Hans Opolka

Composite numbers, Galois theory and automorphic forms

Braunschweig : Institut für Analysis und Algebra, 2009

Veröffentlicht: 21.07.2009

http://www.digibib.tu-bs.de/?docid=00028755

COMPOSITE NUMBERS, GALOIS THEORY AND AUTOMORPHIC FORMS

Hans Opolka
TU Braunschweig
Institut für Analysis und Algebra
Pockelsstrasse 14
D - 38106 Braunschweig

e-mail: h.opolka@tu-bs.de

Abstract: It is shown that for every squarefree composite integer d, $d \notin \{0,1\}$, every nontrivial decomposition $d = ab$ yields a set $\mathfrak{R}_{a,b}$ of irreducible 2-dimensional complex representations of the absolute Galois group of the field of rational numbers. Applying the technique of automorphic induction it turns out that every $\rho \in \mathfrak{R}_{a,b}$ corresponds to an automorphic representation $\kappa = \kappa(\rho)$ which for $a, b > 1$ corresponds to a wave form for a certain congruence subgroup of the group of unimodular (2×2)-matrices over the ring of integers.

AMS Classification 2000: 11 F 80, 11 R 34, 11 F 70, 11 F 37

Key words and phrases: Galois theory of number fields, Galois cohomology, automorphic representations, modular forms

§1. Introduction

In this note we show how a square free composite integer $d = ab$, $d \notin \{0,1\}$, gives rise to irreducible 2-dimensional representations of the absolute Galois group of the rational number field $\mathbb{Q}$ and point out that these representations yield automorphic representations which correspond to modular forms for a certain congruence subgroup of the group of all unimodular (2×2)-matrices over the ring of integers $\mathbb{Z}$. The construction is part of the general framework developed in [O]. It makes use of the technique of lifting of projective Galois representations, comp. [$SE1$] ,§6, and of the induction process for automorphic representations as developed in [AC] . The emphasis in the present note is on the lifting of the underlying projective Galois representations in dependence of d. The examples of modular forms which arise in this way include also examples of indefinite modular forms mentioned in [HE] and [HI] , Chapter 3, especially 3.4. If in a nontrivial decomposition $d = ab$ the integers a, b are both > 1 then the mentioned modular forms are so called wave forms with eigenvalue $\frac{1}{4}$ in the sense of H. Maass [M]. For investigations, results and examples related to Maass wave forms, especially to those which arise from Galois theory, comp. [BS] ; [BU] , 1.9, pp. 103 ff; [CKM] , Lecture 2; [CH] ; [FR] ; [HT] ; [KT] ; [$SN1$] ; [$SN2$] ; [V]. We mention that there are also relations between the constructions in the present

paper and $[JL]$. For concepts and results on automorphic forms and representations which are used in the present note we refer to $[AC], [BU], [CM]$ and of course $[L]$. As a basic reference for concepts and results from algebraic number theory, including class field theory, we use $[AT]$ and $[CF]$.

§2. Statement of results

According to a well known result of R. Dedekind and K. Hensel the absolute discriminant of a number field $L/\mathbb{Q}$ of degree n is equal to

$$\prod_p p^{\delta_p}$$

where the product is taken over all prime numbers which are ramified in $L/\mathbb{Q}$ and where

$$\delta_p \leq n - 1 + n\log(n)/\log(p);$$

see $[SE3]$, Chapter III, §6, Remarks. 1), p. 58, as well as $[SE4], §1$, and the literature mentioned there. We follow remarks in $[SE2]$, section 4.1, p. 49, which are based on this result, and define two invariants depending on a given squarefree positive integer d, $d \notin \{0, 1\}$, as follows. For any odd prime divisor p of d denote by 2^{m_p} the maximal 2-power dividing $p-1$ and put $m_2 := 1$. Define

$$g_d := \max\left\{2^{m_p+2} : p \text{ divides } 2d\right\}$$

$$f_d := \prod_{p/2d} p^{[\delta_p]} \text{ where } \delta_p := 2g_d - \tfrac{1}{2} + \tfrac{2g_d\log(4g_d)}{\log(p)}$$

where $[x]$ denotes the largest integer $\leq x$. These invariants g_d and f_d will be used below.

For any number field k with algebraic closure $\overline{k}$ and any finite subextension K/k of $\overline{k}/k$ denote by $G_K = G(\overline{k}/K)$ the absolute Galois group of K. If m is a positive integer then W_m denotes the group of all roots of unity in $\mathbb{C}$ of order dividing m.

Theorem *Assume that $d = ab$ is a nontrivial decomposition. Then there is a set $\mathfrak{R}_{a,b}$ of irreducible 2-dimensional complex Galois representations ρ of the absolute Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}$ whose conductors divide f_d and whose character values belong to the cyclotomic field $\mathbb{Q}(W_{g_d})$. Moreover, every $\rho \in \mathfrak{R}_{a,b}$ is induced by a linear character ψ of G_M where $M/\mathbb{Q}$ is any quadratic subextension of $\mathbb{Q}(\sqrt[2]{a}, \sqrt[2]{b})$.*

For a number field K denote by $\mathbb{A}_K$ the adele ring of K.

Corollary *For every $\rho \in \mathfrak{R}_{a,b}$ there is a cuspidal automorphic representation $\kappa = \kappa(\rho)$ of $GL(2, \mathbb{A}_{\mathbb{Q}})$ such that for every prime number p which is prime to $2d$ the Frobenius conjugacy class ρ_p of ρ at p is equal to the conjugacy class κ_p of the Hecke-matrix of κ at p and such that $\kappa(\rho)$ corresponds to a modular form $\phi = \phi(\rho)$ for the congruence subgroup $\Gamma(f_d)$ of $SL(2, \mathbb{Z})$. For every $\rho \in \mathfrak{R}_{a,b}$ the cuspidal automorphic representation $\kappa(\rho)$ is automorphically induced by a linear character of $GL(1, \mathbb{A}_M)$ where $M/\mathbb{Q}$ is any quadratic subextension of $\mathbb{Q}(\sqrt[2]{a}, \sqrt[2]{b})$. If $a, b > 1$ then for every $\rho \in \mathfrak{R}_{a,b}$ the modular form $\phi(\rho)$ is a wave form for $\Gamma(f_d)$ with eigenvalue $\frac{1}{4}$.*

§3. Construction of Galois representations and associated automorphic representations

Assume that $K = \mathbb{Q}(\sqrt[2]{a}, \sqrt[2]{b})$ is a biquadratic extension with Galois group $G = G(K/\mathbb{Q})$ for which we fix generators s and t such that for fixed square roots $\alpha = \sqrt[2]{a}$, $\beta = \sqrt[2]{b}$

$$s(\alpha) = (-1)^{\lambda_a(s)}\alpha,\ s(\beta) = \beta,\ t(\beta) = (-1)^{\lambda_b(t)}\beta,\ t(\alpha) = \alpha$$

where $\lambda_a : G \to \mathbb{Z}/2\mathbb{Z}$ resp. $\lambda_b : G \to \mathbb{Z}/2\mathbb{Z}$ is the homomorphism corresponding to a resp. b by Kummer theory. Then it is easily shown that the map $c : G \times G \to W_2$ defined by

$$c(u, v) := (-1)^{\lambda_b(v)\lambda_a(u)},\ \ u, v \in G,$$

is a nonsymmetric central 2-cocycle. It follows from a result of R. Frucht that the image of the cocycle class (c) in $H^2(G, \mathbb{C}^*)$ under the homomorphism $H^2(G, W_2) \to H^2(G, \mathbb{C}^*)$ which is induced by the embedding $W_2 \hookrightarrow \mathbb{C}^*$ corresponds uniquely to the isomorphism class of an irreducible projective representation $P : G \to PGL(2, \mathbb{C}^*)$, comp. e.g. $[Y]$, §6, section 6.1, Corollary, p. 183. Since for every number field k the cohomology group $H^2(G_k, \mathbb{C}^*)$ is trivial, see e.g. $[SE1]$, §6, there is an irreducible linear representation $\rho : G_{\mathbb{Q}} \to GL(2, \mathbb{C})$ such that the corresponding projective representation $\overline{\rho} : G_{\mathbb{Q}} \to PGL(2, \mathbb{C})$ is equal to P. With methods which have been applied by the author at several occasions, e.g. in $[O]$, one can show that ρ can be chosen in such a way that the central character $\chi : G_K \to \mathbb{C}^*$ of ρ, which is defined as the unique irreducible constituent of the restriction of ρ to G_K, has order dividing the invariant g_d which was defined in §2 and that χ is unramified outside all places which divide the rational prime divisors of $2d$ and the infinite place. It should be remarked however that this bound for the order of the central character χ of ρ is very rough and can sometimes be improved considerably, e.g. by using results in $[SW]$ on the isotropy of rational ternary quadratic forms over fields of roots of unity of order a suitable power of 2. Especially, if the equation

$$a = X^2 - bY^2$$

has a rational solution $(X, Y) = (x_0, y_0) \neq (0, 0)$, then instead of g_d we can simply take 2. For $a, b > 1$ another improvement comes from the fact that $\mathbb{Q}(\sqrt[2]{a}, \sqrt[2]{b})$ is totally real. One result which is used in proving the claimed bound for the order of the central character for ρ says that the central simple $\mathbb{Q}$- algebra $A(a, b)$ which is defined by the 2-cocycle c is split by the cyclotomic extension which is obtained from $\mathbb{Q}$ by adjoining to $\mathbb{Q}$ a primitive root of unity of order $g_d/2$; this can be seen quite easily by using the local global principle about central simple algebras over number fields and the theory of central simple algebras over local number fields; for the theory of central simple algebras over local and global number fields comp. $[D]$. We mention that this result is also related to $[SW]$, 4.15. From this one deduces that the central embedding problem for $G_{\mathbb{Q}}$ which is defined by the cocycle $c_{2,g_d} : G \times G \xrightarrow{c} W_2 \hookrightarrow W_{g_d}$ has a proper solution which is unramified outside the set of prime divisors of $2d$ and infinity by using results in $[HM]$, especially 2.1, 6.1, and the global duality theorem of Tate and Poitou for which we refer to $[P]$. Having chosen ρ in such a way it follows that the Galois extension $L/\mathbb{Q}$ which corresponds to the kernel of ρ has degree $n = 4g_d$ and that ρ is realizable over the field $\mathbb{Q}(W_{g_d})$. The conductor-discriminant formula, comp. $[SE3]$, Chapter VI, §3, Corollary 2, implies that the square of the conductor $f(\rho)$ of ρ divides the discriminant of $L/\mathbb{Q}$, and therefore by the result of Hensel mentioned at the beginning of §2 the conductor $f(\rho)$ divides f_d. Put

$$\mathfrak{R}_{a,b} := \left\{ \begin{array}{c} \lambda \otimes \rho : \lambda : G_{\mathbb{Q}} \to W_{g_d} \text{ any continuous character} \\ \text{such that } f(\lambda \otimes \rho) \text{ divides } f_d \end{array} \right\}.$$

Clifford´s Theory $[CL]$ implies that if $M/\mathbb{Q}$ is any quadratic subextension of $K/\mathbb{Q}$ then for every $\rho \in \mathfrak{R}_{a,b}$ there is a linear character ψ of G_M such that ρ is isomorphic to the representation which is induced by ψ:

$$\rho \cong Ind_{G_M}^{G_{\mathbb{Q}}}(\psi).$$

Denote by $\kappa(\psi)$ the representation of $GL(1, \mathbb{A}_M)$ (Hecke character) corresponding to ψ by the Artin reciprocity homomorphism $\mathbb{A}_M^*/M^* \to G_M^{ab}$, where G_M^{ab} denotes the Galois group of the maximal abelian extension of M, and let

$$\kappa(\rho) := AutInd_{GL(1,\mathbb{A}_M)}^{GL(2,\mathbb{A}_Q)}(\kappa(\psi))$$

denote the automorphically induced representation of $GL(2, \mathbb{A}_{\mathbb{Q}})$ in the sense of $[AC]$, Chapter 3, sections 6 and 7. $\kappa(\rho)$ is cuspidal, comp. $[AC]$, Chapter 3, section 7. It should be noted that the process of automorphic induction developed by J. Arthur and L. Clozel in $[AC]$ is very profound, involved and powerful and can be applied in much more general situations. It is well known, see e.g. $[CM]$ and $[V]$ that $\kappa(\rho)$ corresponds to a modular form $\phi(\rho)$.

§4. The case of wave forms

The following description of the connection between 2-dimensional Galois representations of $G_{\mathbb{Q}}$ and wave forms is taken from [$SN1$], §1 and Appendix 1, and from [V] , section 3. Let $\rho : G_{\mathbb{Q}} \to GL(2, \mathbb{C})$ be an irreducible Galois representation with conductor f. For any prime number p which is unramified for ρ, i.e. which does not divide f, denote by $s_p \in G_{\mathbb{Q}}$ a Frobenius automorphism and put $\rho_p := \rho(s_p)$. Following E. Artin one defines, comp. [HL],

$L(s, \rho) := \prod_{p \nmid f} \det(Id - \rho_p p^{-s})$, $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$,

where Id denotes the identity matrix of degree 2. This product can be written as a Dirichlet series

$L(s, \rho) = \sum_{n=1}^{\infty} a_\rho(n) n^{-s}, s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$.

If $s_\infty \in G_{\mathbb{Q}}$ is the Frobenius substitution at infinity, i.e. s_∞ corresponds to the complex conjugation automorphism, put $\rho_\infty := \rho(s_\infty)$. We assume that ρ is even, i.e. that ρ_∞ is a scalar matrix, and define $\alpha \in \{0, 1\}$ by

$\rho_\infty := (-1)^\alpha . Id.$

If one assumes that all the L-series $L(s, \lambda \otimes \rho)$, where λ any linear character of $G_{\mathbb{Q}}$, are entire, then the complex valued function $\phi : \mathcal{H} \to \mathbb{C}$ on the upper half plane $\mathcal{H} := \{z := x + iy \in \mathbb{C} : y > 0\}$ which is defined by

$\phi(z) := \phi(x, y) :=$

$:= \sqrt[2]{y} \cdot \sum_{n \in \mathbb{Z}, n \neq 0} a_\rho(|n|) sign(n))^\alpha K_0(2\pi |n| y) e^{2\pi i n x}$, $z = x + iy \in \mathcal{H}$

where

$K_0(x) := \int_0^\infty (1 + t^2)^{-1/2} \cos(xt) dt$, $x \in \mathbb{R}$, $x > 0$,

is a wave form for $\Gamma(f)$ with eigenvalue $\frac{1}{4}$, i.e. it satifies the following three conditions (i),(ii),(iii):

(i) $\Delta\phi = -\frac{1}{4}\phi$

where

$\Delta := y^2(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2})$

is the Laplace operator on the upper half plane $\mathcal{H}$

(ii) $\int_{\Gamma(f)\backslash\mathcal{H}} |\phi(z)|^2 \, dA(z) < \infty$ where $dA(z) := \frac{dxdy}{y^2}$

(iii) $\phi(\gamma z) = \phi(z)$ for all $\gamma \in \Gamma(f)$,

where $\Gamma(f)$ denotes the principal congruence subgroup modulo f of $SL(2,\mathbb{Z})$.

If $d = ab$ is a nontrivial decomposition such that $a, b > 1$ then the extension $\mathbb{Q}(\sqrt[2]{a}, \sqrt[2]{b})/\mathbb{Q}$ is totally real and therefore for every representation $\rho \in \mathfrak{R}_{a,b}$ the matrix ρ_∞ is a scalar matrix. Moreover, since every ρ is induced by a onedimensional character all the Artin L-series $L(s, \lambda \otimes \rho)$, $\lambda \in Hom(G_{\mathbb{Q}}, \mathbb{C}^*)$, are entire. Hence in this case for every $\rho \in \mathfrak{R}_{a,b}$ the modular form $\phi(\rho)$ is a wave form for $\Gamma(f_d)$ with eigenvalue $\frac{1}{4}$.

References

[AC] J. Arthur, L. Clozel: Simple algebras, base change and the advanced theory of the trace formula, Annals of Mathematics Studies, 120, Princeton University Press, New Jersey, 1989

[AT] E. Artin, J. Tate: Class field theory, Addison Wesley, 1990

[BS] A. R. Booker, A. Strömbergsson: Numerical computations with the trace formula and the Selberg eigenvalue conjecture, JRAM, 607, 2007, 113-161

[BU] D. Bump: Automorphic functions and representations, Cambridge Studies in Advanced Mathematics, 55, Cambridge University Press, Cambridge, 1997

[CM] W. Casselmann: On some results of Atkin-Lehner, Mathematische Annalen, 201, 1973, 301-314

[CL] A.H. Clifford: Representations induced in an invariant subgroup, Annals of Mathematics, 38, 1937, 533-550

[CKM] J.W. Cogdell, H.H. Kim, M. Ram Murty: Lectures on automorphic L-functions, Fields Institute Monographs, 20, AMS, Prividence Rhode Island, 2004

[CF] J.W.S. Cassels, A. Fröhlich (eds.): Algebraic Number Theory, Academic Press, New York, 1967

[CH] H. Cohen: q-identities for Maass wave forms, Inventiones Mathematicae, 91, 1988, 409-422

[D] M. Deuring: Algebren, Zweite, korrigierte Auflage, Springer Verlag, Berlin, 1068

[FR] S. Friedberg: On Maass wave forms and the imaginary quadratic Doi Naganuma lifting, Mathematische Annalen, 1983, 483-508

[HE] E. Hecke: Über einen Zusammenhang zwischen elliptischen Funktionen und Modulfunktionen, in: Mathematische Werke, Vandenhoeck & Ruprecht, Göttingen, 1959. No. 22, 1925, 418-427

[HI] T. Hiramatsu: Theory of automorphic forms of weight 1, Advanced Studies in Pure Mathematics, 13, 1988, 503-584

[HL] H. Heilbronn: Zeta functions and L-functions, in [CF] , 204-230

[HM] K. Hoechsmann: Zum Einbettungsproblem, JRAM, 229, 1968, 81-106

[HT] N. Hurt: Letter to the author, dated May 31, 2005

[JL] H. Jacquet, R. Langlands: Automorphic forms on $GL(2)$, Lecture notes in mathematics, 114, 1970

[KT] S.I. Kato: A remark on Maass wave forms attached to real quadratic fields, Journal of the Faculty of Science of the University of Tokyo, Section I, Math., 34, 1987, 193-201

[L] R. P. Langlands: Problems in the theory of automorphic forms, in: Lectures in modern analysis and applications, Lecture Notes in Matematics, 170, Springer Verlag, New York, 1970, 18-86

[M] H. Maass: Über eine neue Art von nichtanalytischen automorphen Funktionen und die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, Mathematische Annalen, 121, 1949, 141-183

[O] H. Opolka: Central pairs, Galois theory and automorphic forms, Algebras and Representation Theory, Kluwer Academic Publishers, 6, 2003, 449-459

[P] G. Poitou: Cohomologie galoisienne des modules finis, Dunod, Paris, 1967

[$SN1$] P. Sarnak: Spectra of hyperbolic surfaces, Bulletin of the AMS, 40, 2003, 441-478

[$SN2$] P. Sarnak: Maass cusp forms with integer coefficients; in: A panorama of number theory or the view from Baker's garden, Cambridge University Press, Cambridge, 2002; 121-127

[SW] G. Schwant: Isotropie ternärer quadratischer Formen mit rationalen Koeffizienten, Diplomarbeit, TU Braunschweig, 1995

[$SE1$] J.P. Serre: Modular forms of weight one and Galois representations, in: A. Fröhlich (ed.), Algebraic number fields, Academic Press, New York, 1977, 193-286

[$SE2$] J. P. Serre: Lectures on the Mordell-Weil theorem, Aspects of Mathematics, Vieweg Verlag, Braunschweig, 1997

[$SE3$] J. P. Serre: Local fields, Springer Verlag, New York, 1979

[$SE4$] J.P. Serre: Quelques propriétés du théoreèm de densité de Chebotarev, Publ. Math. I.H.E.S., 54, 1981, 123-202

[V] M. F. Vigneras: Représentations Galoisiennes paires, Glagow Mathematical Journal, 27, 1985, 223-237

[Y] K. Yamazaki: On projective representations and ring extensions of finite groups, Journal of the Faculty of Science of the University of Tokyo, Section I, Math., 10, 1963/64, 147-195

Typeset with Scientific Word and LaTex