# A DEVICE FOR GENERATING FIELDS OF EVEN CLASS NUMBER

HARVEY COHN[1]

The device in question is typefied by the following two theorems:

QUADRATIC THEOREM. *If for integral $g(>0)$, $m$, $k(>1)$*

$$m = \frac{k^2 - 1}{g} + g, \tag{1}$$

*and $f = m^2 + 4$ is square-free, then the quadratic field of discriminant $f$ has even class number.*

CUBIC THEOREM. *If for integral $g(>0)$, $m$, $k(>1)$,*

$$m = \frac{k^2 - 2g - 1}{g(g+1)} + g - 1, \tag{2}$$

*and $f = m^2 + 3m + 9$ is a square-free[2] integer, then an abelian cubic field of discriminant $f^2$ has even class number.*

PROOF OF THEOREMS.

| Quadratic | * | Cubic |
|---|---|---|
| $n = 2$ | * | $n = 3.$ |

We consider a square-free number $f$ of the form

$$f = m^2 + 4, \qquad * \qquad f = m^2 + 3m + 9,$$

with $m > 0$, together with the equation $F(\xi) = 0$, where

$$F(x) = x^2 - mx - 1. \qquad * \qquad F(x) = x^3 - mx^2 - (m+3)x - 1.$$

The equation has (root) discriminant

$$\prod_{i>j} (\xi_i - \xi_j)^2 = f^{n-1}$$

where $\xi_1, \cdots, \xi_n$ are the roots which generate the abelian field $R(\xi)$.

Received by the editors August 23, 1955.

[1] Presented June 24, 1955 as an invited address to the National Science Foundation Research Conference on The Theory of Numbers at Pasadena under the title *Accessibility of algebraic numbers with rounded norms.* The author is indebted to Drs. S. Rosen and A. W. Jacobson of the Wayne University Computation Center for making the UDEC available for the computation of the table.

[2] If 9 divides $f$ the hypothesis can be broadened to include values of $f$ for which $f/3$ is square-free, by a slight modification of the proof. Compare footnote 3.

The quantity $f^{n-1}$ is also the discriminant of the field $R(\xi)$, as follows from the fact that $f$ is square-free while

$$R(\xi) \qquad * \qquad R(\xi, \rho), \ [\rho^2 + \rho + 1 = 0]$$

is formed by the adjunction of the irreducible radical[3]

$$f^{1/2} \text{ to } R \qquad * \qquad [f(m - 3\rho)]^{1/3} \text{ to } R(\rho).$$

As a result, the most general integer in $R(\xi)$ is given by the expression $\lambda = A_0 + \cdots + A_{n-1}\xi^{n-1}$ where $A_0, \cdots, A_{n-1}$ are rational integers. It also follows, by subtraction, that no two of the $n$ conjugates $\xi_1 - g, \cdots, \xi_n - g$ can have as common factors *different* conjugates of a prime ideal. Thus any number of the form $\xi - g$ with square norm must generate a square ideal. We finally note, in preparation, that a unit which is totally positive (i.e., for which all three conjugates are positive) is the square of another unit in $R(\xi)$. To see this, we need only display the following $2^n$ units which exhibit all possible $2^n$ arrays of $+$ and $-$ signs when their $n$ conjugates are listed:

$$+1, -1, +\xi_1, -\xi_1. \qquad * \qquad +1, -1, +\xi_1, -\xi_1, +\xi_2, -\xi_2, +\xi_3, -\xi_3.$$

In fact, in some order of listing,

$$\begin{array}{lcl} m < \xi_1 < m + 1, & * & m + 1 < \xi_1 < m + 2, \\ -1 < \xi_2 < 0. & * & -1 < \xi_2 < 0, \\ & * & -2 < \xi_3 < -1. \end{array}$$

We consider now integers $g$, $k$ such that

$$F(g) = N(g - \xi) = - k^2, \qquad (k > 1). \tag{3}$$

This result leads on expansion to equations (1), (2). Then,

$$0 < g < m + 1; \qquad * \qquad 0 < g < m + 2; \tag{4}$$

and the number, of norm $k^2$,

$$\zeta = \xi(\xi - g) \tag{5}$$

must be totally positive. Thus $\xi - g$ generates the square of an ideal which could not be principal unless $\zeta$ were a perfect square. We shall now eliminate this last possibility, completing the proofs.

In the quadratic case, the equation $(A_0 + A_1\xi)^2 = \xi(\xi - g)$ leads to a triviality, all the more so in the cubic case ($A_2 = 0$). Henceforth we

[3] This argument, superfluous when $f$ is prime, uses the only nonelementary result here. See H. Hasse, *Arithmetiche Bestimmung von Grundeinheit und Klassenzahl in zyklischen, kubischen und biquadratischen Zahlkörpern*, Berlin, 1950.

restrict ourselves to the cubic case, writing in terms of three conjugates

$$A_0 + A_1\xi_i + A_2\xi_i^2 = \pm \zeta_i^{1/2} \qquad (i = 1, 2, 3),$$

with choice of sign open. We solve for $A_2$, recalling that $f^2$ is the (root) discriminant, so that

$$fA_2 = \pm \zeta_1^{1/2}(\xi_2 - \xi_3) \pm \zeta_2^{1/2}(\xi_3 - \xi_1) \pm \zeta_3^{1/2}(\xi_1 - \xi_2). \tag{6}$$

We find, from equations (4) and (5) that

$$\begin{aligned} |\zeta_1| &< (m + 1)^2, & |\xi_2 - \xi_3| &< 2, \\ |\zeta_2| &< (m + 1), & |\xi_3 - \xi_1| &< m + 4, \\ |\zeta_3| &< 2m, & |\xi_1 - \xi_2| &< m + 3, \end{aligned}$$

so that from equation (6),

$$|A_2| \leqq [2(m + 1) + (1 + 2^{1/2})(m + 1)^{1/2}(m + 4)]/(m^2 + 3m + 9).$$

Thus if $m \geqq 12$, $A_2 = 0$, leading to a triviality. (The smaller $m$ can be checked by hand as the values of $g$ are limited by equation (4) and the values of $k$ by equation (2).)

COROLLARY. *If* $g \equiv 0 \bmod 4$, *then the fields* $R(\xi)$ *referred to in the above theorems have an unramified quadratic extension produced by* $[\xi(\xi - g)]^{1/2}$.

The proofs depend on the relation[4] $\zeta \equiv \xi^2 \bmod 4$. We should note that with $g \equiv 0 \bmod 4$ the condition "$g(>0)$" in the (cubic) theorems is superfluous from the integral nature of $m$, as $k^2 \not\equiv -1 \bmod (g+1)$.

**Tabulation.** The above proofs still leave unanswered the question of *how effective* a method we have for (say) finding *cubic* fields of even class number where the discriminant is $f^2$, for $f(=m^2+3m+9)$ restricted to *prime* values. Under such a restriction we have a convenient basis of comparison in Mr. Peter Swinnerton-Dyer's unpublished table (abbreviated SDT) of class numbers as computed from the cyclotomic units (rather than the ideal structure). The table below lists $g$, $k$, $m$, $f$ and the class number $h$ (where provided by SDT) for $f < 100{,}000$, $m < 316$, $g \equiv 0 \bmod 4$. The first field of even class number that does not emerge has $f = 18{,}913$ with $h = 100$ according to SDT.

---

[4] See D. Hilbert, *Über die Theorie der relativ-Abelschen Zahlkörper*, Acta Math. vol. 26 (1902) pp. 99–132.

We now have another illustration of the classical observation that the composite norms (such as $-k^2$) which are so useful in determining class structures[5] are more readily accessible than one would believe on the basis of known theory alone. In this case the desired norms are found from the generating polynomial, i.e., $F(g)$, without requiring the use of the full (ternary) norm expression for the general integer of the field. This convenient state of affairs, as expected, becomes dissipated as $f \to \infty$, however.

TABLE OF UNRAMIFIED QUADRATIC EXTENSIONS OF CUBIC FIELDS OF EVEN CLASS NUMBER AND PRIME CONDUCTOR $f = m^2+3m+9 < 100{,}000$, FORMED BY ADJOINING $[\xi(\xi-g)]^{1/2}$, OF NORM $k$, WHERE $\xi^3 - m\xi^2 - (m+3)\xi - 1 = 0$.

| $g$ | $k$ | $m$ | $f$ | $h$ | $g$ | $k$ | $m$ | $f$ | $h$ |
|---|---|---|---|---|---|---|---|---|---|
| 4 | 13 | 11 | 163 | 4 | . . . | . . . | 136 | 18,913 | 100 |
| 12 | 5 | 11 | 163 | 4 | 72 | $13\cdot 47$ | 142 | 20,599 | 112 |
| 4 | 17 | 17 | 349 | 4 | 4 | 53 | 143 | 20,887 | 64 |
| 12 | 31 | 17 | 349 | 4 | 28 | 307 | 143 | 20,887 | 64 |
| 24 | 7 | 23 | 607 | 4 | 64 | 577 | 143 | 20,887 | 64 |
| 16 | 47 | 23 | 607 | 4 | 124 | 557 | 143 | 20,887 | 64 |
| 12 | 47 | 25 | 709 | 4 | 144 | 17 | 143 | 20,887 | 64 |
| 4 | 23 | 29 | 937 | 4 | 36 | $7\cdot 59$ | 163 | 27,067 | ? |
| 28 | 41 | 29 | 937 | 4 | 156 | 443 | 163 | 27,067 | ? |
| 24 | 157 | 64 | 4,297 | 16 | 144 | $11\cdot 67$ | 169 | 29,077 | ? |
| 24 | 193 | 85 | 7,489 | ? | 168 | 239 | 169 | 29,077 | ? |
| 4 | 43 | 95 | 9,319 | 28 | 88 | $5\cdot 167$ | 176 | 31,513 | ? |
| 84 | 293 | 95 | 9,319 | 28 | 100 | $29\cdot 31$ | 179 | 32,587 | ? |
| 40 | $11\cdot 29$ | 101 | 10,513 | 64 | 180 | 19 | 179 | 32,587 | ? |
| 60 | 499 | 127 | 16,519 | 52 | 88 | 1,013 | 218 | 48,187 | ? |
| 72 | 557 | 130 | 17,299 | 52 | 84 | $11\cdot 107$ | 277 | 77,569 | ? |
| 24 | 257 | 133 | 18,097 | 52 | 112 | 1,567 | 305 | 93,949 | ? |

STANFORD UNIVERSITY

[5] Compare H. Cohn, *Some experiments in ideal factorization on the MIDAC*, J. Assoc. Comput. Mach. vol. 2 (1955) pp. 111–116.