Lecture Notes in Mathematics 1677

Nikolai Proskurin

Cubic Metaplectic Forms and Theta Functions

Springer

Nikolai Proskurin

Cubic Metaplectic Forms and Theta Functions

Springer

Author

Nikolai Proskurin
St. Petersburg Branch of the Mathematical Institute
Russian Academy of Sciences
Fontanka 27
St. Petersburg 191011, Russia
e-mail: proskn@pdmi.ras.ru

Library of Congress Cataloging-in-Publication Data

Proskurin, Nikolai, 1953-
Cubic metaplectic forms and theta functions / Nikolai Proskurin.
p. cm. -- (Lecture notes in mathematics ; 1677)
Includes bibliographical references and index.
ISBN 3-540-63751-6 (softcover : alk. paper)
1. Automorphic forms. 2. Discontinuous groups. 3. Functions, Theta. I. Title. II. Series: Lecture notes in mathematics (Springer-Verlag) ; 1677.
QA3.L28 no. 1677
[QA243]
510 s--dc21
[512'.7]

Mathematics Subject Classification (1991): Primary: 11F55, 11F60, 11F30
Secondary: 33C10

ISSN 0075-8434
ISBN 3-540-63751-6 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready TEX output by the author
SPIN: 10553411 46/3143-543210 - Printed on acid-free paper

Editorial Policy

§ 1. Lecture Notes aim to report new developments - quickly, informally, and at a high level. The texts should be reasonably self-contained and rounded off. Thus they may, and often will, present not only results of the author but also related work by other people. Furthermore, the manuscripts should provide sufficient motivation, examples and applications. This clearly distinguishes Lecture Notes manuscripts from journal articles which normally are very concise. Articles intended for a journal but too long to be accepted by most journals, usually do not have this "lecture notes" character. For similar reasons it is unusual for Ph. D. theses to be accepted for the Lecture Notes series.

§ 2. Manuscripts or plans for Lecture Notes volumes should be submitted (preferably in duplicate) either to one of the series editors or to Springer- Verlag, Heidelberg . These proposals are then refereed. A final decision concerning publication can only be made on the basis of the complete manuscript, but a preliminary decision can often be based on partial information: a fairly detailed outline describing the planned contents of each chapter, and an indication of the estimated length, a bibliography, and one or two sample chapters - or a first draft of the manuscript. The editors will try to make the preliminary decision as definite as they can on the basis of the available information.

§ 3. Final manuscripts should preferably be in English. They should contain at least 100 pages of scientific text and should include

- a table of contents;
- an informative introduction, perhaps with some historical remarks: it should be accessible to a reader not particularly familiar with the topic treated;
- a subject index: as a rule this is genuinely helpful for the reader.

Further remarks and relevant addresses at the back of this book.

Lecture Notes in Mathematics 1677

Editors:
A. Dold, Heidelberg
F. Takens, Groningen

Springer
Berlin
Heidelberg
New York
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Santa Clara
Singapore
Tokyo

Preface

The subject of these notes does not have a long history. It takes its origin from the very short paper published by Kubota in 1965. Let F be a totally imaginary algebraic number field containing the full group of m^{th} roots of 1, denoted by $\mu_m(F)$, and let $\Gamma^{(n)}_{\text{princ}}(q)$ be the principal congruence subgroup module ideal q in $\mathrm{SL}(n, \mathcal{O}_F)$, $\mathcal{O}_F$ being the integers ring of F. Kubota showed [51] that, under some conditions on q, the reciprocity low yields

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{cases} \left(\frac{c}{d}\right)_m & \text{if } c \neq 0 \\ 1 & \text{if } c = 0 \end{cases}$$

is a group homomorphism $\Gamma^{(2)}_{\text{princ}}(q) \to \mu_m(F)$; here we write $\left(\frac{\cdot}{\cdot}\right)_m$ for the m^{th} degree residue symbol. This theorem has very far-reaching consequences.

In a series of papers [52], [53], ... , [57] Kubota studied automorphic forms under the group $\Gamma^{(2)}_{\text{princ}}(q)$ with the homomorphism above as a multiplier system (= a factor of automorphy), the so called metaplectic forms of degree m. That are real analytic forms, in the sence of Maaß and Selberg, defined on $\mathbf{H}^r$, where $\mathbf{H} \simeq \mathrm{SL}(2, \mathbf{C})/\mathrm{SU}(2)$ is the 3-dimentional hyperbolic space, and r is the number of complex places of F. The metaplectic Eisenstein series are of particular interest. Their Fourier coefficients are the Dirichlet series whose coefficients are the Gauß sums of degree m. The general principles yield then that these Dirichlet series have meromorphic continuations and satisfy some functional equations. This remarkable observation gives the key to solve Kummer problem [37].

Taking the residues of the metaplectic Eisenstein series at some 'exceptional' poles Kubota constructed metaplectic forms which it is reasonable to consider as m^{th} degree analoques of the classical quadratic theta function. In particular, taking $F = \mathbf{Q}(\sqrt{-3})$, $q = (3)$ and $m = 3$, we get the cubic theta function $\Theta_{\text{K-P}}: \mathbf{H} \to \mathbf{C}$. Patterson [69] could find an explicit form for its Fourier expansion. We refer $\Theta_{\text{K-P}}$ as the Kubota–Patterson cubic theta function, it playes a crucial role in these notes. For $m \geq 4$, Fourier coefficients of the m^{th} degree theta functions are not known yet. Some particular results were obtained by

Suzuki [94] and by Eckhardt and Patterson [20] for the biquadratic theta series, i.e., for the case $m = 4$. Patterson considered also the case $m = 6$. It seems reasonable to think that unknown Fourier coefficients of the m^{th} degree theta functions, $m \geq 4$, could be treated as Gauß sums in some extended sence, in this connection see [72], [73].

One more line of thought relates the Kubota homomorphism with the congruence subgroup problem. The relation becames clear if we notice that the kernel of the Kubota homomorphism is the subgroup of finite index in $\mathrm{SL}(2, \mathcal{O}_F)$, and that it does not contain any principle congruence subgroup. To deal with the congruence subgroup problem in more general context, Bass, Milnor and Serre [5] constructed homomorphisms extending Kubota's one.

Due to Bass, Milnor and Serre, we have homomorphisms $\Gamma^{(n)}_{\text{princ}}(q) \to \mu_m(F)$, $n \geq 2$, and we can treat them as multiplier systems to define metaplectic forms on spaces others than that considered originally by Kubota. This is just the point of view accepted by the author in the series of papers [78], ... , [84] and in the present notes.

In other words, the metaplectic forms we define and deal with are 'classical' but not 'adelic' ones. The adelic point of view was accepted by Kubota in [54] and then by Deligne [18], Flicker [27], Kazhdan and Patterson [46], [47], Patterson and Piatetski-Shapiro [74], Flicker and Kazhdan [28]. In this framework metaplectic forms are treated as adelic automorphic forms defined on metaplectic groups.

These notes are organized into three parts.

Part 0 contains essentially known material (except that in subsections 0.3.14 and 0.4.3). Writing Part 0 we had in mind to prepare the necessary background for our research in the forthcoming two parts, and also to gather together the main results concerning the cubic metaplectic forms on $\mathbf{H}$ given by Kubota and by Patterson, which one can find yet in original papers only. The contents of Part 0 is described in details in subsection 0.1.1.

In Part 1 and Part 2 we study cubic metaplectic forms on the symmetric space $\mathbf{X} \simeq \mathrm{SL}(3, \mathbf{C})/\mathrm{SU}(3)$ and, respectively, $\mathbf{X} \simeq \mathrm{Sp}(4, \mathbf{C})/\mathrm{Sp}(4)$. These two parts are independent one from another. For $\mathrm{SL}(3, \mathbf{C})$-case our results are more complete and our exposition is more detailed rather than that for $\mathrm{Sp}(4, \mathbf{C})$-case. In the meantime, Part 1 and Part 2 have entirely similar structure, and this should emphasize the similarity of the methods. In both cases, given a cubic metaplectic form $f\colon \mathbf{H} \to \mathbf{C}$, we have the Eisenstein series $\mathrm{E}(\cdot, s; f)\colon \mathbf{X} \to \mathbf{C}$, $s \in \mathbf{C}$, attached to f in accordance with the general Eisenstein series theory. Our primary goal is to find their Fourier coefficients. For this we apply specific '$sl(2)$-triples technique' developed in [81], [82] and [84]. Then we consider one particular case $f = \Theta_{\text{K-P}}$. The series $\mathrm{E}(\cdot, s; \Theta_{\text{K-P}})$ are very interesting metaplectic forms. We find they have some 'exceptional' poles, and, taking residues, we get cubic theta function Θ on $\mathrm{SL}(3, \mathbf{C})/\mathrm{SU}(3)$ and two cubic theta functions, $\Theta_\natural$ and $\Theta_\sharp$, on $\mathrm{Sp}(4, \mathbf{C})/\mathrm{Sp}(4)$.

The function Θ on $\mathrm{SL}(3, \mathbf{C})/\mathrm{SU}(3)$ has been constructed by the author [78] and by Kazhdan and Patterson [46]. This theta function, as well as $\Theta_{\text{K-P}}$, occurs in [46] as particular representative of a wide class of theta functions defined on metaplectic coverings of the general linear groups. The Fourier coefficients of Θ were evaluated in [78]. The technique used in [78] is not perfect, and this is one reason to review [78] again, in order to simplify and clarify it.

Two cubic theta functions on $\mathrm{Sp}(4,\mathbf{C})/\mathrm{Sp}(4)$, $\Theta_\natural$ and $\Theta_\sharp$ in the notations of these notes, were constructed in [80], [81]. One of them is the residue of the Eisenstein series $\mathrm{E}(\cdot, s; \Theta_{\mathrm{K\text{-}P}})$ at the maximal pole, and it looks like symplectic analogue of the theta functions described in Kazhdan–Patterson theory. The second one, being the residue of $\mathrm{E}(\cdot, s; \Theta_{\mathrm{K\text{-}P}})$ at the second pole, has slightly different origin. For better understanding it would be pleasureable to involve both $\Theta_\natural$ and $\Theta_\sharp$ into general symplectic metaplectic forms theory. We hope our observations might by useful to develope such theory.

It should be pointed out that a lot of things we deal with in first four sections of Part 1 as well as of Part 2 are not related to cubic metaplectic forms and theta functions only. In particular, the basic theorems which give us expressions for the Eisenstein series $\mathrm{E}(\cdot, s; f)$ Fourier coefficients in subsections 1.4.1 and 2.4.1 are valid for the Eisenstein series with almost arbitrary multiplier systems. Among other such things, there is our treatment of Whittaker functions on the group $\mathrm{SL}(3,\mathbf{C})$ in subsections 1.3.10, 1.4.7 and on the group $\mathrm{Sp}(4,\mathbf{C})$ in subsections 2.3.7, 2.4.7. We show that the integrals defining Whittaker functions can be evaluated, that gives rise to simple and useful expressions.

In [84] we studied cubic metaplectic forms on the Lie group $\mathrm{G}_2(\mathbf{C})$ of type G_2. There were found two 'exceptional' poles of the Eisenstein series $\mathrm{E}(\cdot, s; \Theta_{\mathrm{K\text{-}P}})$ on $\mathrm{G}_2(\mathbf{C})$. Unfortunatly there are too many open questions concerning the theta functions associated with these poles. For this reason, we do not include this part of our research into these notes having in mind first to resolve at least some of them and only then to overview the subject.

I would like to thank U. Christian, H. Helling, S. J. Patterson and D. Hejhal for invitations to Göttingen, Bielefeld and Uppsala where I have worked supported by SFB-170, SFB-343 and Uppsala University. This work was supported also by RFFI (grant 96-01-00663). I especially wish to thank S. J. Patterson for his interest to my work and for stimulating encouragement over many years.

Contents

Part 0

0.1 Preliminaries

0.1.1 Suggestions to the reader. 0.1.2 Notations. 0.1.3 Cubic residue symbol. 0.1.4 Arithmetic functions. 0.1.5 Dirichlet series. 0.1.6 Special functions.

0.1.1 Suggestions to the reader. We would like to give some commentary on the present section and the whole Part 0, to save the time and effort of the reader.

In subsection 0.1.2 we have collected some basic notations which will be used throughout these notes. In subsection 0.1.3 we state the properties of the cubic residue symbol. The next two subsections — 0.1.4 and 0.1.5, — contain elementary facts on Gauß and Ramanujan sums, some arithmetic functions, the Dedekind zeta function $\zeta_{\mathbf{Q}(\sqrt{-3})}$ and some cubic Hecke series. We only deal with the field $\mathbf{Q}(\sqrt{-3})$, so prerequisited knowlege of the algebraic number theory is not significant. We hope however the reader feels free with the computations like that in 0.1.4. The most convenient source is the book of Ireland and Rosen [41], where we find detailed description of the arithmetic of the field $\mathbf{Q}(\sqrt{-3})$, including the proof of the cubic reciprocity low. That is all we need except some facts on the Dedekind zeta function and Hecke series for which we can refer to Weil [102]. For reference convenience, we give in subsection 0.1.6 the definitions and some useful facts on special functions — the Euler gamma-function Γ, the Bessel–MacDonald function K_m, the Airy function Ai and the hypergeometric functions ${}_2F_1$ and ${}_3F_2$.

Section 0.2 begins, subsection 0.2.1, with the definitions of some congruence subgroups of $\mathrm{SL}(n, \mathcal{O})$. In the next subsections — 0.2.2,..., 0.2.5 — we present the remarkable Kubota's theorem and its generalization given by Bass, Milnor and Serre. These theorems are of the fundamental importance for us. As to the explicit formulae for the Bass–Milnor–Serre homomorphisms, given in subsection 0.2.5, they are not so important, and we shall not use them.

Section 0.3 is written as a short review of the theory of cubic metaplectic forms on 3-dimensional hyperbolic space $\mathbf{H} = \mathbf{C} \times \mathbf{R}_+^* \simeq \mathrm{SL}(2, \mathbf{C})/\mathrm{SU}(2)$. By the cubic metaplectic forms are understood the automorphic functions with specific multiplier system discovered by Kubota. The material is taken in the main from the works of Kubota [53], [54] and Patterson [69], [70], and includes some new things, particularly in subsection 0.3.14. We give all necessary definitions and statements, but only a few proofs. There is no book on this subject yet, and our operating assumption is that our reader knows somethat the basic concepts of the theory of automorphic functions on complex upper half-plane, including Maaß theory of real analytic automorphic functions. This knowlege would be very helpful for a complete understanding of our exposition. (We can recommend Koblitz [50], Shimura [91], Kubota [58], Venkov [99].) The classical complex upper half-plane is nothing but 2-dimensional hyperbolic space and it can be understood also as $\mathrm{SL}(2,\mathbf{R})/\mathrm{SO}(2)$. It is not a wonder that a lot of things go on $\mathrm{SL}(2,\mathbf{C})/\mathrm{SU}(2)$ quite similar to that on $\mathrm{SL}(2,\mathbf{R})/\mathrm{SO}(2)$. The main difference is that $\mathrm{SL}(2,\mathbf{C})/\mathrm{SU}(2)$ is not a complex analytic manifold, but only a real analytic one. For this reason the automorphic functions one can define on $\mathrm{SL}(2,\mathbf{C})/\mathrm{SU}(2)$ are analogues of the Maaß wave forms, but not of the classical analytic automorphic forms. Certainly, the theory of the automorphic functions on $\mathrm{SL}(2,\mathbf{C})/\mathrm{SU}(2)$ can be viewed as a part of the general automorphic functions theory developed by Selberg [87], [88], Harish-Chandra [32], Langlands [59], Jacquet [43] and others, and such viewpoint leads to better understanding. (We can recommend Baily [2].)

To demonstrate the importance of the cubic metaplectic forms theory for the number theory, we collected in Section 0.4 some of its consequences concerninig the Dirichlet series whose coefficients are the cubic Gauß sums and the squares of the cubic Gauß sums.

0.1.2 Notations. $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ are the ring of rational integers, the field of rational, the field of real and the field of complex numbers; $\mathbf{C}^*$ is the multiplicative group of $\mathbf{C}$; $\mathbf{R}_+^*$ is the multiplicative group of real positive numbers.

$\Re(z)$, $\Im(z)$, $|z|$ are the real part, the imaginary part and the absolute value of $z \in \mathbf{C}$; $\bar{z}$ is the complex conjugate of z and $e(z) = \exp\big(2\pi i(z+\bar{z})\big)$.

For $z \in \mathbf{C} \setminus (-\infty, 0]$ and $s \in \mathbf{C}$ we write z^s for $\exp(s \log z)$, log being the principle logarithm, i.e., $\log z \in \mathbf{R}$ for $z \in \mathbf{R}_+^*$.

${}^t\gamma$ is the matrix transpose to γ, e_n is the identity matrix $n \times n$, and $\mathrm{diag}(c_1, c_2, \ldots, c_n)$ is $n \times n$ diagonal matrix with c_i at the intersection of i^{th} row and i^{th} column.

All integrals we shall deal with are intergals over the standard Lebesgue measures on $\mathbf{R}$ or on $\mathbf{C}$, and it will be easy to distinguish one case from another just from context.

We shall use standard notation $\mathrm{SL}(n,\mathbf{C})$ for the special linear group of order n over $\mathbf{C}$, and $\mathrm{SU}(n)$ for the special unitary groups of order n,

$$\mathrm{SU}(n) = \{k \in \mathrm{SL}(n,\mathbf{C}) \mid k\,{}^t\bar{k} = e_n\}.$$

$\mathrm{Sp}(4,\mathbf{C})$ will denote the symplectic group of rank 2 over $\mathbf{C}$, see 2.1.1 for the definition.

$\mathcal{O} = \mathbf{Z}[\omega]$ is the ring of integers of the field $\mathbf{Q}(\sqrt{-3}\,)$,

$$\omega = \exp(2\pi i/3) = (-1+\sqrt{-3}\,)/2.$$

$\|\cdot\|$: $\mathbf{Q}(\sqrt{-3}) \to \mathbf{Q}$ is the norm, $\|z\| = z\bar{z}$ for all $z \in \mathbf{Q}(\sqrt{-3})$.

By q we mean an ideal of $\mathcal{O}$, also considered as a lattice in $\mathbf{C}$. Then, $\mathbf{C}/q$ is a fundamental domain of the lattice q in $\mathbf{C}$ and $\mathrm{vol}(\mathbf{C}/q)$ is its volume (with respect to the Lebesgue measure on $\mathbf{C}$). We shall assume that $q \subset (3)$ and $q \neq 0$. The fractional ideal dual to q is

$$q^* = \{c \in \mathbf{Q}(\sqrt{-3}) \mid (cd + \overline{cd}) \in \mathbf{Z} \text{ for all } d \in q\}.$$

One can describe q^* also as the set of all $c \in \mathbf{Q}(\sqrt{-3})$ such that $e(cd) = 1$ for all $d \in q$. If $q = (r)$, i.e., q is generated by $r \in \mathcal{O}$, then $\mathrm{vol}(\mathbf{C}/q) = \sqrt{3}\|r\|/2$, and $q^* = (\sqrt{-3}\,r)^{-1}\mathcal{O}$.

Given $l \in \mathcal{O}$ and $A, B \subset \mathcal{O}$, we write lA for the set $\{la \mid a \in A\}$, $l + A$ for the set $\{l + a \mid a \in A\}$, and $A + B$ for the set $\{a + b \mid a \in A,\ b \in B\}$.

We recall [11], [41] that $\mathcal{O}$ is a ring of principal ideals with the Euclidean algorithm and with a unique factorization of the elements into prime factors. Its group of units is $\mathcal{O}^* = \{\zeta \in \mathbf{C}^* \mid \zeta^6 = 1\} = \{\pm 1, \pm\omega, \pm\omega^2\}$. One can represent each element $k \in \mathcal{O}$, $k \neq 0$, uniquely as the product

$$k = \zeta(\sqrt{-3})^m c \tag{0.1.1}$$

with $\zeta \in \mathcal{O}^*$, $m \in \mathbf{Z}$, $m \geq 0$, $c \in \mathcal{O}$, $c \equiv 1 \pmod 3$.

$\mathcal{O}_{\mathrm{ass}}$ is the subset of $\mathcal{O}$ consisting of 0 and of the numbers $k \in \mathcal{O}$ with $\zeta = 1$ in factorization (0.1.1). Sometimes we shall not make a distinction between an ideal of $\mathcal{O}$ and its generator in $\mathcal{O}_{\mathrm{ass}}$. For each prime $p \in \mathcal{O}$, there exists a unique prime $p' \in \mathcal{O}_{\mathrm{ass}}$ which is associated with p. Certainly, $p' \equiv 1 \pmod 3$ or $p' = \sqrt{-3}$. Throughout these notes, by primes in $\mathcal{O}$ we shall mean primes in $\mathcal{O}_{\mathrm{ass}}$ only. With this agreement, for each prime p we have either $p \equiv 1 \pmod 3$ or $p = \sqrt{-3}$, and sometimes we write $p \equiv 1 \pmod 3$ only to exclude from the consideration $\sqrt{-3}$.

As usual, if $a, b \in \mathcal{O}$, $a \neq 0$, then $a \mid b$ denotes that a divides b; $a \nmid b$ denotes that a does not divide b; $a \mid b^\infty$ denotes that $a \mid b^r$ for some rational integer $r \geq 1$.

For $c \in \mathbf{Q}(\sqrt{-3}) \setminus \{0\}$ and prime $p \in \mathcal{O}$ we denote by $\mathrm{ord}_p\, c$ the rational integer t such that $c = p^t ab^{-1}$ with some $a, b \in \mathcal{O}$, $p \nmid ab$. Sometimes we write $p \mid c$ instead of $\mathrm{ord}_p\, c \geq 1$, and $p^t \parallel c$ instead of $\mathrm{ord}_p\, c = t$. We set also $\mathrm{ord}_p\, 0 = \infty$.

We shall use $\mid$ and $\nmid$ also in a little more general context than it is described above. For $a \in \mathcal{O} \setminus \{0\}$ and $b \in \mathbf{Q}(\sqrt{-3})$:

$a \mid b$ means that, for each prime p, if $\mathrm{ord}_p\, a \geq 1$, then $\mathrm{ord}_p\, b \geq \mathrm{ord}_p\, a$;

$a \nmid b$ means that there exists prime p so that $\mathrm{ord}_p\, a \geq 1$, $\mathrm{ord}_p\, b < \mathrm{ord}_p\, a$;

$a \mid b^\infty$ means that, for each prime p, if $\mathrm{ord}_p\, a \geq 1$, then $\mathrm{ord}_p\, b \geq 1$.

Certainly, for $b \in \mathcal{O}$ these definitions coincide with those given before.

For $c_1, \ldots, c_n \in \mathcal{O}$ let $k \in \mathcal{O}_{\mathrm{ass}}$ be so that, for each prime p, $\mathrm{ord}_p\, k = \min\{\mathrm{ord}_p\, c_j \mid j = 1, \ldots, n\}$. We say that k is the greatest common divisor of $c_1, \ldots, c_n$ and denote it as $\gcd(c_1, \ldots, c_n)$. In some cases we have $a, b \in \mathbf{Q}(\sqrt{-3})$ and we have to say that there is no prime $p \in \mathcal{O}$ such that both

$\operatorname{ord}_p a > 0$ and $\operatorname{ord}_p b > 0$. For this we shall write $\gcd(a, b) = 1$. Certainly, this coincides with usual $\gcd(a, b) = 1$ (as defined above), if it so happens that $a, b \in \mathcal{O}$, and thus this will not lead to misunderstanding.

We say that $k \in \mathcal{O} \setminus \{0\}$ is square-free if k is of the form (0.1.1) with $\zeta = \pm 1$, $m = 0, 1$ and $\operatorname{ord}_p c \leq 1$ for all prime $p \equiv 1 \pmod 3$. Eeach $l \in \mathcal{O} \setminus \{0\}$ can be factored as $l = kr^2$ with square-free k, uniquely determined by l, and with $r \in \mathcal{O} \setminus \{0\}$.

We say that $k \in \mathcal{O} \setminus \{0\}$ is cube-free if k is of the form (0.1.1) with $\zeta = 1, \omega, \omega^2$, $m = 0, 1, 2$ and $\operatorname{ord}_p c \leq 2$ for all prime $p \equiv 1 \pmod 3$. Each $l \in \mathcal{O} \setminus \{0\}$ can be factored as $l = kr^3$ with cube-free k, uniquely determined by l, and with $r \in \mathcal{O} \setminus \{0\}$.

We say that $l \in \mathbf{Q}(\sqrt{-3})$ is a cube, or is a cube in $\mathbf{Q}(\sqrt{-3})$, if $l = r^3$ with some $r \in \mathbf{Q}(\sqrt{-3})$. Clearly, if $l \in \mathcal{O}$ is a cube in $\mathbf{Q}(\sqrt{-3})$, then $l = r^3$ with $r \in \mathcal{O}$, and this case we can say l is a cube in $\mathcal{O}$.

Let $c \in \mathcal{O} \setminus \{0\}$. A set $\mathfrak{c}(c) \subset \mathcal{O}$ is said to be a complete residue system $\operatorname{mod} c$ if it contains a unique representative of each residue class $\operatorname{mod} c$. It is said to be a reduced residue system $\operatorname{mod} c$ if it contains a unique representative of each residue class $\operatorname{mod} c$ coprime with c. We shall use script gothic letters to denote residue systems.

For short, we shall write sometimes $a \equiv b\,(c)$ instead of $a \equiv b \pmod c$.

0.1.3 Cubic residue symbol. If $c, d \in \mathcal{O}$, $\gcd(3c, d) = 1$ and $d = \varepsilon p_1^{\omega_1} \ldots p_n^{\omega_n}$ is the canonical factorization into prime factors, $\varepsilon \in \mathcal{O}^*$, then we set

$$\left(\frac{c}{d}\right) = \prod_{1 \leq j \leq n} \left(\frac{c}{p_j}\right)^{\omega_j},$$

where, for prime $p \equiv 1 \pmod 3$, the symbol $\left(\frac{c}{p}\right)$ is equal to $\zeta \in \mathbf{C}^*$ uniquely determined by the conditions

$$\zeta^3 = 1 \quad \text{and} \quad c^{(\tau-1)/3} \equiv \zeta \pmod p \quad \text{with} \quad \tau = \|p\|.$$

(The multiplicative group of the ring $\mathcal{O}/(p)$ has order $\tau - 1$, and it contains the cyclic subgroup of order 3 generated by ω. This yields $c^{\tau-1} \equiv 1 \pmod p$ and $\tau - 1 \equiv 0 \pmod 3$, and so, the ζ required exists.)

The cubic residue symbol $\left(\frac{\cdot}{\cdot}\right)$ has the following properties.

(a) If $a \equiv b\,(d)$, then $\left(\frac{a}{d}\right) = \left(\frac{b}{d}\right)$;

(b) $\left(\frac{c}{ab}\right) = \left(\frac{c}{a}\right)\left(\frac{c}{b}\right)$;

(c) $\left(\frac{ab}{d}\right) = \left(\frac{a}{d}\right)\left(\frac{b}{d}\right)$;

(d) If $c, d \equiv \pm 1\,(3)$, then $\left(\frac{c}{d}\right) = \left(\frac{d}{c}\right)$ (the cubic reciprocity law);

(e) If $\omega = \exp(2\pi i/3)$ and $d = \zeta\big(1 + 3(m + n\omega)\big)$, $\zeta \in \mathcal{O}^*$, $m, n \in \mathbf{Z}$, then

$$\left(\frac{\omega}{d}\right) = \omega^{-m-n}, \quad \left(\frac{\sqrt{-3}}{d}\right) = \omega^{-n}$$

(the supplement to the reciprocity law);

(f) If $a \equiv b\,(c)$ and $a \equiv b\,(9)$, then $\left(\frac{c}{a}\right) = \left(\frac{c}{b}\right)$;

(g) $\left(\frac{\pm 1}{d}\right) = 1$;

(h) If $c, d \in \mathbf{Z}$, then $\left(\frac{c}{d}\right) = 1$.

The cubic resiprocity law (d) and the supplement (e) are known due to Eisenstein [21], [22], [23]. Other points are rather simple. See [41], [34], [17].

Throughout these notes we shall assume that

$$\left(\frac{0}{d}\right) = 1 \qquad \text{for} \quad d \in \mathcal{O}, \quad \gcd(d, 3) = 1,$$

and sometimes we shall write for simplicity

$$\left(\frac{c}{d}\right) \quad \text{instead of} \quad \left(\frac{a}{d}\right)\left(\frac{b}{d}\right)^{-1}$$

if $c = a/b$ with $a, b \in \mathcal{O}$ and $\gcd(ab, d) = 1$. We hope, there will not be misunderstandings, though these agreements are not commonly used.

We shall use the residue symbol very often. At first we shall try to point out explicitly which of formulae (a),..., (g) we need, but then, we hope, this will not be necessary.

0.1.4 Arithmetic functions. For $c \in \mathcal{O} \setminus \{0\}$ we define

$$\tilde{\mu}(c) = \begin{cases} (-1)^l & \text{if } c \text{ is square-free with } l \text{ prime divisors,} \\ 0 & \text{if } c \text{ is not square-free} \end{cases} \qquad \text{(Möbius function),}$$

$$\tilde{\varphi}(c) = \sum_{k \in \mathfrak{c}(c)} 1 \qquad \text{(Euler's totient function),} \tag{0.1.2}$$

where $\mathfrak{c}(c)$ is a reduced residue system $\bmod c$. We have used ~ in the notations to emphasize the functions above are attached to the ring $\mathcal{O}$ (but not to $\mathbf{Z}$), and to save the letters μ, φ for other purposes.

One says that a function $f\colon \Omega \to \mathbf{C}$, Ω being a subset of $\mathcal{O}$, is multiplicative if $ab \in \Omega$ and $f(ab) = f(a)f(b)$ for all $a, b \in \Omega$ with $\gcd(a,b) = 1$. One can easily find the functions defined in (0.1.2) are multiplicative.

For $\lambda \in q^*$, $q \subset (3)$, $c \in 1+q$ let us write

$$\begin{aligned} C(\lambda, c) &= \sum_{k \in \mathfrak{c}(c)} e(\lambda k/c) \quad \text{(Ramanujan sum)}, \\ S(\lambda, c) &= \sum_{k \in \mathfrak{c}(c)} \left(\frac{k}{c}\right) e(\lambda k/c) \quad \text{(Gauß sum)}, \end{aligned} \tag{0.1.3}$$

where $\mathfrak{c}(c)$ is a reduced residue system $\bmod c$, which we can, have and do assume to be a subset of q. Next, if $c' \in \mathcal{O}$ can be represented in the form ld^3 with $l \mid c^\infty$, $\gcd(d,3) = 1$, $l, d \in \mathcal{O}$, then we set

$$S(\lambda, c, c') = \sum_{k \in \mathfrak{c}(c,c')} \left(\frac{k}{c}\right)\left(\frac{k}{c'}\right) e(\lambda k/c) \quad \text{(Gauß sum)}, \tag{0.1.4}$$

where $\mathfrak{c}(c,c') \subset q$ is a reduced residue system $\bmod c$ composed of numbers coprime with c'. Notice that $S(\lambda, 1, c') = 1$ if $c' = d^3$ with some $d \in \mathcal{O}$, $\gcd(d,3) = 1$, and that $S(\lambda, 1, c')$ is not defined for other c'. For λ, q as above and $c \in q$ we set

$$S_*(\lambda, c) = \sum_{\substack{k \in \mathfrak{c}(cq) \\ k \equiv 1(3)}} \left(\frac{c}{k}\right) e(\lambda k/c) \quad \text{(Gauß sum)}, \tag{0.1.5}$$

where $\mathfrak{c}(cq)$ is a reduced residue system $\bmod cq$.

Notice that the terms in all the sums in (0.1.3), (0.1.4), (0.1.5) do not depend on the choice of reduced residue systems involved in their definitions. The sums $S_*(\lambda, c)$ depend essentially on the ideal q involved. The sums in (0.1.3), (0.1.4) do not depend on q in a sense that whichever the ideal q with the properties $q \subset (3)$, $\lambda \in q^*$, $c \in 1+q$ is considered in their definitions, for given λ and c these sums are the same. One says λ to be a parameter and c to be a module of the sums (0.1.3), (0.1.4), (0.1.5), while c' should be considered as a supplementary module of the sum (0.1.4).

All the sums in (0.1.2), (0.1.3) are the sums of type (0.1.4). In fact we have

$$S(\lambda, c, c') = \begin{cases} S(\lambda, c) & \text{if } c' \text{ is a cube}, \\ C(\lambda, c) & \text{if } cc' \text{ is a cube}, \\ \tilde{\varphi}(c) & \text{if } cc' \text{ is a cube and } \lambda = 0. \end{cases} \tag{0.1.6}$$

Here are some elementary properties of the sums above:

(a) $\tilde{\varphi}(c) = \|c\| \prod_{\substack{p \mid c \\ p \text{ is prime}}} \left(1 - \frac{1}{\|p\|}\right);$

(b) $S(0,c) = \begin{cases} \tilde{\varphi}(c) & \text{if } c \text{ is a cube,} \\ 0 & \text{otherwise;} \end{cases}$

(c) $C(\lambda, c_1 c_2) = C(\lambda, c_1) C(\lambda, c_2)$ if $\gcd(c_1, c_2) = 1$;

(d) $C(\delta\lambda, c) = C(\lambda, c)$ if $\delta \in \mathcal{O}$, $\gcd(\delta, c) = 1$;

(e) For prime $p \equiv 1\,(3)$ one has $C(p^\varepsilon, p^\alpha) = \begin{cases} \tilde{\varphi}(p^\alpha) & \text{if } \alpha \le \varepsilon, \\ -\|p\|^{\alpha-1} & \text{if } \alpha = \varepsilon + 1, \\ 0 & \text{if } \alpha \ge \varepsilon + 2; \end{cases}$

(f) $|S(1,c)|^2 = \begin{cases} \|c\| & \text{if } c \text{ is square-free,} \\ 0 & \text{otherwise;} \end{cases}$

(g) $S(\lambda, c_1 c_2, c_1' c_2') = \left(\frac{c_1}{c_2 c_2'}\right)\left(\frac{c_2}{c_1 c_1'}\right) S(\lambda, c_1, c_1') S(\lambda, c_2, c_2')$
if $\gcd(c_1 c_1', c_2 c_2') = 1$;

(h) For prime $p \equiv 1\,(3)$, if $\delta = \operatorname{ord}_p \lambda$ and $\lambda' = \lambda p^{-\delta}$, then

$$S(\lambda, p^\alpha, p^\beta) = \begin{cases} 1 & \text{if } \alpha = 0,\ \beta \equiv 0(3), \\ \tilde{\varphi}(p^\alpha) & \text{if } 1 \le \alpha \le \delta,\ \alpha + \beta \equiv 0(3), \\ -\|p\|^\delta & \text{if } \alpha = \delta + 1,\ \alpha + \beta \equiv 0(3), \\ \|p\|^\delta S(\lambda', p) & \text{if } \alpha = \delta + 1,\ \alpha + \beta \equiv 1(3), \\ \|p\|^\delta \overline{S(\lambda', p)} & \text{if } \alpha = \delta + 1,\ \alpha + \beta \equiv 2(3), \\ 0 & \text{in all other cases;}^\dagger \end{cases}$$

(i) $S(\lambda, c, c') \ne 0$ if and only if for each prime $p \equiv 1\,(3)$ one has either $\operatorname{ord}_p c = \operatorname{ord}_p \lambda + 1$ or $0 \le \operatorname{ord}_p c \le \operatorname{ord}_p \lambda$, $\operatorname{ord}_p c + \operatorname{ord}_p c' \equiv 0\,(3)$;

(j) $S(\delta\lambda, c, c') = \left(\frac{\delta}{cc'}\right)^{-1} S(\lambda, c, c')$ if $\delta \in \mathcal{O}$, $\gcd(\delta, cc') = 1$;

(k) Let $q = (3)$ and $\lambda = \xi(\sqrt{-3})^m \delta$, $c = \varepsilon(\sqrt{-3})^l$ with $\xi, \varepsilon \in \mathcal{O}^*$, $m, l \in \mathbf{Z}$, $m \ge -3$, $l \ge 2$, $\delta \in \mathcal{O}$, $\delta \equiv 1\,(3)$. Then, with $j, k \in \mathbf{Z}$ defined $\bmod 6$ by $\varepsilon\xi^{-1} = \exp(\pi i j/3)$ and $\varepsilon = \exp(-\pi i k/3)$, one has

$$S_*(\lambda, c) = 3^l e\big(\xi\varepsilon^{-1}(\sqrt{-3})^{m-l}\big)\left(\frac{\varepsilon(\sqrt{-3})^l}{\delta}\right)^{-1}$$

if $l - m \le 3$, $k \equiv l \equiv 0\,(3)$, or
$l - m = 4$, $l \equiv k + (-1)^j \equiv 0\,(3)$, or
$l - m = 5$, $l \equiv (-1)^j\,(3)$, $k \equiv (-1)^j j\,(3)$,
and $S_*(\lambda, c) = 0$ for all other j, k, l, m.

---

† Notice however that $S(\lambda, p^\alpha, p^\beta)$ is not defined for $\alpha = 0$, $\beta \not\equiv 0 \pmod 3$.