CLASS NUMBER RELATIONS FOR SOME SALEM EXTENSIONS

W. DUKE

Abstract. A new class number relation is given between members of a family of sextic Salem extensions and certain quartic number fields.

1. Introduction

Among the early class number relations was one found by Dirichlet [4]. In the language of number fields it states that for $D > 1$ square-free the class number of the field $\mathbb{Q}(\sqrt{-D}, \sqrt{D})$ equals the product of the class numbers of $\mathbb{Q}(\sqrt{-D})$ and $\mathbb{Q}(\sqrt{D})$ or half of this product. Dirichlet's result is a consequence of a simple relation between the Dedekind zeta functions of these fields, the class number formula and the fact that the resulting quotient of regulators (and numbers of roots of unity) can be explicitly computed. This last problem becomes more difficult when seeking relations between the class numbers of number fields of higher degrees. Some basic references on this subject are Hilbert [10], Herglotz [9], Kuroda [11], Hasse [7], Nehrkorn [14], Brauer [3], and Schertz [15].

My object here is give a family of examples of simple new class number relations based on certain sextic Salem extensions.[1] I will show the following. For an integer $a \geq 0$ the polynomial

$$f_6(x) = x^6 - ax^5 - x^4 + (2a-1)x^3 - x^2 - ax + 1 \tag{1.1}$$

is irreducible over $\mathbb{Q}$ and has two positive roots $\epsilon > 1$ and ϵ^{-1}, while the others occur as complex conjugate pairs on the unit circle, say $\epsilon', \overline{\epsilon'}$ and $\epsilon'', \overline{\epsilon''}$. Thus ϵ is a Salem number and the number field $k_6 = \mathbb{Q}(\epsilon)$ is a Salem extension of its subfield $k_3 = \mathbb{Q}(\alpha)$, where $\alpha = \epsilon + \epsilon^{-1}$, which is a totally real cubic number field. Here $f_3(\alpha) = 0$ where

$$f_3(x) = x^3 - ax^2 - 4x + 4a - 1 \tag{1.2}$$

is irreducible over $\mathbb{Q}$. Let $\mathcal{O}_3$ be the ring of integers in k_3 and suppose that $\mathcal{O}_3 = \mathbb{Z}[\alpha]$. A related quartic field is $k_4 = \mathbb{Q}(\rho)$, where ρ is a root of

$$f_4(x) = x^4 + ax^2 + x + 1. \tag{1.3}$$

This field k_4 is totally complex and its discriminant equals that of k_3. For $j = 3, 4, 6$ let h_j be the (wide) class number of k_j. The main result of this paper is the following class number relation. Unlike most other such relations that are known, it does not involve undetermined regulator indices.

Theorem 1. *If $\mathcal{O}_3 = \mathbb{Z}[\alpha]$, then*

$$h_6 = h_3 h_4.$$

As an example, when $a = 100$, we have that $h_3 = 412$, $h_4 = 112$ and $h_6 = 46144$. Concerning the condition that $\mathcal{O}_3 = \mathbb{Z}[\alpha]$, this certainly holds if the discriminant of f_3, which is

$$D_a = 16a^4 - 4a^3 - 128a^2 + 144a + 229, \tag{1.4}$$

[1] Useful references on Salem numbers and Salem extensions are [5] and [16].

is square-free. It is conjectured that D_a is square-free for more than 75% of integers $a \in \mathbb{Z}^+$ (see e.g. [13]). In general, for the integers $0 \le a \le 100$ we have that $\mathcal{O}_3 = \mathbb{Z}[\alpha]$ except when

$$a \in \{20, 28, 32, 34, 69, 81, 82, 84, 85\}.$$

The result of the theorem actually holds for all of the many values of a tested (using PARI/GP) and it is tempting to conjecture that it holds for all $a \ge 0$.

Another result of this paper is an independent proof and refinement of a (very) special case of a theorem of Stark [17, Theorem 2] on the derivative of an Artin L-function at $s = 0$.

Theorem 2. *Suppose that $\mathcal{O}_3 = \mathbb{Z}[\alpha]$. Let χ be the non-trivial quadratic character of k_6/k_3 and $L(s, \chi)$ be the associated Artin/Hecke L-function. Then*

$$h_3 L'(0, \chi) = h_6 \log \epsilon,$$

where a basis for the fundamental units of k_6 is given by $\{\epsilon - 1, \epsilon, \epsilon + 1\}$.

Acknowledgement. I am very grateful to Chris Smyth for showing me an argument that ϵ cannot be the square of another Salem number when $a \ne 2$ and for allowing me to include it here.

2. The number fields

In this section I will give some needed properties of the number fields k_3, k_6 and k_4. In the process I will apply results from [18], [16], [2], [12] and especially [8].

Lemma 1. *For integral $a \ge 0$ the cubic*

$$f_3(x) = x^3 - ax^2 - 4x + 4a - 1$$

is irreducible over $\mathbb{Q}$ and has discriminant D_a from (1.4). The polynomial f_3 has three real roots $\alpha = \alpha, \alpha', \alpha''$ that satisfy

$$\alpha > 2 \ \text{ and } \ |\alpha'| < 2, |\alpha''| < 2.$$

Suppose that $\mathcal{O}_3 = \mathbb{Z}[\alpha]$. Then the unit group of k_3 is generated by -1 and the pair

$$\eta_1 = \alpha - 2, \qquad \eta_2 = \alpha + 2. \tag{2.1}$$

Proof. For $a < 4$ these results can be checked directly. For $a \ge 4$ they follow from [18, p.158, Satz 7], after making a simple change of variables in f_3 (see also [19, Thm. 3.9]). □

In particular, the cubic field k_3 is totally real. Recall the notation from the above Theorem 1.

Lemma 2. *Suppose that $\mathcal{O}_3 = \mathbb{Z}[\alpha]$. The field $k_6 = \mathbb{Q}(\epsilon)$ is an unramified quadratic extension of k_3 with ϵ a Salem number and with discriminant $d_6 = D_a^2$. The ring of integers $\mathcal{O}_6$ in k_6 is $\mathbb{Z}[\epsilon]$. The signature of k_6 is $[2, 2]$ and the infinite part of the unit group has rank 3, while the torsion part is $\{\pm 1\}$.*

Proof. Observe that

$$x^3 f_3(x + x^{-1}) = f_6(x).$$

Since f_3 is irreducible over $\mathbb{Q}$ so is $f_6(x)$ (c.f. [2, p.864]). That $\mathbb{Q}(\epsilon)$ is a Salem extension of k_3 follows Lemma 1 and [16, Prop. 3 (i)]. A computation shows that the discriminant of f_6 is D_a^2 and so the fact that k_6 is unramified over k_3 follows, since by assumption the discriminant of k_3 is D_a. Therefore the discriminant of k_6 is D_a^2 and $\mathcal{O}_6 = \mathbb{Z}[\epsilon]$. The final statement is easily verified. □

Note that

$$\epsilon = \tfrac{1}{2}(\alpha + \sqrt{\alpha^2 - 4}), \quad \epsilon' = \tfrac{1}{2}(\alpha' + \sqrt{\alpha'^2 - 4}), \quad \epsilon'' = \tfrac{1}{2}(\alpha'' + \sqrt{\alpha''^2 - 4}). \tag{2.2}$$

The relative norm from k_6 to k_3 is given by $\beta \mapsto N_{k_6/k_3}(\beta) = \beta\beta^\sigma$ where $\beta \mapsto \beta^\sigma$ is the Galois conjugation induced by $\epsilon \mapsto \frac{1}{\epsilon}$. It can be checked that

$$N_{k_6/k_3}(\epsilon - 1) = -\eta_1 \quad N_{k_6/k_3}(\epsilon + 1) = \eta_2 \quad N_{k_6/k_3}(\epsilon) = 1. \tag{2.3}$$

The subgroup $U \subset \mathcal{O}_6^*$ given by

$$U = \{\eta \in \mathcal{O}_6^*;\ \eta > 0 \text{ and } N_{k_6/k_3}(\eta) = 1\} \tag{2.4}$$

is cyclic and generated by $\epsilon_0 > 1$, say. Thus $\epsilon = \epsilon_0^\ell$ for some $\ell \in \mathbb{Z}^+$. We will show in the next section that $\ell = 1$. The following result is now readily proven, using (2.3) and the final statement of Lemma 1.

Lemma 3. *Assumptions as above, the unit group $\mathcal{O}_6^*$ is generated by $-1, \epsilon - 1, \epsilon + 1$ and ϵ_0.*

After Lemma 2 we can make use of the fact that these fields k_3, k_6 are among those treated by Heilbronn in [8]. Let $\overline{k}_3$ be the normal closure of k_3. Then Heilbronn shows that $k_{24} = \overline{k}_3(\epsilon, \epsilon')$ is normal over $\mathbb{Q}$ with Galois group S_4.

Lemma 4. *Suppose that $\mathcal{O}_3 = \mathbb{Z}[\alpha]$. We have that*

$$k_4 = \mathbb{Q}(\epsilon + \epsilon' + \epsilon'').$$

The field k_4 is totally complex with discriminant $d_4 = D_a$ and ring of integers $\mathcal{O}_4 = \mathbb{Z}[\rho]$. The unit group of k_4 is generated by -1 and ρ. We have the identity

$$|\rho|^2 = \epsilon^{\pm 1},$$

where ϵ is the Salem number.

Proof. A calculation shows that $g_4(\gamma) = 0$ where $\gamma = \epsilon + \epsilon' + \epsilon''$ and

$$g_4(x) = x^4 - 2ax^3 + (a^2 + 2)x^2 - (2a - 1)x + 1.$$

Another calculation gives that $f_4(\rho) = 0$ where

$$-\rho^{-1} = \gamma^3 - 2a\gamma^2 + (a^2 + 1)\gamma - (a - 1) \tag{2.5}$$

and f_4 is from (1.3). Furthermore, using (2.5) it holds that $\gamma = -\rho^2$. Thus $k_4 = \mathbb{Q}(\gamma)$ so k_4 coincides with Heilbronn's quartic field.

The discriminant of f_4 is D_a. Heilbronn shows that

$$\zeta(s)\zeta(s, k_6) = \zeta(s, k_3)\zeta(s, k_4) \tag{2.6}$$

and uses this to deduce that for d_j the discriminant of k_j for $j = 3, 4, 6$ we have

$$d_6 = d_3 d_4.$$

This can also be deduced from [6]. By assumption, $d_3 = D_a$ and so by Lemma 2 we have that $d_4 = D_a$ and $\mathcal{O}_4 = \mathbb{Z}[\rho]$.

After an obvious change of variables, it follows from [12, Prop 19] that k_4 is totally complex and contains no roots of unity other than ± 1 and that ρ gives a fundamental unit for k_4, when $a \geq 3$. The remaining cases are checked directly. A computation shows that $|\rho|^2$ satisfies $f_6(|\rho|^2) = 0$. Thus we have

$$|\rho|^2 = \epsilon^{\pm 1}.$$

□

3. Proof of Theorem 1

The class number formula (at $s=0$) states that for a number field k with unit rank r that contains w roots of unity, has class number h and regulator R, we have

$$\lim_{s\to 0} s^{-r}\zeta(s,k) = -\frac{hR}{w}.$$

Thus by the identity (2.6) and the fact that the only roots of unity in any of our fields are ± 1, we have

$$h_6R_6 = h_3R_3h_4R_4$$

Lemma 5. *For R_j the regulator of k_j for $j=3,4,6$ and ℓ from below (2.4) we have*

$$R_6 = \ell R_3R_4.$$

Proof. By Lemma 3 we have that ℓR_6 is the absolute value of

$$\det\begin{pmatrix} \log\epsilon & \log(\epsilon-1) & \log(\epsilon+1) \\ -\log\epsilon & \log|\epsilon^{-1}-1| & \log|\epsilon^{-1}+1| \\ 2\log|\epsilon'| & 2\log|\epsilon'-1| & 2\log|\epsilon'+1| \end{pmatrix} = \det\begin{pmatrix} \log\epsilon & \log(\epsilon-1) & \log(\epsilon+1) \\ 0 & \log|2-\epsilon-\epsilon^{-1}| & \log|2+\epsilon+\epsilon^{-1}| \\ 0 & 2\log|\epsilon'-1| & 2\log|\epsilon'+1| \end{pmatrix},$$

after using that $|\epsilon'|=1$ and adding the first row to the second. Recall that

$$\alpha = \epsilon + \epsilon^{-1}.$$

By using Lemma 1, the definitions (2.1) and that from (2.2) $|\epsilon'-1|^2 = 2-\alpha' = |\eta_1'|$ and $|\epsilon'+1|^2 = 2+\alpha' = |\eta_2'|$, where η_1' and η_2' are corresponding Galois conjugates of η_1 and η_2, we get

$$\ell R_6 = \left|\det\begin{pmatrix} \log\epsilon & \log(\epsilon-1) & \log(\epsilon+1) \\ 0 & \log|\eta_1| & \log|\eta_2| \\ 0 & \log|\eta_1'| & \log|\eta_2'| \end{pmatrix}\right| = (\log\epsilon)R_3.$$

Now the result follows since by Lemma 3 we have $\epsilon = |\rho|^{\pm 2}$, where ρ is a fundamental unit for k_4. □

After Lemma 5 and the line above it, what is left is to show that $\ell = 1$, that is $\epsilon_0 = \epsilon$. Since the Galois group of $k_{24}/\mathbb{Q}$ is S_4, it follows from Lemma 5 and a result of Brauer [3, Satz 4, Bemerkungen 2, p.174] that the only primes that can divide ℓ must divide $\#S_4 = 24$, hence are 2 and 3. This can also be deduced from [1, Thm. 1.2], which gives another proof of Brauer's result. We may of course assume that $a \neq 2$.

It can be seen (recall (2.4)) that ϵ_0 is a Salem number. Hence it is enough to show that for integers b, c, d and

$$g(x) = x^6 + bx^5 + cx^4 + dx^3 + cx^2 + bx + 1$$

both kinds of factorizations

$$f_6(x^2) = g(x)g(-x) \tag{3.1}$$

and, for $\omega = e^{\frac{2\pi i}{3}}$,

$$f_6(x^3) = g(x)g(\omega x)g(\omega^2 x), \tag{3.2}$$

are impossible. Here f_6 is given in (1.1).

To show that (3.1) cannot occur, I follow Smyth's communication and equate coefficients in it to get

$$-b^2+2c = -a, \qquad 2c+c^2-2bd = -1, \qquad 2-2b^2+2c^2-d^2 = -1+2a \tag{3.3}$$

and eliminate b and d to obtain

$$(c+1)^4 - 4(a+2c)(3-4a+2c^2-4c) = 0. \tag{3.4}$$

It can be checked using the genus-degree formula

$$g = \tfrac{(d-1)(d-2)}{2} - \delta$$

that (3.4) determines a curve of genus $g = 0$. Here the degree $d = 4$ and the (projective) curve has a singularity at $(1, 0, 0)$ with delta invariant $\delta = 3$. Thus the curve can be parametrized by rational functions. Probably the simplest parameterization is given by

$$a = 2 + \tfrac{(t^3+8t^2-8)t}{4(t^2-1)^2}, \quad c = -1 - \tfrac{t}{t^2-1}.$$

Thus from (3.3) we also have (with same choice of $\pm$)

$$d = \pm\tfrac{1}{t^2-1} \text{ and } b = \pm\tfrac{t^2}{2(t^2-1)}.$$

Seeking a solution $t \neq 0$ such that $a, b, c, d \in \mathbb{Z}$, we see from the formula for d that t^2 must be rational, and then from the formula for c that t is rational. From the d-formula we get $t^2 = (d \pm 1)/d$, which is a rational square for integral d only for $d = \mp 1$ and $t = 0$. Note that d and $d \pm 1$ are relatively prime. Hence a, b, c and d cannot all be integers when $a \neq 2$.

To show that (3.2) cannot occur, we again equate coefficients:

$$\begin{aligned} b^3 - 3bc + 3d &= -a \\ 3 + 3b^2(-1+c) - 3c^2 + c^3 - 3bcd + 3d^2 &= -1 \\ 6b(-1+c)c - 3b^2d + d(6 - 3c^2 + d^2) &= -1 + 2a. \end{aligned}$$

By eliminating a and d from these equations we must have

$$\begin{aligned} R(b,c) := {} & 81b^4c^5 - 567b^4c^4 + 1296b^4c^3 - 648b^4c^2 - 1296b^4c + 1296b^4 + 27b^3c^3 - 81b^3c^2 \\ & + 108b^3 - 18b^2c^7 - 18b^2c^6 + 432b^2c^5 - 144b^2c^4 - 3168b^2c^3 + 4320b^2c^2 + 2304b^2c \\ & - 4608b^2 - 27bc^4 + 324bc^2 - 432bc + c^9 + 9c^8 - 168c^6 - 144c^5 + 1296c^4 \\ & + 768c^3 - 4608c^2 + 4123 = 0. \end{aligned}$$

Reducing modulo 3 gives $c^9 + 1 \equiv 0 \pmod 3$ so we must have for some integer n that $c = 3n - 1$. But $R(b, 3n-1) \equiv 27 \pmod{81}$, which is a contradiction.

We have shown that neither 2 nor 3 can divide ℓ and thus, after Brauer, that $\ell = 1$. This finishes the proof of Theorem 1. □

4. Proof of Theorem 2

Since

$$L(s, \chi) = \frac{\zeta(s, k_6)}{\zeta(s, k_3)},$$

the class number formula gives

$$L'(0, \chi) = \frac{h_6 R_6}{h_3 R_3}.$$

Theorem 2 follows from Lemma 3 and the formula

$$\frac{R_6}{R_3} = \ell R_4 = \log \epsilon$$

of Lemma 5, together with the fact shown above that $\ell = 1$. □

References

[1] Bartel, A. On Brauer-Kuroda type relations of S-class numbers in dihedral extensions. J. Reine Angew. Math. 668 (2012), 211–244.

[2] Boyd, D. W. On the beta expansion for Salem numbers of degree 6. Math. Comp. 65 (1996), no. 214, 861–875, S29–S31.

[3] Brauer, R. Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers. Math. Nachr. 4 (1951), 158–174., in Collected Papers III, p.497–513.

[4] Dirichlet, G. L. Recherches sur les formes quadratiques à coëfficients et à indéterminées complexes. Première partie. J. Reine Angew. Math. 24 (1842), 291–371, XXXII in Werke I.

[5] Ghate, E.; Hironaka, E. The arithmetic and geometry of Salem numbers. Bull. Amer. Math. Soc. (N.S.) 38 (2001), no. 3, 293–314.

[6] Godwin, H. J. On relations between cubic and quartic fields. Quart. J. Math. Oxford Ser. (2) 13 (1962), 206–212.

[7] Hasse, H. Über die Klassenzahl abelscher Zahlkörper. Akademie-Verlag, Berlin, 1952. xii+190 pp.

[8] Heilbronn, H. On the 2-classgroup of cubic fields.Studies in Pure Mathematics (Presented to Richard Rado), pp. 117–119 Academic Press, London-New York, 1971

[9] Herglotz, G. Über einen Dirichletschen Satz. Math. Z. 12 (1922), no. 1, 255–261.

[10] Hilbert, D. Über den Dirichlet'schen biquadratischen Zahlkörper. Math. Ann. 45 (1894), no. 3, 309–340.

[11] Kuroda, S. Über den Dirichletschen Körper. J. Fac. Sci. Imp. Univ. Tokyo Sect. I. 4 (1943), 383–406.

[12] Louboutin, S. R. The fundamental unit of some quadratic, cubic or quartic orders. J. Ramanujan Math. Soc. 23 (2008), no. 2, 191–210.

[13] Murty, M.R.; Pasten, H. Counting squarefree values of polynomials with error term, International Journal of Number Theory Vol. 10, No. 7 (2014) 1743–1760.

[14] Nehrkorn, H. Über die absolute Idealklassengruppe und Einheiten in algebraischen Zahlkörpern, Abh. Math. Sem. Univ. Hamburg 9 (1933) 318–334.

[15] Schertz, R. Über die Klassenzahl gewisser nicht galoisscher Körper 6-ten Grades. Abh. Math. Sem. Univ. Hamburg 42 (1974), 217–227.

[16] Smyth, C. Seventy years of Salem numbers. Bull. Lond. Math. Soc. 47 (2015), no. 3, 379–395.

[17] Stark, H. M. L-functions at $s = 1$. II. Artin L-functions with rational characters. Advances in Math. 17 (1975), no. 1, 60–92.

[18] Stender, H.-J. Einheiten für eine allgemeine Klasse total reeller algebraischer Zahlkörper. J. Reine Angew. Math. 257 (1972), 151–178.

[19] Thomas, E. Fundamental units for orders in certain cubic number fields. J. Reine Angew. Math. 310 (1979), 33–55.

UCLA Mathematics Department, Box 951555, Los Angeles, CA 90095-1555

Email address: wdduke@g.ucla.edu