \in G$ characters $\chi_{\underline{y}}$ are defined by, $\chi_{\underline{y}} = (-1)^{\underline{x} \cdot \underline{y}}$ where $\underline{y}$ runs through G. This expression is symmetric in $\underline{x}$ and $\underline{y}$, thus $\chi_{g_j}(g_i)$ $(= (-1)^{g_i \cdot g_j}) = \chi_{g_i}(g_j)$, i.e. there exist labellings such that $\underline{\underline{A}} = \underline{\underline{A}}^T$. Hence if $a_{ij} := \chi_i(g_j)$ then,

$$\begin{aligned}
(\underline{\underline{A}}^T \underline{\underline{A}})_{ik} &= \sum_{j=1}^{2^n} a_{ji} a_{jk} \\
&= \sum_{j=1}^{2^n} \chi_j(g_i) \chi_j(g_k) \\
&= \sum_{g \in G} a_g \chi(g_i g_k^{-1}) \\
&= 2^n \delta_{ik} \quad \text{where } \delta_{ik} = \begin{cases} 1 & \text{if } g_i = -g_k \\ 0 & \text{otherwise} \end{cases}
\end{aligned}$$

We deduce that $\underline{\underline{A}}^2 = \underline{\underline{A}}^T \underline{\underline{A}} = 2^n \underline{\underline{I}}$ □

This result helps us to characterise $\{\underline{\underline{A}}\,\underline{x}; \underline{x} \in \mathbf{Z}^{2^n}\}$. For the critical exponent, we must decide which $\underline{c} = (c_1, c_2, \ldots, c_{2^n}) \in \mathbf{Z}^{2^n}$ are such that $\underline{\underline{A}}\,\underline{x} = \underline{c}$ has a solution $\underline{x} \in \mathbf{Z}^{2^n}$ with $2 \mid \prod_{i=1}^{2^n} c_i$. (The c_i correspond to the b_{χ_i}).

From now on assume $n = 2$. From $\underline{\underline{A}}\,\underline{x} = \underline{c}$ we have $\underline{\underline{A}}^2 \underline{x} = \underline{\underline{A}}\,\underline{c}$, hence $\underline{\underline{A}}\,\underline{c} = 4\underline{x}$ by Lemma 15. $\underline{\underline{A}}$ is easily computed; it is given by

$$\underline{\underline{A}} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

From the equation $\underline{\underline{A}}\,\underline{c} = 4\underline{x}$ we obtain the following set of simultaneous

congruences for $c_1, c_2, c_3, c_4 \in \mathbf{Z}$:

$$\left.\begin{array}{l} c_1+c_2+c_3+c_4 \equiv 0 \ (mod\ 4) \\ c_1-c_2+c_3-c_4 \equiv 0 \ (mod\ 4) \\ c_1+c_2-c_3-c_4 \equiv 0 \ (mod\ 4) \\ c_1-c_2-c_3+c_4 \equiv 0 \ (mod\ 4) \end{array}\right\} \quad (*)$$

A series of row subtractions yields $c_2 \equiv c_3 \equiv c_4 \ (mod\ 2)$ and $c_1 \equiv c_2 \ (mod\ 4)$.

If any of the c_i are odd, then all are and so $2 \not| \ c_1c_2c_3c_4$. Thus we need c_1, c_2, c_3 and c_4 all even and hence $det(\mathbf{Z}G) \subseteq 16\mathbf{Z}$. Now choosing $c_1 \equiv c_2 \equiv 2 \ (mod\ 4)$ and $c_3 \equiv c_4 \equiv 0 \ (mod\ 4)$ satisfies (*) and yields $det(\mathbf{Z}G) \supseteq 16\mathbf{Z}$. The proposition is proved$\square$

(3.(vi)) For $n = 2$, and any odd prime p, this kind of approach yields:

PROPOSITION 16 *For an odd prime p, if* $G = {C_p}^2$, *then* $det(\mathbf{Z}G) \supseteq p^{p^2}(p\mathbf{Z} \pm 1)$.

Proof We define characters as in (3.(ii)), with γ, b_χ and $\underline{\underline{A}}$ as in (3.(v)). We would like to characterise $\{\underline{\underline{A}}\,\underline{x};\ \underline{x} \in \mathbf{Z}^{p^n}\}$. This is apparently difficult, so instead, to automatically satisfy $p \mid \prod_{i=1}^{p^2} c_i$, where $\underline{c} = (c_1, \ldots, c_{p^2}) \in \mathbf{Z}^{p^2}$, we consider which $\underline{c}$ are such that $\underline{\underline{A}}\,\underline{x} = p\underline{c}$. Then $det\ \gamma = \prod_{i=1}^{p^2} pc_i;\ c_i \in \mathbf{Z}$. Recall that the characters of $\hat{C}_{p^2}$ are defined by: for $\underline{x} = (x_1, x_2) \in {\mathbf{F}_p}^2$, $\underline{x} \mapsto \zeta^{\underline{x}\cdot\underline{y}}$. Here $\underline{\underline{A}} = [\zeta^{\underline{x}\cdot\underline{y}}]_{\underline{x},\underline{y} \in {\mathbf{F}_p}^2}$, where $\zeta = e^{2\pi i/p}$. Let $\underline{r} = (r_1, r_2) \in {\mathbf{F}_p}^2$, $\underline{s} = (s_1, s_2) \in {\mathbf{F}_p}^2$. Then the $(r_1p + r_2 + 1, s_1p + r_2 + 1)$ entry is $\zeta^{r_1s_1 + r_2s_2}$. We now compute $\underline{\underline{A}}^2$.

For fixed r_1, r_2, s_1 and s_2 the $(r_1p + r_2 + 1, s_1p + s_2 + 1)$ entry is given by

$$\begin{aligned} &\sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \zeta^{(jr_1+ir_2)+(js_1+is_2)} \\ &= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \zeta^{i(r_2+s_2)}\zeta^{j(r_1+s_1)} \\ &= \sum_{i=0}^{p-1} \zeta^{i(r_2+s_2)} \sum_{j=0}^{p-1} \zeta^{j(r_1+s_1)} \\ &= p\delta(r_2, s_2)p\delta(r_1, s_1), \end{aligned}$$

$$\text{where } \delta(x,y) = \begin{cases} 1 & \text{if } x+y \equiv 0 \ (mod\ p) \\ 0 & \text{otherwise} \end{cases} \tag{3.11}$$

We have that (3.11) is satisfied exactly once in each row and in each column, with all other entries being zero. Thus we have $p^2\times$ some permutation of $\underline{\underline{I}}_{p^2}$. Relabel the x_i's so that WLOG we have:

$$p^2\underline{x} = p\underline{\underline{A}}\,\underline{c}. \tag{3.12}$$

Examining $\underline{\underline{A}}$ we note that its first row consists entirely of 1's so,

$$c_1 + c_2 + \ldots + c_{p^2} \equiv 0 \ (mod\ p). \tag{3.13.1}$$

For rows 2 to p^2, given $\underline{r} = (r_1, r_2)$, we have two cases:

a) $r_2 \not\equiv 0 \ (mod\ p)$. Then as s_1 runs through $0, 1, \ldots, p-1$, then $r_1s_1 + r_2s_2$ runs over the complete set of residues in $\mathbf{F}_p^*$ as s_2 does. Hence row $r_1p + s_2 + 1$ consists of p blocks of $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$ in some order. Hence we have a congruence of the following type:

$$(c_{i_{(1,1)}} + \ldots + c_{i_{(1,p)}}) + (c_{i_{(2,1)}} + \ldots + c_{i_{(2,p)}})\zeta + \ldots$$

$$+(c_{i_{(p,1)}} + \ldots + c_{i_{(p,p)}})\zeta^{p-1} \equiv 0 \ (mod\ p) \tag{3.13.2}$$

b) Suppose $r_2 \equiv 0 \ (mod\ p)$. Then $r_2s_2 \equiv 0 \ (mod\ p)$. Hence we obtain blocks of length p of $\zeta^{r_1s_1}$ for each s_1. Similarly again, as s_1 varies over $\mathbf{F}_p$ then so does r_1s_1. Noting that for $s_1 = 0$, $\zeta^{r_1s_1} = 1$, we obtain a congruence,

$$(c_1 + c_2 + \ldots + c_p) + (c_{j_1} + \ldots + c_{j_1+p-1})\zeta + \ldots$$

$$+(c_{j_{p-1}} + \ldots + c_{j_{p-1}+p-1})\zeta^{p-1} \equiv 0 \ (mod\ p) \tag{3.13.3}$$

(3.13.1), (3.13.2) and (3,13,3) cover between them all congruences possible from $p\underline{x} = \underline{\underline{A}}\,\underline{c}$. Note that in (3.13.2) and (3.13.3) the number of coefficients of $\zeta^a = p$.

Thus $c_i \equiv a \ (mod\ p)$, any $a \in \mathbf{F}_p$ is a solution of the three congruences. In particular, $\underline{c} = -\underline{1}$ gives

$$det(\mathbf{Z}G) \supseteq p^{p^2}(p\mathbf{Z}+1)^{p^2} = p^{p^2}(p\mathbf{Z}+1)$$

and $\underline{c} = \underline{1}$ gives

$$det(\mathbf{Z}G) \supseteq p^{p^2}(p\mathbf{Z}-1)_{\square}$$

We may now easily deduce the following:

LEMMA 17 *Let* $G = {C_3}^2$. *Then* $det(\mathbf{Z}G) \supseteq 3^9\mathbf{Z}$.

Proof By Proposition 16, $det(\mathbf{Z}G) \supseteq 3^9(3\mathbf{Z} \pm 1)$. Hence it only remains to show that $det(\mathbf{Z}G) \supseteq 3^9(3\mathbf{Z})$.

In (3.12) we have WLOG $\prod_{i=1}^{9} c_i \in det(\mathbf{Z}G)$, in which $c_i \in \mathbf{Z}$ $(i = 1, 2, \ldots, 9)$ satisfy $3\underline{x} = \underline{\underline{A}}\,\underline{c}$, where $\underline{x} = (x_1, \ldots, x_9) \in \mathbf{Z}^9$, $\underline{\underline{A}} = [\zeta^{\underline{x}\cdot\underline{y}}]_{\underline{x},\underline{y}\in\mathbf{F}_p{}^2}$ (see (3.11)). We have explicitly,

$$3\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix} = \begin{pmatrix} c_1 + c_2 + c_3 + c_4 + c_5 + c_6 + c_7 + c_8 + c_9 \\ c_1 + \zeta c_2 + \zeta^2 c_3 + c_4 + \zeta c_5 + \zeta^2 c_6 + c_7 + \zeta c_8 + \zeta^2 c_9 \\ c_1 + \zeta^2 c_2 + \zeta c_3 + c_4 + \zeta^2 c_5 + \zeta c_6 + c_7 + \zeta^2 c_8 + \zeta c_9 \\ c_1 + c_2 + c_3 + \zeta c_4 + \zeta c_5 + \zeta c_6 + \zeta^2 c_7 + \zeta^2 c_8 + \zeta^2 c_9 \\ c_1 + \zeta c_2 + \zeta^2 c_3 + \zeta c_4 + \zeta^2 c_5 + c_6 + \zeta^2 c_7 + c_8 + \zeta c_9 \\ c_1 + \zeta^2 c_2 + \zeta c_3 + \zeta c_4 + c_5 + \zeta^2 c_6 + \zeta^2 c_7 + \zeta c_8 + c_9 \\ c_1 + c_2 + c_3 + \zeta^2 c_4 + \zeta^2 c_5 + \zeta^2 c_6 + \zeta c_7 + \zeta c_8 + \zeta c_9 \\ c_1 + \zeta c_2 + \zeta^2 c_3 + \zeta^2 c_4 + c_5 + \zeta c_6 + \zeta c_7 + \zeta^2 c_8 + c_9 \\ c_1 + \zeta^2 c_2 + \zeta c_3 + \zeta^2 c_4 + \zeta c_5 + c_6 + \zeta c_7 + c_8 + \zeta^2 c_9 \end{pmatrix}$$

In each row we require the coefficients of $1, \zeta$ and ζ^2 to be equal $(mod\ 3)$. Thus, we arrive at the following set of simultaneous congruences for the c_i:

$$\left.\begin{array}{r} c_1 + c_4 + c_7 \underset{3}{\equiv} c_2 + c_5 + c_8 \underset{3}{\equiv} c_3 + c_6 + c_9 \\ c_1 + c_2 + c_3 \underset{3}{\equiv} c_4 + c_5 + c_6 \underset{3}{\equiv} c_7 + c_8 + c_9 \\ c_1 + c_6 + c_8 \underset{3}{\equiv} c_2 + c_4 + c_9 \underset{3}{\equiv} c_3 + c_5 + c_7 \\ c_1 + c_5 + c_9 \underset{3}{\equiv} c_3 + c_4 + c_8 \underset{3}{\equiv} c_2 + c_6 + c_7 \\ c_1 + c_2 + c_3 + c_4 + c_5 + c_6 + c_7 + c_8 + c_9 \underset{3}{\equiv} 0 \end{array}\right\}$$

By inspection, $\{c_1 \equiv_3 0; c_2, c_3, c_6, c_8 \equiv_3 1;\ c_4, c_5, c_7, c_9 \equiv_3 2\}$ yields the solution $det(\mathbf{Z}G) \supseteq 3^9(3\mathbf{Z}(3\mathbf{Z}+1)^4(3\mathbf{Z}-1)) = 3^9(3\mathbf{Z})$ as required$\square$

(3.(vii)) *Allowable Exponents*

For circulants (i.e. when $G = C_n$) we shall establish explicitly, in Chapter 3, what are the corresponding critical exponents: in particular, it will be shown that all m coprime with n are values of the circulant.

However, for general abelian groups this appears to be a rather difficult problem. For the elementary abelian case, all we have shown so far, apart from some minor cases, is that there are gaps, i.e. sets $K = \{1, \ldots, k;\ \text{some } k \in \mathbf{N}\}$ of exponents of primes p which are such that $p^i \not| \ m$ $(i \in K)$ for any $m \in det\ (\mathbf{Z}{C_p}^n);\ n \in \mathbf{N}$.

These are at the two extremes in terms of existence of critical exponents, so for other abelian groups the divisibility question lies somewhere in between them. At present, a method to tackle the critical exponents for general abelian groups is still lacking. So instead we consider the question of allowable exponents: if $n = \#G$, $p \mid n$ is a prime, is there an $n_0 \in \mathbf{N}$ such that $\forall n_1 > n_0\ \exists\ m \in det(\mathbf{Z}G)$ such that $p^{n_1} \| m$; i.e. are all sufficiently large exponents allowed? By Theorem 11, we consider G of prime power order.

Recall the following elementary Lemma: if $(a, b) = 1$, where $a, b \in \mathbf{N}$, then $\forall n \in \mathbf{N};\ n > ab\ \exists x, y \in \mathbf{N}$ such that $n = ax + by$. Now, by the absolute multiplicative property of norms, if $m_1, m_2 \in det(\mathbf{Z}G)$ such that $p^{k_1} \| m_1,\ p^{k_2} \| m_2$ then $m_1^{a_1} m_2^{a_2} \in det(\mathbf{Z}G)$ with $p^{a_1 k_1 + a_2 k_2} \| m_1^{a_1} m_2^{a_2}$, where $a_1, a_2 \in \mathbf{N}$. Hence it is sufficient to show that there exists $k_1, k_2 \in \mathbf{N}$ such that $p^{k_1} \| m_1,\ p^{k_2} \| m_2$ and $(k_1, k_2) = 1$ where $m_1, m_2 \in det(\mathbf{Z}G)$. Careful selection of α of the form $\sum_{g \in G} n_g g;\ n_g \in \mathbf{Z}$ may reveal the necessary p-values in the formula $det\ \alpha = \prod_{\chi \in \hat{G}} \chi(\alpha)$. However, the simple method in the following Lemma is sufficient.

LEMMA 18 *Let G be a finite abelian p-group; $\#G = p^n$ say. Then $\exists n_0 \in \mathbf{N}$ such that $\forall n_1 > n_0$ $\exists \alpha \in \mathbf{Z}G$ with $p^{n_1} \| det\ \alpha$.*

Proof We have $\mathbf{Q}G \cong \bigoplus_{j\in J} K_j$, where at least one summand, K_1 say, is $\mathbf{Q}$, and as usual let $S = \bigoplus_{j\in J} \mathbf{Z}_j \supseteq \mathbf{Z}G$. For $\alpha = (\alpha_j)_{j\in J}$ $(\alpha_j \in \mathbf{Z}_j)$, we have

$$\alpha \in \mathbf{Z}G \Leftrightarrow \sum_{j\in J} T_j(\alpha_j \overline{\chi_j}(g)) \in p^n\mathbf{Z}. \tag{3.14}$$

Let $\beta \in S$ be arbitrary, and take $\alpha = p^n\beta$. Then, for all $j \in J$ we have

$$T_j(\alpha_j\overline{\chi_j}(g)) = p^n T_j(\beta_j\overline{\chi_j}(g)\ \in p^n\mathbf{Z},$$

so certainly, by (3.14), $\alpha \in \mathbf{Z}G$. Suppose $p^k \| \ det\ \alpha$. Let $k_1 \in \mathbf{N}$. We form a new $\alpha^* \in S$ by putting $\alpha_1^* = p^{k_1}\alpha_1$, and $\alpha_j^* = \alpha_j$ for $j > 1$. Then, again by (3.14), $\alpha^* \in \mathbf{Z}G$ and $p^{k+k_1} \| det\ \alpha^*$. □

CHAPTER 3
Circulants

0. Introduction

In this chapter, by specialising to the case $K = \mathbf{Q}C_n$, $\mathcal{O} = \mathbf{Z}C_n$, we are able to present a complete description of critical exponents. We start with some general results obtained by elementary methods - these were first proved by Morris Newman in [5,6]. However, Newman showed that there is no simple formula for $det(\mathbf{Z}C_{p^k})$. Hence we are prompted to use the machinery of Chapter 1, giving a fully detailed account of ranges which are specially modified in this case. We show that almost every m with allowable exponents at the $p \mid n$ has a maximal range. We conclude the chapter by showing almost all $m \leq x$ with allowable exponents lie in $det(\mathbf{Z}C_n)$, giving an asymptotic expansion for the number of exceptions.

1. The Group Determinant for the Cyclic Group

For the group determinant $det(\mathbf{Z}G)$, let $G = C_n$, the cyclic group of order n, which we may regard as the group of integers under addition modulo n. Hence its elements are, say, $g_1, g_2, \ldots, g_n$ where $g_i \equiv i-1 \ (mod\ n); i = 1, 2, \ldots, n$. Thus in the matrix, for the (i,j) position we put x_k where $k \equiv i + j - 1 \ (mod\ n)$. For any $0 \neq \alpha \in \mathbf{Q}G$ we define, as in §1 of Chapter 2, $L_\alpha : \mathbf{Q}G \to \mathbf{Q}G$ by $x \mapsto \alpha x$ $(\forall x \in \mathbf{Q}G)$, which gives us a $\mathbf{Q}-$linear map $(\mathbf{Q}^n \to \mathbf{Q}^n)$. Recall also that $N(\alpha) := det\ L_\alpha$.

Suppose $\alpha \in \mathbf{Z}G$, then L_α is given by an $n \times n$ matrix with integer entries. In fact, suppose $\alpha = \sum_{k=1}^{n} z_{n-k} g_k$, where $z_{n-k} \in \mathbf{Z}$. Then L_α is given by:

$$\alpha g_i = \sum_{k=1}^{n} z_{n-k} g_k g_i; \quad i = 1, 2, \ldots, n.$$

$$= \sum_{j=1}^{i} z_{i-j} g_j + \sum_{j=i+1}^{n} z_{n-(j-i)} g_j \quad ; i = 1, 2, \ldots, n.$$

So we have in matrix form:

$$L_\alpha = \begin{pmatrix} z_0 & z_{n-1} & \dots & z_1 \\ z_1 & z_0 & \dots & z_2 \\ \vdots & \vdots & \ddots & \vdots \\ z_{n-1} & z_{n-2} & \dots & z_0 \end{pmatrix} \tag{1.1}$$

Hence L_α is a circulant. We now proceed to find norms by examining the determinant of this matrix.

2. Some results for Circulants

To emphasise the matrix form, for $G = C_n$, we denote $det(\mathbf{Z}G)$ by $\Delta_n(\underline{x})$.

Let ζ be an n^{th} root of unity. In (1.1), relabelling the $x_i's$ and multiplying row i $(1 \leq i \leq n)$ by ζ^i gives:

$$\zeta^{-\sum_{i=1}^{n} i} \quad \Delta_n(\underline{x}) = \begin{vmatrix} x_0\zeta^{-1} & x_1\zeta^{-1} & \dots & x_{n-1}\zeta^{-1} \\ x_{n-1}\zeta^{-2} & x_0\zeta^{-2} & \dots & x_{n-2}\zeta^{-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1\zeta^{-n} & x_2\zeta^{-n} & \dots & x_0\zeta^{-n} \end{vmatrix} \tag{2.1}$$

Add all the rows into row n to give all entries in row n of the form $\zeta^k(x_0 + \zeta x_1 + \ldots + \zeta^{n-1}x_{n-1})$ where $k \in \mathbf{Z}$. Thus, in $\mathbf{C}[\underline{x}]$, for each ζ, $x_0 + \zeta x_1 + \ldots + \zeta^{n-1}x_{n-1}$ divides $\Delta_n(\underline{x})$. This implies

$$\Delta_n(\underline{x}) = \left\{ \prod_{\zeta^n=1} \left(\sum_{i=0}^{n-1} x_i\zeta^i \right) \right\} .u(\underline{x}), \text{ where } u(\underline{x}) \text{ is some polynomial in } \mathbf{C}[\underline{x}].$$

By comparing degrees $u(\underline{x})$ is a constant and so $c = 1$ (e.g. $x_0 \mapsto 1$; $x_j \mapsto 0$, $j > 0$ gives $\Delta_n(\underline{x}) = 1$).

Thus we have

$$\Delta_n(\underline{x}) = \prod_{\zeta^n=1} f(\zeta) \text{ , where}$$

$$f(T) = x_0 + x_1T + \ldots + x_{n-1}T^{n-1} \quad ; \underline{x} \in \mathbf{Z}^n. \tag{2.2}$$

General case : some particular values

Consider

$$1 + x + \ldots + x^{n-2} + x^{n-1} \left(= \frac{x^n - 1}{x - 1} \right) = \prod_{\zeta^n = 1 \neq \zeta} (x - \zeta).$$

Then putting $x = 1$ gives

$$n = \prod_{\zeta^n = 1 \neq \zeta} (1 - \zeta) \tag{2.3}$$

Suppose $(r, n) = 1$, for some $r \in \mathbf{N}$. Then, by Euclid, $\exists s, t \in \mathbf{Z}$ such that $1 = rs + nt$. Hence $\zeta = \zeta^{rs'}$ where $s' \equiv s \ (mod\ n)$, $1 \leq s' < n$. Thus if $\zeta \neq 1$ then

$\frac{1-\zeta^r}{1-\zeta} = 1+\zeta+\zeta^2+\ldots+\zeta^{r-1} = \frac{1-\zeta^r}{1-(\zeta^r)^s} = \frac{1}{g(\zeta)}$, with $g(\zeta) \neq 0$ a unit in $\mathbf{Z}[\zeta]$; hence $\frac{1-\zeta^r}{1-\zeta}$ is a unit in $\mathbf{Z}[\zeta]$. Now choose

$f(T) = a(1+T+T^2+\ldots+T^{n-1})+(1-T^r)$, where $a \in \mathbf{Z}$, $0 < r < n$, $(r, n) = 1$.

Then $\zeta^n = 1 \neq \zeta$ implies $f(z) = 1 - \zeta^r$ (for the sum of the roots of unity is zero). Also, $f(1) = an$. Hence,

$$\Delta_n(\mathbf{Z}^n) \supseteq an \prod_{\zeta^n = 1 \neq \zeta} (1 - \zeta^r) = an \prod_{\zeta^n = 1 \neq \zeta} (1 - \zeta) = an^2.$$

Putting $a = \pm 1, \pm 2, \ldots$ gives

$$\Delta_n(\mathbf{Z}^n) \supseteq n^2 \mathbf{Z}. \tag{L.1}$$

So the circulant has a positive density of values.

Now let

$$f(T) = a(1 + T + \ldots + T^{r-1}) + b(1 + T + T^2 + \ldots + T^{n-1}).$$

Then for $\zeta^n = 1 \neq \zeta$, $f(\zeta) = a\left(\frac{1-\zeta^r}{1-\zeta}\right)$, and $f(1) = ar + bn$. Hence

$$\Delta_n(\mathbf{Z}^n) \supseteq (ar + bn)a^{n-1}.1$$

Putting $a = 1$ gives

$$\Delta_n(\mathbf{Z}^n) \supseteq r = b + n \text{ where } (r, n) = 1 \text{ and } b \text{ arbitrary } \in \mathbf{Z} \qquad (L.2)$$

Thus $\Delta_n(\mathbf{Z}^n)$ contains all integers k which are coprime with n.

Case : $\Delta_p(\mathbf{Z}^p)$, p prime

(i) $p = 2$: From (2.2) we have

$$\Delta_n(\underline{x}) = (x_0 - x_1)(x_0 + x_1) = k, \text{ say } (x_i, k \in \mathbf{Z}).$$

Necessary conditions for k are: $k = de$ where $d \mid k$, $e \mid k$, $x_0 - x_1 = d$, $x_0 + x_1 = e$) and $d \equiv e \ (mod\ 2)$. Hence d, e are both odd or both even, and these are sufficient conditions for k as

$$\left.\begin{aligned} x_0 &= \frac{1}{2}(e + d) \\ x_1 &= \frac{1}{2}(e - d) \end{aligned}\right\} \Rightarrow \ x_o, x_1 \in \mathbf{Z}.$$

Thus $k \in \Delta_2(\mathbf{Z}^2)$ iff $k \not\equiv 2 \ (mod\ 4)$, i.e.

$$\Delta_2(\mathbf{Z}^2) = (\mathbf{Z} \setminus 2\mathbf{Z}) \dot{\cup} 2^2\mathbf{Z}. \qquad (L.3)$$

(ii) odd prime p: From (L.1) and (L.3), $\Delta_p(\mathbf{Z}^p)$ contains $(\mathbf{Z} \setminus p\mathbf{Z}) \dot{\cup} p^2\mathbf{Z}$. We show, after a couple of Lemmas, that this is all. For the remainder of this section we let $\zeta_n = e^{2\pi i/n}$.

LEMMA 19 *For any $\alpha \in \mathbf{N}$, $p\mathbf{Z}_K = (1 - \zeta_{p^\alpha})^{\phi(p^\alpha)}$, where $K = \mathbf{Q}(\zeta_{p^\alpha})$.*

Proof In Appendix C it is shown for the field $K = \mathbf{Q}(\zeta_{p^\alpha})$, that p ramifies totally in $\mathbf{Z}_K$, i.e. $p\mathbf{Z}_K = \wp_\alpha^{\phi(p^\alpha)}$, where $\wp_\alpha$ is the prime ideal $(p, 1 - \zeta_{p^\alpha})$.

However, we have

$$p = \prod_{p \nmid s} (1 - \zeta_{p^r}^s)$$

So p belongs to $(1 - \zeta_{p^\alpha})$; hence $\wp_\alpha$ is just $(1 - \zeta_{p^\alpha})$□

LEMMA 20 (a)*Suppose* $k \in \Delta_n(\mathbf{Z}^n)$, *with* $n \in \mathbf{N}$, $k \in p\mathbf{Z}$. *Then,*

$$k = \prod_{d|n} N_d(f(\zeta_d)),$$

where $f(T) \in \mathbf{Z}[T]$; $\partial f < n$, $N_d(\beta) := N_{\mathbf{Q}(\zeta_d)/\mathbf{Q}}(\beta)$.

(b) Suppose further that $n = p^l$ *is a prime power. Then* $p \mid f(1)$, $p \mid N_d(f(\zeta_d))$ *for each* d *in the product.*

Proof (a): From (2.2) we have

$$k = \prod_{\zeta^n=1} f(\zeta),$$

where $f(T) \in \mathbf{Z}[T]$, $\partial f < n$. Then

$$k = \prod_{d|n} \left\{ \prod_{ord\ \zeta=d} f(\zeta) \right\}.$$

Since the bracketed term is just a product of all conjugates in $\mathbf{Q}(\zeta_d)$ ($\phi(d)$ in total), then

$$k = \prod_{d|n} N_d(f(\zeta_d)).$$

(b) We now assume that $n = p^l$ where $l \in \mathbf{N}$. In $\mathbf{Z}[\zeta_n]$ we have by Lemma 19 that $p\mathbf{Z}[\zeta_n] = \wp^{\phi(n)}$, where $\wp = (1 - \zeta_n)$ is prime. As $p \mid k = \prod_{\omega^n=1} f(\omega)$, we deduce that $\wp \mid$ some $f(\omega) = f(\zeta_n^r)$. However $x - y \mid f(x) - f(y)$ in $\mathbf{Z}[x, y]$. Hence for every s, $\zeta_n^r - \zeta_n^s \mid f(\zeta_n^r) - f(\zeta_n^s)$ in $\mathbf{Z}[\zeta_n]$. But $\zeta_n^r - \zeta_n^s \in \wp$, and also $f(\zeta_n^r) \in \wp$. Consequently $f(\zeta_n^s) \in \wp$ for all s. In particular, for every $d \mid n$, $N_d(\zeta_d)) \in \wp \cap \mathbf{Z} = p\mathbf{Z}$. The case $d = 1$ gives $p \mid f(1)$□

COROLLARY 21 *If* $n = p^l$, *then* $p^{l+1} \mid k$.

Proof We have $p \mid f(1)$, $p \mid N_{p^\alpha}(f(\zeta_{p^\alpha}))$, $\alpha = 1, \ldots, l$□

COROLLARY 22 $\Delta_p(\mathbf{Z}^p) = (\mathbf{Z} \setminus p\mathbf{Z}) \dot{\cup} p^2\mathbf{Z}$.

Proof From Corollary 21, if $k \in p\mathbf{Z}$ then $k \in p^2\mathbf{Z}$ and now the result follows from (L.1) and (L.2) $\square$

Considering circulants of order p^2, we observe $\Delta_{3^2}(\mathbf{Z}^{3^2}) \supseteq 3^3\mathbf{Z}$ (in (2.2) put $f(x) = 1 + x + x^3$). But in general, $\Delta_{p^2}(\mathbf{Z}^{p^2}) \neq (\mathbf{Z} \setminus p\mathbf{Z}) \dot{\cup} p^3\mathbf{Z}$: Newman showed (in [6]) that for odd primes $p > 3$, $k > 1$ that $p^{k+1} \notin \Delta_{p^k}(\mathbf{Z}^{p^k})$.

For $p = 2$ there is a slight strengthening on Corollary 21.

LEMMA 23 *Suppose* $n = 2^k$ $(k - 1 \in \mathbf{N})$. *Then if* $m \in \Delta_n(\mathbf{Z}^n)$, *and* $2|m$, *then* $2^{k+2}|m$.

Proof Take $k \geq 3$. From (2.2) and Lemma 20 we have:

$$m = f(1)f(-1)f(i)f(-i)\prod_{j=3}^{k} N_{2^j}\left(f(\zeta_{2^j})\right),$$

where f is a polynomial; $\partial f = n - 1$,

By Lemma 20, $2 \mid N_{2^j}(f(\zeta_{2^j}))$ for $j = 3, \ldots k$. So 2^{k-2} divides the $\prod_{j>2} N_{2^j}(f(\zeta_{2^j}))$.

We now show that $2^4 \mid f(1)f(-1)f(i)f(-i)$ (which will hence include also the case $k = 2$). Reduce $f \ mod\ x^4 - 1$, so WLOG $\partial f \ (mod\ x^4 - 1) < 4$; so $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3$, say. Suppose $2 \| f(1)$, $2 \| f(-1)$, and $2 \| f(i)f(-i)$ - by the previous argument these are the smallest powers - then we have:

$$\begin{array}{rcrll} f(1) & = & a_0 + a_1 + a_2 + a_3 & = 4b + 2 & < 1 > \\ f(-1) & = & a_0 - a_1 + a_2 - a_3 & = 4c + 2 & < 2 > \\ f(i)f(-i) & = & (a_0 - a_2)^2 + (a_1 - a_3)^2 & = 4d + 2 & < 3 > \end{array}$$

Adding $< 1 >$ and $< 2 >$ gives $a_0 + a_2 = 2(b + c + 1)$, which is even. Hence $a_0 - a_2$ is even. Similarly, subtracting $< 2 >$ from $< 1 >$ gives $a_1 - a_3$ even. Thus, $2^2 \mid (a_0 - a_2)^2 + (a_1 - a_3)^2$ which is a contradiction to $< 3 >$, and so $2^4 | f(1)f(-1)f(i)f(-i)$, as required $\square$

LEMMA 24 $\Delta_4(\mathbf{Z}^4) = (\mathbf{Z} \setminus 2\mathbf{Z}) \dot{\cup} 16\mathbf{Z}$

Proof We have, by (L.2), $\Delta_4(\mathbf{Z}^4) \supseteq (\mathbf{Z} \setminus 2\mathbf{Z})$ and by Lemma 23, $\Delta_4(\mathbf{Z}^4) \subseteq$

$\subseteq (\mathbf{Z} \setminus 2\mathbf{Z}) \dot{\cup} 16\mathbf{Z}$. But (L.1) gives $\Delta_4(\mathbf{Z}^4) \supseteq 16\mathbf{Z}$. Thus the assertion of the Lemma is forced$\square$

We've shown necessary conditions for powers of primes which divide possible values of the circulant. By a simple trick, which uses the Binomial Theorem, we show that provided certain conditions are satisfied then there are circulants which may be divisible by arbitrarily high powers of a given prime divisor of n.

PROPOSITION 25 *Suppose that for an odd prime p, $p^s \parallel n$ ($s \in \mathbf{N}$). Then $\forall t \in \mathbf{N}$ there exists a value of the circulant $\Delta_n(\mathbf{Z}^n) = m$, such that $p^{s+t} \parallel m$.*

Proof In (2.2), let $f(x) = a + bx$, $a, b \in \mathbf{Z}$. So the corresponding value of the circulant is given by,

$$\begin{aligned} m &= \prod_{\zeta^n=1} (a + b\zeta) \\ &= (-b)^n \prod_{\zeta^n=1} \left(\frac{-a}{b} - \zeta \right) \\ &= (-b)^n \left(\left(\frac{-a}{b} \right)^n - 1 \right) \\ &= a^n - (-1)^n b^n. \end{aligned}$$

Now put $a = 1 + cb$ ($c \in \mathbf{Z}$), and let $b = -1$. Then, $m = (1 - c)^n - 1$. For any $p \mid n$, now suppose $n = p^s e$, where $p \nmid e$. Put $c = p^t d$ with $(d, n) = 1$, any $t \in \mathbf{N}$. Then,

$$\begin{aligned} m &= (1 - dp^t)^{ep^s} - 1 \\ &= \sum_{k=0}^{ep^s} \binom{ep^s}{k} (-dp^t)^k - 1 \\ &= \sum_{k=1}^{ep^s} \binom{ep^s}{k} (-dp^t) \\ &= d^k ep^{s+t} + \ldots \end{aligned}$$

We show that p^{s+t+1} divides all except the first term. Hence $p^{s+t} \parallel m$. For this it is sufficient to show that $k' > l$ where $p^{k'} \parallel \binom{ep^s}{a}$ ($a \geq 2$) and $p^l \parallel ep^s c$. So

consider the powers of p in the numerator and denominator of

$$\frac{\binom{n}{a}c^a}{nc} \quad (n = ep^s). \tag{2.4}$$

We want to show that the power of p which divides the numerator is greater than that which divides the denominator. In (2.4) we may cancel a factor of n, so we are left with

$$\frac{A}{B} \quad \text{where} \begin{cases} A &= (n-1)(n-2)\dots(n-a+1)c^{a-1} \\ B &= 1.2\dots(a-1)a \end{cases} \quad (a \geq 2) \tag{2.5}$$

Three cases arise:

(i) If $a < p$ then p does not divide the denominator and we are done.

(ii) If $a = p$ then $p^{p-1} \mid$ the numerator, whereas $p \parallel$ the denominator, and we are done.

(iii) If $a > p$, consider products of the form

$$A_N = \prod_{\alpha=1}^{p^N} \alpha \ , \text{ so e.g. } A_2 = 1\dots p\dots 2p\dots(p-1)p\dots p^2.$$

Let $p^{k_N} \parallel A$. Then $k_2 = p+1$, $k_3 = p(p+1)+p$, $\dots$, $k_N = pk_{N-1}+1$. And it is then trivial to show that

$$k_N = \sum_{i=0}^{N-1} p^i = \frac{p^m - 1}{p-1} \tag{2.6}$$

(a) Consider now the power of p which divides $(n-1)(n-2)\dots(n-a+1)$; $(a-1$ terms). Then, *mod* p, these terms cover all the residue classes at least $\left[\frac{a-1}{p}\right]$ times, where $[x]$ denotes the largest integer less than or equal to x. In fact, it is an easy exercise to show that $p|A$ $\sum_{\alpha=1}^{\infty}\left[\frac{a-1}{p^\alpha}\right]$ times.

(b) Next, we look at the denominator of (2.5). Suppose $lp^{N-1} < a \leq$ $\leq (l+1)p^{N-1}$, where $1 \leq l < p$ $(N \geq 2)$, then

$$V_p(a) \leq (l+1)k_{N-1} + 1. \tag{2.7}$$

In (2.5), $p^j \,|\, c^{a-1}$ where $j \geq a-1 \geq lp^{N-1}$, and $p^{j'} \,|\, (n-1)(n-2)\ldots(n-a+1)$ where $j' \geq \left[\frac{a-1}{p}\right] \geq lp^{N-2}$. Hence

$$V_p(A) \geq lp^{N-1} + lp^{N-2}. \tag{2.8}$$

Now using (2.6) in (2.7) gives:

$$\begin{aligned}(l+1)k_{N-1}+1 &= (l+1)\left(\frac{p^{N-1}-1}{p-1}\right)+1 \\ &\leq \left(\frac{l+1}{2}\right)(p^{N-1}-1)+1 \\ &\leq \left(\frac{l+1}{2}\right)p^{N-1} \\ &< lp^{N-1}+lp^{N-2}.\end{aligned}$$

This is as required. Now put $c = \prod_{p|n} c_p$. Then clearly $m = (1-c)^n - 1 \in \Delta_n(\mathbf{Z}^n)$ with required critical exponents $\square$

We may perform the above procedure in turn for each prime divisor of n, but no indication is given of possible primes, dividing m and coprime with n, i.e. which are 'compatible." This is a significant problem which we address after tidying up the discussion on critical exponents, by establishing sufficient conditions for 2 dividing n.

LEMMA 26 *Suppose that* $2^s \,\|\, n$ $(s \in \mathbf{N})$. *Then* $\forall t \geq 2$ *there exists a value of the circulant* $\Delta_n(\mathbf{Z}^n) = m$, *such that* $2^{t+s} \,\|\, m$.

Proof The proof is exactly as in the Proposition, putting $p = 2$, except that condition (i) does not apply; and in (ii), if $a = 2$ then an extra exponent for c is forced. In this case we have in (2.5) that $A = (n-1)c$, and $B = 2$. Hence $2^t \,|\, A$, so that with $2 \,\|\, B$, we need $t > 1$. The rest of the proof goes through$\square$

Circulants of order p^2 and their corresponding ideals in the group ring.

The main purpose of using ray-classes, as will be shown in the next section, is to establish asymptotic results. However, in a few simple cases, for a given

prime exponent e of a value of a circulant, we may find information concerning the corresponding ideals in S. We illustrate this for the case $\Delta_{p^2}(\mathbf{Z}^{p^2})$, p odd.

We've shown that if $m \in \Delta_{p^2}(\mathbf{Z}^{p^2})$, $p \mid m$, then $p^3 \mid m$ (Corollary 21), and also that $\exists m \in \Delta_{p^2}(\mathbf{Z}^{p^2})$ such that $p^3 \parallel m$ (Proposition 25). So let $m = p^3 r$. From (L.1), $\Delta_{p^2}(\mathbf{Z}^{p^2}) \supseteq p^4\mathbf{Z}$ so the only values of the circulant still to be shown are those m with $p \nmid r$. The question of which r are allowed seems difficult to answer. However, such r do exist and it is for the corresponding m that we find associated ideals $\boldsymbol{a} \lhd S$; $N\boldsymbol{a} = m$. By the discussion in Chapter 1, §1, $\boldsymbol{a} = \boldsymbol{b}g$, $N\boldsymbol{b} = p^3$ and $Ng = r$. The $\mathbf{Q}$-algebra isomorphism in Theorem 9, (1.1), gives $\mathbf{Q}G \cong \mathbf{Q} \bigoplus \mathbf{Q}(\zeta_p) \bigoplus \mathbf{Q}(\zeta_{p^2})$. Here $S = \mathbf{Z} \bigoplus \mathbf{Z}[\zeta_p] \bigoplus \mathbf{Z}[\zeta_{p^2}]$ and $\boldsymbol{a}$ may be expressed as $\boldsymbol{a}_1 \bigoplus \boldsymbol{a}_2 \bigoplus \boldsymbol{a}_3$, with $\boldsymbol{b} = \boldsymbol{b}_1 \bigoplus \boldsymbol{b}_2 \bigoplus \boldsymbol{b}_3$, $\boldsymbol{g} = \boldsymbol{g}_1 \bigoplus \boldsymbol{g}_2 \bigoplus \boldsymbol{g}_3$, indicating the 'bad' and 'good' components in each summand. We have from (2.2) and Lemma 20,

$$m = \prod_{\zeta^{p^2}=1} f(\zeta) = \prod_{f \mid p^2} N_d\left(f(\zeta)\right) = f(1) N_p\left(f(\zeta_p)\right) N_{p^2}\left(f(\zeta_{p^2})\right).$$

From Lemma 20 we deduce further that $N\boldsymbol{b}_i = p^{\alpha_i}$; $\alpha_i \in \mathbf{N}$. Hence $\alpha_1 = \alpha_2 = \alpha_3 = 1$ is the only possibility.

Put $f(T) = A + BT$, where $A, B \in \mathbf{Z}$. Then in (2.2), $m = A^n - (-B)^n$ is a value of the circulant. Let $A := a + cp$, $B = -a$; $a, c \in \mathbf{Z}$, with $p \nmid a$, $p \nmid c$. Then it is easily seen from the Binomial Theorem that $p^3 \parallel m$. We have:

$$\begin{aligned} m &= \prod_{\zeta^{p^2}=1} (1 + \frac{cp}{a} - \zeta) \\ &= a^{p^2} \frac{cp}{a} N_p(1 + \frac{cp}{a} - \zeta_p) N_{p^2}(1 + \frac{cp}{a} - \zeta_{p^2}). \\ &= N\boldsymbol{a}. \end{aligned}$$

Hence

$$\boldsymbol{a} = a^{p^2-1} cp\mathbf{Z} \bigoplus (1 + \frac{cp}{a} - \zeta_p) \bigoplus (1 + \frac{cp}{a} - \zeta_{p^2}),$$

where $\mathfrak{b}_1 = p\mathbf{Z}$, $\mathfrak{b}_2 = (1-\zeta_p)$ and $\mathfrak{b}_3 = (1-\zeta_{p^2})$ (see Lemma 19). By Theorem A6, $N\mathfrak{b}_i = p$; $i = 1,2,3$). The corresponding $\mathfrak{g}$ is given by

$$\mathfrak{g}_1 = a^{p^2-1}c\mathbf{Z},\ \mathfrak{g}_2 = \left(1+\frac{pc}{a(1-\zeta_p)}\right),\ \mathfrak{g}_3 = \left(1+\frac{pc}{a(1-\zeta_{p^2})}\right).$$

3. Asymptotics for values of a circulant

So far we have shown (after Newman) that $\Delta_n(\mathbf{Z}^n)$ contains all integers a such that a and n are coprime (see (L.2)). We've also shown that if $p^{k_p} \parallel n$, where p is an odd prime and $k_p \in \mathbf{N}$, then there is a value m of the circulant such that $p^{k_p+s} \parallel m$ for any $s \in \mathbf{N}$. For $p = 2$, if $p \parallel n$, then there is a value m of the circulant such that $p^{1+s} \parallel m$ for any $s \in \mathbf{N}$; if $p^{k_p} \parallel n$, with $k_p - 1 \in \mathbf{N}$, then there is a value m of the circulant such that $p^{k_p+s} \parallel m$ for any $s \in \mathbf{N}$. (These results are all from the previous section.)

Suppose for any prime p that $p^{k_p+s} \parallel m$. Let $\rho(p^{k_p+s})$ be the density of those integers g coprime with p such that $m = gp^{k_p+s}$ is a value of $\Delta_n(\mathbf{Z}^n)$. More formally,

$$\rho(p^{k_p+s}) := \lim_{N\to\infty} \frac{\#\{g;\ (g,p)=1,\ p^{k_p+s} \in \Delta_n(\mathbf{Z}^n),\ g \le N\}}{\#\{g \le N\}},$$

provided that the limit exists.

We shall show that the density of those integers which are values of the circulant is

$$\prod_{p|n} \delta_p, \tag{3.1}$$

where

$$(p>2) \qquad \delta_p = \left(1-\tfrac{1}{p}\right) + \textstyle\sum_{t=k_p+1}^{\infty} \rho(p^t)p^{-t}$$

$$(p=2) \quad \delta_2 = \begin{cases} 1-\frac{1}{2}+\frac{1}{2^2} & (k_2=1) \\ 1-\frac{1}{2}+\sum_{t=k_p+2}^{\infty} \rho(2^t)2^{-t} & (k_2>1) \end{cases}$$

We show that in (3.1), for each t, $\rho(p^t)$ has density 1. In fact, we show that for odd primes p,

$$\delta_p = 1 - \frac{1}{p} + \frac{1}{p^{k_p}(p-1)},$$

and for $p = 2$,

$$\delta_2 = \begin{cases} 1 - \frac{1}{2} + \frac{1}{2^2} & (k_2 = 1) \\ 1 - \frac{1}{2} + \frac{1}{2^{1+k_2}} & (k_2 > 1) \end{cases}$$

This requires the methods of Chapter 1.

Modified Ray Classes

We have $G = \mathbf{C}_n$, the cyclic group with n elements. Now define K_j and $\mathbf{Z}_j$ as in §1, Chapter 2, and let $S = \sum_{j \in J} \mathbf{Z}_j$. Let $R = \mathbf{Z}G$, then certainly $1 \in R$ and setting $f = n$, $fS \subseteq R$ (for instance, we may regard S/R as an abelian group under addition, which clearly has order dividing f). Hence those (integral) ideals $\boldsymbol{a}$ which are members of I, the set of ray-classes (see §1, Chapter 1) are members of R. For the circulants problem, we may define a modified ray-class equivalence relation $\dot{\sim}$ as follows.

For ideals $\boldsymbol{g}_1$, $\boldsymbol{g}_2$, with $\boldsymbol{g}_1 + fS = \boldsymbol{g}_2 + fS = S$ we define

$$\boldsymbol{g}_1 \dot{\sim} \boldsymbol{g}_2 \iff \rho_1 \boldsymbol{g}_1 = \rho_2 \boldsymbol{g}_2$$

where ρ_1, $\rho_2 \in R$, $N(\rho_1 \rho_2) > 0$, and $(\rho_1, fS) = (\rho_2, fS) = S$.

It is easy to check that by defining $[\boldsymbol{g}]_0 = \{\boldsymbol{g}';\ \boldsymbol{g}' \dot{\sim} \boldsymbol{g}\}$ and $[\boldsymbol{g}_1]_0 \circ [\boldsymbol{g}_2]_0 = [\boldsymbol{g}_1 \boldsymbol{g}_2]_0$, then the set of modified ray-classes form a group Γ_0, which is a quotient group of I since $\sim \Rightarrow \dot{\sim}$.

We define also a 'range', $\mathcal{R}_0(g) := \{$ classes $[\boldsymbol{g}]_0 \in \Gamma_0;\ N\boldsymbol{g} = g\}$.

Our aim can now be expressed as follows: we wish to show that given b, which consists solely of prime factors of n satisfying the conditions for critical exponents, then almost every g, which consists of prime factors coprime with n,

is such that bg is a norm of some $\rho \in R$. This condition will be satisfied if given such 'b', almost every g has non-empty range, i.e. $\mathcal{R}_0(g) \neq \emptyset$.

We are able to achieve our objective with moderate effort because of the fact that for the circulants case since $g \in \Delta_n(\mathbf{Z}^n)$ where $(g,n) = 1$, then $\exists r \in R$ such that $N(rS) = g$ (some $r \in R$); hence as $[rS]_0 = [S]_0 = [1]_0$, the principal ray-class in I, $\mathcal{R}_0(g) \supseteq \{[1]_0\}$, the identity subset of 2^{Γ_0}. For an arbitrary finite group G, this is not true in general.

Ranges

Results for ranges $\mathcal{R}(g)$ carry over immediately to ranges $\mathcal{R}_0(g)$. To summarise then, we have:

LEMMA 27 *For $g_1, g_2 \in \mathbf{N}$, $\mathcal{R}_0(g_1 g_2) \supseteq \mathcal{R}_0(g_1)\mathcal{R}_0(g_2)$.*

LEMMA 28 *The identity subset $\{[1]_0\}$ has a unique maximal range, H_0, say.*

LEMMA 29 *The maximal ranges are precisely the cosets of H_0 in Γ_0.*

Now we use the special property of ranges for circulants.

LEMMA 30 $H_0 = \Gamma_0$. *(i.e. all the maximal ranges are equal to the whole group Γ_0.)*

Proof We have $[1]_0 \in \mathcal{R}_0(g)\ \forall g; (g,n) = 1$. So $\mathcal{R}_0(g) \subseteq H_0$. If $x \in \Gamma_0$, then xH_0 is a maximal range (by Lemma 29). Thus $xH_0 = \mathcal{R}_0(g') \subseteq H_0$. H_0 is a maximal range, so $xH_0 = H_0$ is forced, and hence all the maximal ranges are equal. As all classes are contained in a maximal range, we must have $H_0 = \Gamma_0$.□

Asymptotics

Let $\mathbf{N}_d := \{k \in \mathbf{N};\ (k,d) = 1\}$. Then, given b which satisfies the conditions on its prime exponents, $\exists r \in \mathbf{Z}G$ and at least one $g^* \in \mathbf{N}_n$ such that for each prime $p \,|\, n$, $V_p(N(rS))$ equals the given prime exponent for b; and $rS = \boldsymbol{b}^*$, where $N\boldsymbol{b} = b$, $N\boldsymbol{g}^* = g^*$. In fact a suitable $\boldsymbol{g}^*$ is $(g^*, 1, \ldots, 1) = g^*\mathbf{Z} \bigoplus_{1<d|n} \mathbf{Z}[\zeta_d]$.

We show now that in almost all cases (i.e. with density 1) all classes of Γ_0 contain ideals $\boldsymbol{g} \in S$ with $N\boldsymbol{g} = g$, so that $\mathcal{R}_0(g) = \Gamma_0$, and hence $\exists \boldsymbol{g}' \in S$ such that $N\boldsymbol{g}' = g$ with $\boldsymbol{g}^* \dot{\sim} \boldsymbol{g}'$, thus compatible with $\boldsymbol{b}$.

THEOREM 31

$$\lim_{N\to\infty} \frac{\#\{\text{good } g,\ g \le N;\ \mathcal{R}_0(g) = \Gamma_0\}}{\#\{\text{good } g,\ g \le N\}} = 1.$$

First we prove a general result on sets of prime numbers.

LEMMA 32 *Let $g \in \mathbf{N}_f$, and let $\mathcal{P}_1, \ldots, \mathcal{P}_{k'}$ be any sets of rational primes, each of positive natural density. Let $\Omega_i(g) := \#\{p_i \in \mathcal{P}_i; p_i \mid g$ (counting multiplicities)$\}(i = 1, 2, \ldots k')$. Then, for each i, given any $k \in \mathbf{N}$,*

$$D_i = \frac{\#\{g \in \mathbf{N}_f; \Omega_i(g) \le k\}}{\#\{g \in \mathbf{N}_f; g \le x\}} \to 0 \quad \text{as } x \to \infty.$$

(i.e. $\#\{g \in \mathbf{N}_f; \Omega_i(g)$ is bounded for some $i\}$ is of zero density).

Proof Clearly, WLOG we need only demonstrate this for $\mathcal{P}_1$, say. So suppose $\Omega_1(g) \le k$. We define a generating function $G(s)$ for the number of prime divisors of g with $\le k$ prime factors in $\Omega_1(k)$ by

$$G(s) := \left\{ \sum_{p\in\mathcal{P}_1} p^{-ks} + \sum_{p<q \text{ in } \mathcal{P}_1} p^{-(k-1)s} q^{-s} + \ldots \right\} \prod_{p\notin\mathcal{P}_1} (1 - p^{-s})^{-1} \quad (3.2)$$

$$= \sum_{g\in\mathbf{N}_f} \delta(g) g^{-s}, \text{ where } \delta(g) = \begin{cases} 1 & \text{if } \Omega_1(g) \le k \\ 0 & \text{otherwise} \end{cases} \quad (3.3)$$

From (3.2), noting that the term with k distinct primes is dominant (by virtue of the infinitude of $\mathcal{P}_i$), we obtain,

$$G(s) = \left\{ \sum_{p_1<\ldots<p_k\in\mathcal{P}_1} (p_1 \ldots p_k)^{-s} + J(s) \right\} \prod_{p\notin\mathcal{P}_1} (1 - p^{-s})^{-1}$$

$$= \left\{ \frac{1}{k!} \left(\sum_{p\in\mathcal{P}_1} p^{-s} \right)^k + J'(s) \right\} (s-1)^{-(1-\delta_1)},$$

where $\delta_1 > 0$ is the density of $\mathcal{P}_1$ and $J(s), J'(s)$ are negligible compared with $(\sum p^{-s})^k$ as $s \to 1^+$.

$$G(s) = \left\{ \frac{\delta_k}{k!} \left(\log \frac{1}{s-1} \right)^k + J''(s) \right\} (s-1)^{-(1-\delta_1)}.$$

Hence the singularity of $G(s)$ at $s = 1$ is weaker than $\frac{1}{s-1}$ and hence $D_1 \to 0$ as required. $_{Lemma\ 32}\square$

For details see [3].

Proof of Theorem Consider a prime $p \in \mathbf{N}_n$. We wish to find enough $\boldsymbol{g} \in S$ such that $N\boldsymbol{g} = p$ and the $\dot{\sim}$ classes $[\boldsymbol{g}]_0$ cover Γ_0. To do this, first observe the decomposition of p in $\mathbf{Z}[\zeta_d]$, where $d \,|\, f$. By the results in Appendix A, we have $p\mathbf{Z}[\zeta_d] = \wp_1 \wp_2 \ldots, \wp_g$ where, for $i = 1, \ldots, g$, $\wp_i$ is a prime ideal in $\mathbf{Z}[\zeta_d]$ with $N\wp_i = p^{f'}$ $(f' \in \mathbf{N})$. Then choosing each of the $\wp_i$ in turn will provide us with plenty of $\boldsymbol{g}$'s with $N\boldsymbol{g} = g$; $g \in \mathbf{N}_n$.

Now every $\sim$ class is of the form $(\mathcal{C}_1, \ldots, \mathcal{C}_d, \ldots)_{d|f}$, where $\mathcal{C}_d$ is a ray-class $(mod^{\times} n)$ in $S_d := \mathbf{Z}[\zeta_d]$. We've seen that Γ_0 is a quotient group of I, so we may define a natural epimorphism $\pi \twoheadrightarrow \Gamma_0$ by $\pi([a]) = [a]_0$ $\forall a \lhd S$. Hence

$$\mathcal{R}_0(p) = \{\pi(\mathcal{C}_1, \ldots, \mathcal{C}_d, \ldots);\ (\mathcal{C}_1, \ldots, \mathcal{C}_d, \ldots) \in \mathcal{R}(p)\}.$$

It is a well known fact that for each $d \,|\, f$ there exists an infinite number of primes $p_d \in \mathbf{N}_n$ such that $\pi(1, \ldots, 1, \mathcal{C}_d, 1, \ldots, 1) \in \mathcal{R}_0(p_d)$, and that, in fact,

$$\sum_{(1,\ldots,\mathcal{C}_d,\ldots) \in \mathcal{R}_0(p)} p^{-s} \sim \delta \log \frac{1}{s-1} \quad \text{as } s \to 1^+, \text{ some } \delta > 0.$$

This result is a special case of the theorem that prime ideals are equidistributed amongst ray-classes – see [4], p.326. Thus, for each $d \mid f(= n)$, and each $\mathcal{C}_d$ (a ray-class $mod^{\times} f$ of S_d), there is a set $\mathcal{P}(d, \mathcal{C}_d)$ of primes p_d in $\mathbf{N}$, of positive Dirichlet density, such that $\pi(1, \ldots, 1, \mathcal{C}_d, 1, \ldots, 1) \in \mathcal{R}_0(p_d)$ for all $p_d \in \mathcal{P}(d, \mathcal{C}_d)$.

Choosing one such p_d for all $d \mid f$, we have $\pi(\mathcal{C}_1, \ldots, \mathcal{C}_f) \in \mathcal{R}_0\left(\prod_{d|f} p_d\right)$, while the latter contains 1_0. The Lemma now tells us that, except for a subset of (natural) density 0, the typical members of $\mathbf{N}_f$ have enough prime factors from the various $\mathcal{P}(d, \mathcal{C}_d)$ to ensure that $\mathcal{R}_0(g) = \Gamma_0$, and so we are done$\square$

APPENDIX A

Generalised Minkowski Map

It is well known for a number field K, that $K = \mathbf{Q}(\alpha)$, for some $\alpha \in \mathbf{C}$. If $[K : \mathbf{Q}] = n$, then there are precisely n distinct embeddings of K into $\mathbf{C}$. Complex embeddings (i.e. image $\not\subseteq \mathbf{R}$) occur in complex conjugate pairs; let there be c of these, say. Hence, if r = the number of real embeddings, then $n = r + 2c$. Suppose $\{\alpha_1, \ldots, \alpha_n\}$ is a complete set of zeros of the minimum polynomial of α over $\mathbf{Q}$, then for $x \in K$ the embeddings F_i are of the form

$$F_i(x) = F_i(a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}) = a_0 + a_1\alpha_i + \ldots + a_{n-1}\alpha_i^{n-1}.$$

For non-zero such x, we define the signature $sgn\ x$ of x as the $r-$tuple $[\varepsilon_1, \ldots, \varepsilon_r]$, where ε_i denotes the sign of the $F_i(x)$; and it is assumed that the real conjugates of α are $\alpha_1, \ldots \alpha_r$. For $r = 0$ it is taken as positive in sign.

For a direct sum of number fields $\bigoplus_{j=1}^{k} K_j$, we define the signature to be the row vector of r_j-tuples; $sgn\ (x_j)$, where $x = \bigoplus x_j$ and r_j = the number of real embeddings of K_j into $\mathbf{C}$.

(see [4] p.46).

LEMMA A1 *Suppose ray-classes* $(mod^{\times} fS)$ *are defined as in Chapter 1, with* $I = \{$ *ray-classes* $(mod^{\times} fS)\}$. *Then* $(I, \cdot)$ *is a finite group.*

Proof I is clearly closed, associative and has identity, $\underline{1} = S$, so it remains to show that for all classes in I, there exists an inverse. Consider $\boldsymbol{a} \in S$. Then $\boldsymbol{a} = \bigoplus_{j=1}^{k} \boldsymbol{a}_j$; $0 \neq \boldsymbol{a}_j \triangleleft \mathbf{Z}_j$. For $[\boldsymbol{a}]$ we find $\alpha \in \boldsymbol{a}$ such that $\alpha S + fS = S$; and using the component notation for clarity, then $\alpha S = \bigoplus_{j=1}^{k} \boldsymbol{a}_j(\bigoplus_{j=1}^{k} \boldsymbol{b}_j) \subseteq \bigoplus_{j=1}^{k} \boldsymbol{b}_j$. So $\bigoplus_{j=1}^{k} \boldsymbol{b}_j + fS = S$. Now consider S/fS as a finite ring. $1 \in \mathcal{O} \supseteq fS$. So $\bar{\alpha}$ (the image of α $(mod^{\times} fS)$) is a unit in S/fS. Thus $\alpha^{2n_u} \equiv 1\ (mod^{\times} fS)$ where n_u = the number of units of S/fS. The '2' gives a positive embedding

in the Minkowski map, i.e. $\alpha^{2n_u} \gg 0$. We have also, $\alpha^{2n_u} S = (\alpha S)^{2n_u} = (\bigoplus_{j=1}^{k} \boldsymbol{a}_j)^{2n_u} (\bigoplus_{j=1}^{k} \boldsymbol{b}_j)^{2n_u} = \bigoplus_{j=1}^{k} \boldsymbol{a}_j (\bigoplus_{j=1}^{k} \boldsymbol{c}_j)$ for some $\bigoplus_{j=1}^{k} \boldsymbol{c}_j \triangleleft S$. It follows that $[\alpha^{2n_u} S] = \underline{1} = [\bigoplus_{j=1}^{k} \boldsymbol{a}_j][\bigoplus_{j=1}^{k} \boldsymbol{c}_j]$, which implies $[\bigoplus_{j=1}^{k} \boldsymbol{a}_j]^{-1} = [\bigoplus_{j=1}^{k} \boldsymbol{c}_j]$. The finiteness of $(I, \cdot)$ now follows from the fact that for each j, the ideal class group of S_j is finite (see [4] p.95) $\square$

Functorial properties of the Frobenius symbol

Notation For a Galois extension K_2/K_1 of number fields we denote the Galois group by $G(K_2/K_1)$.

Suppose L/K is Galois. Let $G = G(L/K)$. Now suppose Ω is some intermediate field, with $H = G(L/\Omega)$, $\Gamma = G(\Omega/K)$ (if defined). If $\wp$ is a prime ideal of K, unramified in L, then we have the following tower of fields, with the respective decomposition of $\wp$:

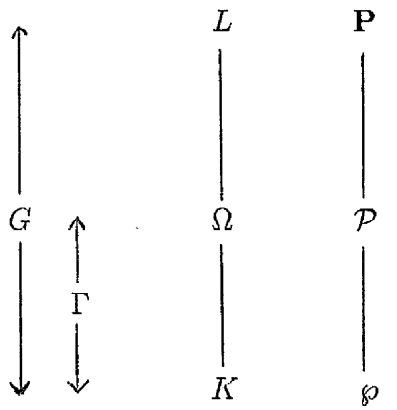

Fig. A.1

Let $\sigma = Frob(\boldsymbol{P}, L/K)$, the Frobenius element of G associated with $\boldsymbol{P}$.

LEMMA A2 *$Frob(\boldsymbol{P}, L/\Omega)$ is the smallest power of σ which lies in H.*

Proof Let $\tau = Frob(\boldsymbol{P}, L/\Omega)$. We may regard $\mathbf{Z}_\Omega/\mathcal{P}$ as an extension of degree f' over $\mathbf{Z}_K/\mathcal{P}$. Hence $N\mathcal{P} = N(\wp)^{\mathrm{f}'}$; since, $\forall x \in \mathbf{Z}_L$, $\sigma(x) \equiv x^{N\wp} (mod\ \boldsymbol{P})$, $\tau(x) \equiv x^{N\mathcal{P}} (mod\ \boldsymbol{P})$, it follows that $\tau = \sigma^{\mathrm{f}'} \in H$. Thus f' is

a multiple of the smallest f with $\sigma^{\mathrm{f}} \in H$. Now $\forall x \in \mathbf{Z}_L$ (and in particular, $\forall x \in \mathbf{Z}_\Omega$), $\sigma^{\mathrm{f}}(x) \equiv x^{(N\wp)^{\mathrm{f}}} (mod\ \boldsymbol{P})$, and so $\forall x \in \mathbf{Z}_\Omega$, $\sigma^{\mathrm{f}}(x) \equiv x^{(N\wp)^{\mathrm{f}}} (mod\ \boldsymbol{P})$. As $x - x^{(N\wp)^{\mathrm{f}}} \in \Omega$, $\sigma^{\mathrm{f}}(x) \equiv x^{(N\wp)^{\mathrm{f}}} (mod\ \boldsymbol{P} \cap \Omega = \mathcal{P})$ in $\mathbf{Z}_\Omega$. But $\mathbf{Z}_\Omega/\mathcal{P}$ is the unique extension of degree f ′ over $\mathbf{Z}_\Omega/\mathcal{P}$ which implies f′ | f, and so f′ =f □

LEMMA A3 *Suppose $G(\Omega/K)$ is defined. If π is the natural map:$G \to G(\Omega/K)$, then $\pi(\sigma) = Frob(\Omega/K, \wp)$.*

Proof We have $\forall x \in \mathbf{Z}_L, \sigma(x) \equiv x^{N\wp} (mod\ \boldsymbol{P})$. Under π, $\sigma(x) \mapsto \sigma'(x)$, where $\sigma' \in G(\Omega/K)$, and $\sigma'(x) \equiv x^{N\wp} (mod\ \boldsymbol{P} \cap F^{\dagger})$, where $F^{\dagger}$ is the fixed field of $ker\ \pi$. But $ker\ \pi = G(\Omega/K)$ fixes Ω, so $\sigma'(x) \equiv x^{N\wp} (mod\ \boldsymbol{P} \cap \Omega)$, i.e. $\sigma'(x) \equiv x^{N\wp} (mod\ \mathcal{P})$ □

APPENDIX B

Elements of norm -1

For any group ring R, if -1 is a norm of some element $r \in R$, then n is a norm of some $r' \in R \Leftrightarrow -n$ is also a norm of some $r'' \in R$. We wish to determine for what finite abelian groups G is -1 a member of the group determinant $det(\mathbf{Z}G)$.

Note that if the order of G is odd then via $\mathbf{Q}G \overset{\cong}{\mathbf{Q}} \bigoplus_{j\in J} K_j$, putting $\alpha = \underline{1} \in \bigoplus_{j\in J} \mathbf{Z}_j$ implies $(-1)^{\#G}\alpha \in \mathbf{Z}G$ and hence $(-\underline{1}) \in \mathbf{Z}G$ with $N(-\underline{1}) = -1$.

Thus we are left to consider G with even order.

We show, in Lemma A4, necessary and sufficient conditions for the existence of an element of G with the desired property. We then complete the task by showing that if there is an element of $\mathbf{Z}G$ whose norm is -1, then there exists an element of G, g say, such that $det\ g = -1$; hence, Lemma A4 is sufficient.

LEMMA A4 *Suppose G is any finite group of even order. Then $\exists g \in G$ with $det\ g = -1$ iff every Sylow 2-subgroup G_2 of G is cyclic.*

Proof Suppose $G = \{g_1, g_2, \ldots, g_n\}$, where $n = \#G$. For G, consider the permutation matrix Π, generated by some $g \in G$; $g_i \mapsto gg_i$ $i = 1, 2, \ldots, n$. Then $det\ g = sign\ \Pi$ where $gg_i = g_{\Pi(i)}$. Let $d = ord\ g$; then $g^0, g^1, \ldots, g^{d-1}$ are distinct and Π is a product of $\frac{n}{d}$ disjoint d cycles. Thus, $sign\ \Pi = (-1)^{(d-1)\frac{n}{d}} = (-1)^n(-1)^{\frac{n}{d}}$. Hence, $det\ g = -1$ iff $n \not\equiv \frac{n}{d}\ (mod\ 2)$. Suppose $n = 2^k s$; $s, k \in \mathbf{N}$ with s odd. Then $n \not\equiv \frac{n}{d}\ (mod\ 2)$ iff $d = 2^k t$ where $t \mid s$ is odd. Certainly, if $d = 2^k$ $(t = 1)$ is allowed then this is sufficient; this happens iff G_2 is cyclic. □

LEMMA A5 *Suppose that G in Lemma A4 is also abelian. Suppose $\exists \alpha \in \mathbf{Z}G$ such that $det\ \alpha = -1$. Then $\exists g \in G$ such that $det\ g = -1$.*

Proof Suppose $-1 = det\ \alpha = \prod_{\chi\in\hat{G}} \chi(\alpha)$, for some $\alpha \in \mathbf{Z}G$. We use the fact that $\mathbf{Q}G \overset{\cong}{\mathbf{Q}} \bigoplus_{j\in J} K_j$. From this, we may bracket together all characters χ which are mutually conjugate. Hence

$$-1 = \prod_{i=1}^{r} \left\{ \prod_{\chi \in C_i} \chi(\alpha) \right\}, \quad \text{where } C_i = i^{th} \text{ class of conjugate. Thus}$$

$$-1 = \prod_{i=1}^{r} N_i(\chi_i(\alpha)),$$

where χ_i is a representative of C_i, and N_i is the norm from $\mathbf{Q}(\chi_i)$ to $\mathbf{Q}$. We observe that $\chi_i(\alpha)$ is an algebraic integer of $\mathbf{Q}(\chi_i)$.

If χ_i has order > 2, then (as there are no real embeddings), $N_i(\chi_i(\alpha)) = 1$. If $ord\ \chi_i \leq 2$, then $N(\chi_i(\alpha)) = \pm 1$, while χ_i is really a character of G/G^2. Thus

$$-1 = \prod_{\chi^2 = \chi_0} \chi(\alpha).$$

Let $\hat{\Gamma} = \{\chi \in \hat{G}; \chi^2 = \chi_0\}$, $\Gamma = \cap_{\chi \in \hat{\Gamma}} ker\ \chi$. Write $\alpha = \sum_{g \in G} c_g g$, and consider the following. Let $h \in G$; we have

$$\sum_{\chi \in \hat{\Gamma}} \chi(h^{-1})\chi(\alpha) = \sum_{\chi \in \hat{\Gamma}} \chi(h^{-1}) \sum_{g \in G} c_g \chi(g) = \#\hat{\Gamma} \sum_{g \in \Gamma_h} c_g.$$

If $\sum_{g \in \Gamma_h} c_g = 0$, $\forall h \in G$, we deduce $\sum_{g \in G} c_g = 0$ which implies $\chi_0(\alpha) = 0$, giving a contradiction. Hence $\exists h \in G$ such that $|\sum_{\chi \in \hat{\Gamma}} \chi(h^{-1})\chi(\alpha)| \geq \#\hat{\Gamma}$. But $\chi(h^{-1})$ and $\chi(\alpha)$ are $\pm 1, \forall \chi \in \hat{\Gamma}$, so the Triangle Inequality shows that $\mathcal{E} = \chi(h^{-1})\chi(\alpha)$ is independent of $\chi \in \hat{\Gamma}$. We now have

$$-1 = \prod_{\chi \in \hat{\Gamma}} \chi(\alpha) = \prod_{\chi \in \hat{\Gamma}} \mathcal{E}\chi(h) = \mathcal{E}^{\#\hat{\Gamma}} \prod_{\chi \in \hat{\Gamma}} \chi(h).$$

But $\#\Gamma$ is even so $\mathcal{E}^{\#\Gamma} = 1$, and $-1 = \prod_{\chi \in \hat{\Gamma}} \chi(h) = det_G h \square$

It is in fact possible to generalise the above result so that the hypothesis G abelian is unnecessary, but this requires more complicated analysis using irreducible representations of G over the algebraic closure of $\mathbf{Q}$.

APPENDIX C

Applications of a theorem by Kummer – Dedekind – Zolatarev to Cyclotomic fields

Suppose $K = \mathbf{Q}(\alpha)$, $0 \neq \alpha \in \mathbf{Z}_K$ (the integral closure of $\mathbf{Z}$ in K). Let $\phi(x)$ be the minimum polynomial of α over $\mathbf{Q}$, which is monic in $\mathbf{Z}[x]$ and irreducible of degree $n = [K : \mathbf{Q}]$. Let $R = \mathbf{Z}[\alpha]$. It is a fact that then $[\mathbf{Z}_K : R] = d < \infty$, for some $d \in \mathbf{N}$.

Let $p \in \mathbf{N}$ be prime, $p \not| d$. Suppose that in $\mathbf{F}_p[x]$, we have

$$\overline{\phi}(x) = \prod_{i=1}^{g} \overline{\phi_i}(x)^{e_i},$$

where $\overline{\phi_i}(x)$ are distinct monic irreducibles, with $deg\ \overline{\phi_i}(x) = f_i$.

In $\mathbf{Z}_K$, let $\wp_i = (p, \phi_i(\alpha))$, where $\phi_i(x) \in \mathbf{Z}[x]$ is any such that $\phi_i(x)\ (mod\ p\mathbf{Z}[x]) = \overline{\phi_i}(x)$.

We then have the following well known theorem (see e.g. [4]):

THEOREM A6

(i) $\wp_1, \ldots, \wp_g$ *are distinct prime ideals in* $\mathbf{Z}_K$,

(ii) $p\mathbf{Z}_K = \prod_{i=1}^{g} \wp_i{}^{e_i}$, *and* $N(\wp_i) = p^{f_i}$.

Applications

LEMMA A7 *If* $K = \mathbf{Q}(e^{2\pi i/n})$, $p \not| n$ *then* $p\mathbf{Z}_K = \wp_1 \ldots, \wp_g$ *where* $g = \frac{\phi(n)}{f}$, $f =$ *the order of* p *in* $(\mathbf{Z}/n\mathbf{Z})^*$, *the group of units mod* n.

Proof $[K : \mathbf{Q}] = \phi(n)$ (=the number of primitive n^{th} roots of unity). Denote $e^{2\pi i/n}$ by ζ_n. Take $\alpha = \zeta_n$, then it is a fact that $\mathbf{Z}[\alpha] = \mathbf{Z}_K \Rightarrow d = 1$. The minimum polynomial of α over $\mathbf{Q}$ is

$$\phi(x) = \Phi_n(x)\ (\text{the } n^{th} \text{ cyclotomic polynomial}) = \prod_{(a,n)=1} (x - \zeta_n{}^a), \quad 1 \leq a < n.$$

We have $p \not| n \Rightarrow x^n - 1$ is separable over $\mathbf{F}_p$. Therefore we seek normal extensions of $\mathbf{F}_p$ which contain all n^{th} roots of 1. It must be ${\mathbf{F}_q}^*$ where $q = p^f$, with $[\mathbf{F}_q : \mathbf{F}_p] = f$. ${\mathbf{F}_q}^*$ is cyclic, order $= q-1$. So $\exists \alpha \in {\mathbf{F}_q}^*$ a zero of $x^n - 1$ (and so of order n) iff $n \mid q-1 \iff q \equiv 1 \ (mod\ n) \iff p^f \equiv 1 \ (mod\ n) \iff$ $f \equiv 0$ (mod the order of p in $G = (\mathbf{Z}/n\mathbf{Z})^*$). Take $f =$ the order of p in G. Then $\mathbf{F}_q$ is a normal extension. Hence, $x^n - 1$ splits in $\mathbf{F}_q$ with the f above and is $\mathbf{F}_p[x]$, $x^n - 1$ is a product of distinct monic irreducibles of degree f ,so there are $\frac{\phi(n)}{f}$ of them$\square$

LEMMA A8 *Suppose* $K = \mathbf{Q}(e^{2\pi i/n})$, $p \mid n$ - *i.e.* $n = p^s k$, $p \not| k$. *Then* $p\mathbf{Z}_K = (\wp_1 \ldots \wp_g)^e$ *where* $g = \frac{\phi(k)}{f}$, *and* $N\wp_i = p^f$ *where* $e = \phi(p^s)$, $f =$ *order of* p *in* $(\mathbf{Z}/k\mathbf{Z})^*$.

Proof In $\mathbf{F}_p$, $\overline{x^n - 1} = \overline{(x^k - 1)^{p^s}}$. So we need only consider the splitting field for $x^k - 1$. Hence, as in Lemma A6, for $x^k - 1$, all the roots lie in $\mathbf{F}_q^* \iff p^f \equiv 1 \ (mod\ k)$. Take $f =$ order of p in $(\mathbf{Z}/k\mathbf{Z})^*$. Then $p\mathbf{Z}_K = (\wp_1 \ldots \wp_g)^e$, where $g = \frac{\phi(k)}{f}$, $N\wp_i = p^f$; and e is some exponent which satisfies (on taking norms of both sides), $\phi(n) = e.g.f$ - so $e = \frac{\phi(n)}{\phi(k)} = \phi(p^s)\square$

COROLLARY A9 *In Lemma A8 take* $k = 1$. *Then* p *ramifies totally in* $\mathbf{Z}_K$.

Proof We have $f = 1$, $\phi(k) = 1 \Rightarrow g = 1 \Rightarrow p\mathbf{Z}_K = \wp^{\phi(p^s)}\square$

Relationships between Relative Norms and Absolute Norms

Let K be a finite extension of $\mathbf{Q}$, the field of rational numbers, so $[K : \mathbf{Q}] = n < \infty$. Then for $\alpha \in K$, $L_\alpha : x \mapsto \alpha x$ is a $\mathbf{Q}$-linear transformation $K \to K$, Define $N_{K/\mathbf{Q}}(\alpha) = \det(L_\alpha)$.

LEMMA A10 *Let* $0 \neq \alpha \in \mathbf{Z}_K$. *Then* $N(\alpha\mathbf{Z}_K) = |N_{K/\mathbf{Q}}(\alpha)|$.

Proof We give below a demonstration which generalises easily. For a quicker proof, see e.g. Stuart & Tall [14] which proceeds by showing:

(a) Every non-zero ideal α of $\mathbf{Z}_K$ has a $\mathbf{Z}$-basis$\{\omega_1, \ldots, \omega_n\}$;

(b) $N(\alpha \mathbf{Z}_K) = \left| \frac{\Delta[\omega_1, \ldots, \omega_n]}{\Delta} \right|^{\frac{1}{2}}$ where Δ is the discriminant.

(c) $\{\alpha\omega_1, \ldots, \alpha\omega_n\}$ is a $\mathbf{Z}$-basis; now substitute in (b).

We assume (a) and now proceed differently from (b) and (c). Thus assume $\omega_1, \ldots, \omega_n$ is a $\mathbf{Z}$-basis of $\mathbf{Z}_K$. If the ω_i's can be chosen so that $d_1\omega_1, \ldots, d_n\omega_n$ form a $\mathbf{Z}$-basis for $\alpha\mathbf{Z}_K$ ($d_i \in \mathbf{N}$; $i = 1, \ldots, n$), then

$$\mathbf{Z}_K/\alpha\mathbf{Z}_K \underset{\mathbf{Z}}{\cong} \mathbf{Z}/d_1\mathbf{Z} \bigoplus \ldots \bigoplus \mathbf{Z}/d_n\mathbf{Z}.$$

Hence $N(\alpha\mathbf{Z}_K) = d_1 d_2 \ldots d_n$.

So we look for a diagonal matrix (with diagonal entries $d_1, \ldots, d_n$) to represent L_α. The method is as follows.

Let $\zeta_1, \ldots, \zeta_n$ be any $\mathbf{Z}$-basis for $\mathbf{Z}_K$. Then $\alpha\zeta_1, \ldots, \alpha\zeta_n$ is a $\mathbf{Z}$-basis for $\mathbf{Z}_K$. Suppose $\underline{\underline{L_\alpha}} := (a_{ij})$, where $\alpha\zeta_i = \sum_{j=1}^{n}(a_{ij})\zeta_j$, $i = 1, \ldots, n$. We look for linear transformations on $\underline{\underline{L_\alpha}}$ which preserve $\det(L_\alpha)$. Suppose $\omega_1, \ldots, \omega_n$ is another $\mathbf{Z}$-basis for $\mathbf{Z}_K$.

Then

$$\begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = \underline{\underline{W}} \begin{pmatrix} \zeta_1 \\ \vdots \\ \zeta_n \end{pmatrix} \text{ where } \underline{\underline{W}} \in M_n(\mathbf{Z}).$$

Also

$$\begin{pmatrix} \zeta_1 \\ \vdots \\ \zeta_n \end{pmatrix} = \underline{\underline{Z}} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Hence,

$$\begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = \underline{\underline{W}}\,\underline{\underline{Z}} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

It follows that $\underline{\underline{W}}\,\underline{\underline{Z}} = \underline{\underline{I}}_n$ whence $\det \underline{\underline{W}} \det \underline{\underline{Z}} = 1$, where $\det \underline{\underline{W}}, \det \underline{\underline{Z}} \in \mathbf{Z}$. Hence $\det \underline{\underline{W}} = \pm 1$, i.e. $\underline{\underline{W}}$ is unimodular. This is thus a necessary condition for preserving $\mathbf{Z}$-bases of $\mathbf{Z}_K$.

Conversely, if $\underline{\underline{H}} \in M_n(\mathbf{Z})$ and $\det \underline{\underline{H}} = \pm 1$ then $\underline{\underline{H}}(adj\ \underline{\underline{H}}) = (\det \underline{\underline{H}})\underline{\underline{I}}_n$ where $adj\ \underline{\underline{H}}$ denotes the adjoint matrix of $\underline{\underline{H}}$; here, $adj\ \underline{\underline{H}} \in M_n(\mathbf{Z})$. Hence $|\det \underline{\underline{H}}| = |\det(adj\ \underline{\underline{H}})| = 1$. So $\underline{\underline{H}}$ is non-singular and hence $\underline{\underline{W}} = \underline{\underline{H}}(\underline{\zeta})^T$ is a $\mathbf{Z}$-basis for $\mathbf{Z}_K$ and $\det(\underline{\underline{L_\alpha}}\ \underline{\underline{H}}) = \det \underline{\underline{L_\alpha}}$.

We seek a new $\mathbf{Z}$-basis of $\mathbf{Z}_K$ such that the matrix $\underline{\underline{L_\alpha}}$ becomes diagonal; in fact, a triangular matrix with $d_1, d_2, \ldots, d_n$ as entries along the diagonal suffices. To achieve this, we use repeated multiplication (on the left or right) by unimodular matrices. So the problem remaining is to find unimodular $\underline{\underline{U}}, \underline{\underline{V}}$ such that $\underline{\underline{U}}\ \underline{\underline{L_\alpha}}\ \underline{\underline{V}} = \underline{\underline{D}}$ where $\underline{\underline{D}}$ is a triangular matrix with diagonal entries $d_1.d_2, \ldots, d_n$. The procedure is as follows.

We have

$$\underline{\underline{L_\alpha}} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} \text{ WLOG } a_{11} \neq 0.$$

Algorithm

Let $k = 1$, let $c = 1$; let $\underline{\underline{A}} = (a'_{i,j}) := \underline{\underline{L_\alpha}}$.

We now apply Euclid's algorithm:

(1) For $m = k+1, \ldots, n$ let $a'_{m,k} := q_m a'_{k,k} + r_{m,1}$, where $0 \leq r_{m,1} < |a'_{k,k}|$; let Row m:=Row m $-$ $q_m \times$(Row k). (These operations just add multiples of one row to another, so the determinant of the revised matrix is preserved, and thus these operations may be represented by unimodular transformations on $\underline{\underline{A}}$ and hence on $\underline{\underline{L_\alpha}}$. Hence column k becomes

$$\begin{pmatrix} a'_{k,k} \\ r_{2,k} \\ \vdots \\ r_{n,k} \end{pmatrix}, \text{ with } r_{m,k} < |a'_{k,k}|.$$

(2) Now suppose $r_{j,k} = \min\{r_{k+1,k}, r_{k+2,k}, \ldots, r_{n,k}\}$ (some j). Swap rows k and j, and put $a^{(c+1)}_{k,k} = r_{j,k}$.

(3) Label the entries of the new matrix $a'_{i,j}$ (for $i, j = k, \ldots, n$).

(4) Let $c := c + 1$.

(5) Repeat steps (1) to (4) inclusive until we have

$$\underline{\underline{A}}\ (\text{col } k) = \begin{pmatrix} a'_{1,k} \\ a'_{2,k} \\ \vdots \\ a'_{k,k} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

(This will happen after a finite number of steps because we have the monotonic decreasing sequence of natural numbers $a^{(1)}_{k,k} > a^{(2)}_{k,k} > \ldots$.)

(6) Let $d_k = a'_{k,k}$. Label the (k, k) entry of $\underline{\underline{A}}\ d_k$. (After one iteration of the main algorithm, we have

$$\underline{\underline{A}} = \begin{pmatrix} d_1 & a'_{1,2} & a'_{1,3} & \ldots & a'_{1,n} \\ 0 & a'_{2,2} & a'_{2,3} & \ldots & a'_{2,n} \\ 0 & a'_{3,2} & . & \ldots & . \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a'_{n,2} & . & \ldots & a'_{n,n} \end{pmatrix}.$$

(7) If $k = n$ then

$$\underline{\underline{A}} = \begin{pmatrix} d_1 & a_{1,2} & a_{1,3} & \ldots & a_{1,2} \\ 0 & d_2 & a_{2,3} & \ldots & a_{2,n} \\ 0 & 0 & d_3 & \ldots & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & ..0 & d_n \end{pmatrix},$$

which is triangular as required, and the $\mathbf{Z}$-basis for $\alpha \mathbf{Z}_K$ is

$$\begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = \underline{\underline{A}} \begin{pmatrix} \zeta_1 \\ \vdots \\ \zeta_n \end{pmatrix}.$$

So we stop here.

If $k \neq n$ then let $k := k + 1$ and proceed now from (1).

Now suppose $r \in \mathbf{Z}G$, where G is a finite abelian group, and let $L_r : \mathbf{Q}G \to \mathbf{Q}G$ be $\mathbf{Q}$-linear $\mathbf{Q}G \to \mathbf{Q}G$. Suppose $A = \bigoplus_{j\in J} K_j \cong_{\mathbf{Q}} \mathbf{Q}G$; Let $S = \bigoplus_{j\in J} \mathbf{Z}_j$ (see §1, Chapter 2 for construction of A). Then we have:

LEMMA A11 $|\det L_r| = N(rS)$.

Proof For each $j \in J$, we may construct a $\mathbf{Z}$-basis for $\mathbf{Z}_j$: $\omega_1^{(j)}, \ldots, w_{n_j}^{(j)}$, where $n_j = [K_j : \mathbf{Q}]$. So for a basis for S we may choose a direct sum of $\mathbf{Z}$-bases,

$$\omega_1^{(1)}, \ldots, \omega_{n_1}^{(1)} \bigoplus \omega_1^{(2)}, \ldots, \omega_{n_2}^{(2)} \bigoplus \cdots \bigoplus \omega_1^{(N)}, \ldots, \omega_{n_N}^{(N)},$$

where $\sum_{j=1}^{N} n_j = n$, the order of G. Hence S may be regarded as a $\mathbf{Z}$-module of dimension n, with $\mathbf{Z}$-basis $\omega_1^{(1)}, \ldots, \omega_{n_1}^{(1)}, \omega_1^{(2)}, \ldots, \omega_{n_2}^{(2)}, \ldots, \omega_1^{(N)}, \ldots, \omega_{n_N}^{(N)}$. Thus it follows that if $r \in \mathbf{Z}G$, then $r\omega_1^{(1)}, \ldots, r\omega_{n_N}^{(N)}$ is a $\mathbf{Z}$-basis for rS. We may now proceed as in Lemma A10$\square$

Index of Notation

$\mathbf{C}$ = the set of complex numbers
$\mathbf{N}$ = the set of natural numbers (1,2,...)
$\mathbf{Q}$ = the set of rational numbers
$\mathbf{R}$ = the set of real numbers
$\mathbf{Z}$ = the set of integers
$\mathbf{F}_p$ = field with p elements

References

[1] I.N.Herstein: *Topics in algebra*, Wiley, 2^{nd} edition (1975).

[2] K.Ireland & M.Rosen: *A classical introduction to modern number theory*, Springer-Verlag, 2^{nd} edition (1990).

[3] S.Lang: *Algebraic number theory*, Addison-Wesley, Reading, Mass. (1970).

[4] W.Narkiewicz: *Elementary and analytic theory of numbers*, Polish Scientific Publishers, Warsaw (1973).

[5] M.Newman: *On a problem suggested by Olga Taussky-Todd* , Illinois J. Maths 24 (1980) pp 156-158.

[6] — *Determinants of circulants of prime power order*, Linear and Multilinear Algebra 9 (1980) pp 187-191.

[7] R.W.K.Odoni: *On norms of integers in a full module of an algebraic number field and the distribution of values of binary integral quadratic forms*, Mathematika 22 (1975) pp 108-111.

[8] — *Some global norm density results obtained from an extended Chebotarev density theorem* in *Algebraic number fields* (ed. A.Frölich), Academic Press (1977) pp 485-495.

[9] — *A new equidistribution property of norms of ideals in given classes*, Acta Arithmetica 33 (1977) pp 53-63.

[10] — *Some remarks on the values taken by abelian group determinants*, Linear and Multilinear Algebra 14 (1983) pp 297-303.

[11] — *Notes on the method of Frobenian functions, with applications to the coefficients of modular forms* in *Elementary and analytic theory of numbers*, Banach Center Publications Vol. 17, Polish Scientific Publishers, Warsaw (1985) pp 371-403.

[12] — *On the distribution of norms of ideals in given ray-classes and the theory of central ray-class fields*, Acta Arith. 52 (1989) pp 373-397.

[13] J.-P.Serre: *Cours d'Arithmétique*, Presses Universitaires de France (1970).

[14] I.N.Stewart & D.O.Tall: *Algebraic number theory*, Chapman and Hall, London,(1979).

[15] O.Taussky-Todd: *Meeting of the American Mathematical Society*, Hayward, California (April 1977).