ON ALGEBRAIC NUMBER FIELDS WITH UNIQUE FACTORIZATION

Ian G. Connell

(received April 2, 1962)

In this note we obtain some simple criteria which show that in certain algebraic number fields factorization of elements is not unique. All the arguments depend only on the most elementary ideas (except in §6) so that probably many of the results are not new. However the proofs are short and direct and therefore should be of some interest.

1. Introduction. We now list some basic facts, whose proofs can be found in any of the books listed in the bibliography, at the same time fixing our notation.

Let θ be a zero of the irreducible polynomial $x^n+a_{n-1}x^{n-1}+\ldots+a_o$ where $a_i \in Z$, the ring of rational integers. We denote by $Q(\theta)$ the field obtained by adjoining θ to the rational field Q, and by J the ring of algebraic integers in $Q(\theta)$; thus $\theta \in J$. An integral basis for J is a set of n elements $\{w_1, \ldots, w_n\} \subset J$ such that

$$J = \{b_1w_1+\ldots+b_nw_n : b_i \in Z\} .$$

The conjugates of θ are the zeros $\theta^{(1)} = \theta, \theta^{(2)}, \ldots, \theta^{(n)}$ of the polynomial $x^n+\ldots+a_o$; these algebraic integers may or may not be in J. Every element $\alpha \in J$ is a polynomial in θ with rational coefficients:

Canad. Math. Bull. vol. 5, no. 2, May 1962.

https://doi.org/10.4153/CMB-1962-017-5 Published online by Cambridge University Press

$$\alpha = C_o + C_1\theta + \ldots + C_{n-1}\theta^{n-1}\ , \quad C_i \epsilon Q$$

(though not all such rational polynomials are in J). The conjugates $\alpha^{(1)} = \alpha$, $\alpha^{(2)}$, ..., $\alpha^{(n)}$ of α are defined by

$$\alpha^{(j)} = C_o + C_1\theta^{(j)} + \ldots + C_{n-1}(\theta^{(j)})^{n-1} .$$

The <u>norm</u> of α is defined by

$$N\alpha = \alpha^{(1)} \cdot \alpha^{(2)} \ldots \alpha^{(n)} .$$

$N\alpha \epsilon Z$ and $N\alpha = 0$ if and only if $\alpha = 0$; also $N(\alpha\beta) = N\alpha . N\beta$. The conjugates $\alpha^{(2)}, \ldots, \alpha^{(n)}$ may or may not be in J ; however $\alpha^{(2)} \ldots \alpha^{(n)} \epsilon J$ since, as a product of algebraic integers it is an algebraic integer, and also

$$\alpha^{(2)} \ldots \alpha^{(n)} = N\alpha / \alpha \epsilon Q(\theta) .$$

Henceforth Latin letters will denote elements of Z (except when definitely stated to be elements of Q) and Greek letters will denote elements of J .

α is called a <u>unit</u> if there exists a β such that $\alpha\beta = 1$; this occurs if and only if $N\alpha = \pm 1$. If $\alpha = \beta\epsilon$ where ϵ is a unit, α and β are called <u>associates.</u> The elements of J which are neither 0 nor units are either <u>primes</u> or <u>composite numbers</u>, a prime π being characterized by the property that if $\pi = \alpha\beta$, then one of α, β is a unit. A rational prime p may or may not be a prime in J ; however if $N\alpha = \pm p$, α is prime. If π is prime so are its conjugates belonging to J and the associates of these numbers.

Every composite number can be written as a product of primes, and if factorization into primes is unique (apart from the order of the factors and ambiguity between associated primes) we shall say that $Q(\theta)$ is <u>simple</u>.

https://doi.org/10.4153/CMB-1962-017-5 Published online by Cambridge University Press

Many of our results will be deduced from

PROPOSITION 1. Let $Q(\theta)$ be simple and let $p^s \| N\alpha$ where p is a rational prime. Then there exists a prime π such that $N\pi = \pm p^t$ where $t \leq s$ and $t \leq n$.

Remarks: $p^s \| N\alpha$ means $p^s | N\alpha$ (p^s divides $N\alpha$) but $p^{s+1} \nmid N\alpha$ (p^{s+1} does not divide $N\alpha$). $n = (Q(\theta):Q)$ always stands for the degree of the extension. Actually we shall use this result only in the weakened form: If p occurs to the first power in a norm then for some β, $N\beta = \pm p$.

Proof: Let $\alpha = \pi\rho \ldots$ be a factorization of α into primes. Then $N\alpha = N\pi \cdot N\rho \ldots$ so that some factor on the right, say $N\pi$ is divisible by p: $N\pi = p^t u$, $1 \leq t \leq s$, $p \nmid u$. Now

$$N\pi = \pi(\pi^{(2)} \ldots \pi^{(n)}) = p^t u$$

and $\pi^{(2)} \ldots \pi^{(n)} \in J$; since factorization is unique, $\pi \mid p$ or $\pi \mid u$. If $\pi \mid u$, $N\pi \mid Nu$, i.e., $p^t u \mid u^n$ which is impossible since $p \nmid u$. Thus $\pi \mid p$ and therefore $N\pi \mid Np$, i.e., $p^t u \mid p^n$. Hence $u = \pm 1$ and $t \leq n$.

2. Quadratic fields (the case $n = 2$). All quadratic extensions of Q are of the form $Q(\sqrt{m})$ where m is a square-free rational integer. An integral basis for J is

$$\{1, \sqrt{m}\} \quad \text{if} \quad m \not\equiv 1 \mod 4$$

$$\left\{1, \frac{\sqrt{m}-1}{2} = \sigma\right\} \quad \text{if} \quad m \equiv 1 \mod 4$$

In other words, the elements of J are $a + b\sqrt{m}$ where $a, b \in Z$ except that when $m \equiv 1 \mod 4$ a and b may also be both halves of odd integers. The conjugates of $\alpha = a + b\sqrt{m}$, itself and $\alpha^{(2)} = a - b\sqrt{m}$ are both in J and

$$N\alpha = N\alpha^{(2)} = \alpha . \alpha^{(2)} = a^2 - mb^2 .$$

If $m \equiv 1 \mod 4$ and the element is expressed in terms of the integral basis this formula becomes

https://doi.org/10.4153/CMB-1962-017-5 Published online by Cambridge University Press

$$N(a + b\sigma) = N(a - \frac{b}{2} + \frac{b}{2}\sqrt{m}) = a^2 - ab - qb^2$$

where $q = \frac{m - 1}{4}$.

For convenience we say that m is simple if $Q(\sqrt{m})$ is simple. We deal with the cases $m < 0$ and $m > 0$ separately.

3. Complex quadratic fields (the case $m < 0$). Here the norm is positive definite: $N(a + b\sqrt{m}) = a^2 - mb^2 = a^2 + |m| b^2$ and solving the equation $N\alpha = 1$ one sees that if $m < -3$ the only units are ± 1. $m = -1, -2, -3$ are known to be simple and we restrict ourselves to $m < -3$.

PROPOSITION 2. ($m < -3$). If m is simple then $m = 1$ mod 4.

Proof: Suppose that $m < -3$ is simple and $m \not\equiv 1$ mod 4. Since m is square-free, $m \equiv 2$ or 3 mod 4, and since m is negative $|m| \equiv 1$ or 2 mod 4. Thus either $|m| = N(\sqrt{m})$ or $1 + |m| = N(1 + \sqrt{m})$ is $\equiv 2$ mod 4, i.e., is divisible by 2 and not by 2^2 , and so by proposition 1, $N\pi = a^2 + |m| b^2 = 2$ is soluble in integers; but this is clearly impossible.

PROPOSITION 3. ($m < -3$). If m is simple then all the following numbers are rational primes:

$$N = a^2 - ab - qb^2$$

provided $1 < N < q^2$ and g.c.d.$(a, b) = 1$.

Proof: By proposition 2, $m \equiv 1$ mod 4 so that

$$N\alpha = N(a + b\sigma) = a^2 - ab - qb^2 = \{a - \frac{b}{2}\}^2 + |q + \frac{1}{4}| b^2$$

where $q = \frac{m - 1}{4} < 0$. Clearly if $b \neq 0$, $N\alpha \geq |q|$.

First we show that if g.c.d.$(a, b) = 1$ and $1 < N\alpha < q^2$ than α is prime. For suppose $\alpha = \beta\gamma$ where $\beta = c + d\sigma$ and $\gamma = e + f\sigma$. Then $N\alpha = N\beta N\gamma < q^2$ so that one of the factors on the right, say $N\beta$, satisfies $N\beta < |q|$. This implies $d = 0$

and $\alpha = ce + cf\sigma$. Hence g. c. d. (ce, cf) = 1, $\beta = c = \pm 1$ is a unit, and α is prime. It follows that $\alpha^{(2)}$ is prime.

Thus we have $N = N\alpha = \alpha\alpha^{(2)}$ expressed as a product of primes. Since $b \neq 0$, none of the associates $\pm\alpha$, $\pm\alpha^{(2)}$ of α and $\alpha^{(2)}$ is rational. If N were not a rational prime, say $N = st$, $1 < s < N$, then either (i) s and t are primes in J or (ii) st splits further into a product of more than two primes in J. Either case leads to non-unique factorization, contrary to supposition.

Putting $b = 1$ we obtain

COROLLARY 1. If $m < -3$ is simple, $a^2 - a + |q|$ is a rational prime for $a = 1, 2, \ldots, |q| - 1$. In particular, $|q|$ is a rational prime.

Since $m \equiv 1 \bmod 4$, $|m| \equiv 3$ or $7 \bmod 8$. If $|m| = 8t + 7$ then $|q| = (|m| + 1)/4 = 2t + 2$ which is not prime if $t > 0$. Thus if $m < -7$ then $|m| \equiv 3 \bmod 8$.

Putting $b = 2$ we obtain

COROLLARY 2. If $m < -7$ is simple

$$a^2 - 2a + 4|q| = (a - 1)^2 + |m|$$

is a rational prime for $a = 1, 3, 5, \ldots, |q| - 2$. In particular, $|m|$ is a rational prime.

Since $|m| \equiv 3 \bmod 8$, $|q| - 2$ is odd. The largest value of N occurs with $a = |q| - 2$ and $N < q^2$ demands that $m < -15$; of the remaining possible m, -11 and -15, the corollary is clearly true for the former, and the latter is not simple by corollary 1.

To the modulus 24 we have the possibilities

$\lvert m\rvert$	$\lvert q\rvert$	comments
$24t + 3$	$6t + 1$	$\lvert m\rvert$ not prime if $t > 0$
$24t + 11$	$6t + 3$	$\lvert q\rvert$ not prime if $t > 0$
$24t + 19$	$6t + 5$	---

Thus we have

COROLLARY 3. If $m < -11$ is simple then $|m| \equiv 19 \bmod 24$.

COROLLARY 4. If $m < -7$ is simple and p is a rational prime $<|q|$ then the Legendre symbol $\left(\frac{p}{|m|}\right) = -1$.

Proof: Since $|m|$ is a prime $\equiv 3 \bmod 8$, $\left(\frac{2}{|m|}\right) = -1$. Thus let $p > 2$. By the law of quadratic reciprocity what we must prove is $\left(\frac{m}{p}\right) = -1$. Now $p < |q| < |m|$ so that $p \nmid m$ and $\left(\frac{m}{p}\right) \neq 0$. Suppose $\left(\frac{m}{p}\right) = 1$; then $x^2 \equiv m \bmod p$ for some $x \neq 0$. Thus $x^2 = m + kp$ and we may assume $p \nmid k$; for if $p|k$, $(x+p)^2 = m + k'p$ where $k' = k + 2x + p$ is not divisible by p. Hence p occurs to the first power in the norm $kp = x^2 - m = N(x + \sqrt{m})$ and therefore $N\pi = N(a + b\sigma) = p < |q|$ is soluble. From above the inequality implies $b = 0$; but then $Na = a^2 = p$, a contradiction. Thus $\left(\frac{m}{p}\right) = -1$. *

It is known that m is simple in the cases

$$-1, -2, -3, -7, -11, -19, -43, -67, -163,$$

and that at most one more simple negative m exists [6]. It is interesting to note that the two criteria that $|m|$ and $|q|$ be prime lead one immediately to these numbers. In eliminating $m < -163$ one has to use occasionally other criteria given by the proposition such as $|q| + 2$ is prime, $|m| + 4$ is prime, etc.

* One can give an alternative proof assuming that $|m|$ is a rational prime $\equiv 3 \bmod 4$, and the theorem in [4], p. 318. It is easy to see that p is not ramified and does not split; hence p is inert and $\left(\frac{m}{p}\right) = -1$.

https://doi.org/10.4153/CMB-1962-017-5 Published online by Cambridge University Press

Assuming that -163 is simple, corollary 1 gives the famous result of Euler that

$$a^2 - a + 41$$

is a rational prime for the 40 consecutive values $a = 1, 2, \dots, 40$; corollary 3 gives

$$\left(\frac{2}{163}\right) = \left(\frac{3}{163}\right) = \left(\frac{5}{163}\right) = \dots = \left(\frac{37}{163}\right) = -1$$

It seems that D. H. Lehmer [7] used a criterion such as that given in the last corollary to show that if the one possible simple $m < -163$ exists, then $m < -5.10^9$.

I have since discovered that Frobenius [1] proved proposition 3 in 1912. However his point of view was different: he found polynomials which like Euler's have many consecutive prime values and he related his results to the theory of quadratic forms.

4. Real quadratic fields (the case $m > 0$). Very much less is known about which $m > 0$ are simple. Proposition 1 does give some information; It is convenient to treat the case $p = 2$ separately.

PROPOSITION 4. ($m > 0$). Let $m \not\equiv 1 \bmod 4$ and let m be simple. Then

(1) m has no prime factor* $\equiv 5 \bmod 8$.

(2) If m has a prime factor $\equiv 3 \bmod 8$ then it has no prime factor $\equiv 7 \bmod 8$, and conversely.

Proof: One of $-m = N(\sqrt{m})$, $1 - m = N(1 + \sqrt{m})$ is divisible by 2 and not by 2^2. Hence by proposition 1, at least one of $a^2 - mb^2 = \pm 2$ is soluble. If q is any prime factor of m this implies $a^2 \equiv \pm 2 \bmod q$. But if $q \equiv 5 \bmod 8$,

* We often use 'prime' when it is clear from the context that we mean 'rational prime'.

https://doi.org/10.4153/CMB-1962-017-5 Published online by Cambridge University Press

$\left(\frac{2}{q}\right) = \left(\frac{-2}{q}\right) = -1$; this proves the first assertion.

If q_3 represents a prime $\equiv 3 \bmod 8$ and q_7 a prime $\equiv 7 \bmod 8$ then

$$\left(\frac{2}{q_3}\right) = -1\,, \quad \left(\frac{-2}{q_3}\right) = 1\,, \quad \left(\frac{2}{q_7}\right) = 1\,, \quad \left(\frac{-2}{q_7}\right) = -1\,.$$

We must show that $q_3 q_7 | m$ is impossible. If $a^2 - mb^2 = 2$ is soluble we would have $a^2 \equiv 2 \bmod q_3$; but the list of Legendre symbols above shows that this congruence is impossible. Similarly $a^2 - mb^2 = -2$ would imply $a^2 \equiv -2 \bmod q_7$, which is impossible.

Passing to primes > 2 we have

PROPOSITION 5. ($m \geq 0$). Let m be simple and let $p > 2$ be a rational prime for which m is a quadratic residue (i.e. $\left(\frac{m}{p}\right) = 0$ or 1). Then

(1) m can have no prime factor $q = 1 \bmod 4$ for which $\left(\frac{p}{q}\right) = -1$.

(2) If s and t are any two prime factors of m distinct from p and $\equiv 3 \bmod 4$ then $\left(\frac{p}{s}\right) = \left(\frac{p}{t}\right)$.

Proof: Since m is a quadratic residue mod p, $x^2 = m + kp$ for some x and k and we may assume $p \nmid k$. For if $p|k$ then $p \nmid x$ since otherwise we would have $p^2 | x^2$ whence $p^2 | m = x^2 - kp$, contradicting the fact that m is square-free. Thus if $p|k$, $(x+p)^2 = m + k'p$ where $k' = k + 2x + p$ is not divisible by p.

Hence p occurs to the first power in the norm $kp = N(x + \sqrt{m})$, and by proposition 1 at least one of

$a^2 - mb^2 = \pm p$, $\pm 4p$ is soluble. (The cases $\pm 4p$ occur when $m \equiv 1 \bmod 4$; for then $N(x + y\sqrt{m}) = x^2 - my^2$ where x and y are either integers or both halves of odd integers; in the latter case we multiply through by 4 to clear denominators). If $q \equiv 1 \bmod 4$ and $q|m$ we have $a^2 \equiv \pm p$, $\pm 4p \bmod q$ and since $\left(\frac{\pm 1}{q}\right) = \left(\frac{\pm 4}{q}\right) = 1$, the solubility of one of these congruences is equivalent to the solubility of $a^2 \equiv p \bmod q$. Hence $\left(\frac{p}{q}\right) \neq -1$.

Now let s and t be prime divisors of m distinct from p and $\equiv 3 \bmod 4$. If $a^2 - mb^2 = (4)p$ is soluble (where the factor 4 may or may not be present), we have $\left(\frac{p}{s}\right) = \left(\frac{p}{t}\right) = 1$; if $a^2 - mb^2 = -(4)p$ is soluble then $\left(\frac{-p}{s}\right) = \left(\frac{-p}{t}\right) = 1$, or since $s \equiv t \equiv 3 \bmod 4$, $\left(\frac{p}{s}\right) = \left(\frac{p}{t}\right) = -1$. Thus $\left(\frac{p}{s}\right) = \left(\frac{p}{t}\right)$ in any case.

For convenience we now restate two particular cases.

COROLLARY 1. ($m > 0$ simple). The case $p = 3$: Let $m \equiv 0$ or $1 \bmod 3$. Then

(1) m can have no prime factor $\equiv 5 \bmod 12$.

(2) If m has a prime factor $\equiv 7 \bmod 12$ then it has no prime factor $\equiv 11 \bmod 12$, and conversely.

COROLLARY 2. ($m > 0$ simple). The case $p = 5$: Let $m \equiv 0, 1$ or $4 \bmod 5$. Then

(1) m has no prime factor $\equiv 13$ or $17 \bmod 20$.

(2) If m has a prime factor $\equiv 3$ or $7 \bmod 20$ then it has no prime factor $\equiv 11$ or $19 \bmod 20$; and conversely.

Looking at the values $0 < m \leq 101$ one readily verifies that the following are not simple:

https://doi.org/10.4153/CMB-1962-017-5 Published online by Cambridge University Press

By proposition 4: 10, 15, 26, 30, 35, 39, 42, 55, 58, 70, 74, 78, 87, 91, 95;

By corollary 1: 10, 15, 30, 34, 51, 55, 58, 70, 82, 85, 87;

By corollary 2: 26, 34, 39, 51, 65, 66, 74, 85, 91.

Complementing, the following m are possibly simple: 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, (79), 83, 86, 89, 93, 94, 97, 101; and in fact these are precisely the simple $m \leq 101$ with the single exception of 79; 79 is the only non-simple prime ≤ 101. (See [12], p. 355, in conjunction with the corrections noted in [3], p. 386.)

5. Cubic fields. Without aiming at complete generality, let us consider $Q(\theta)$ where θ is a zero of the irreducible cubic $x^2 + ax + b$, $a, b \in Z$. The discriminant of the polynomial is [13, p. 82]

$$d = d(\theta) = -4a^3 - 27b^2$$

and the discriminant of the field $Q(\theta)$ is

$$\Delta = \Delta(\theta) = \begin{vmatrix} w_1 & w_2 & w_3 \\ w_1^{(2)} & w_2^{(2)} & w_3^{(2)} \\ w_1^{(3)} & w_2^{(3)} & w_3^{(3)} \end{vmatrix}^2$$

where $\{w_1, w_2, w_3\}$ is an integral basis for J. (The definition of Δ for a field of any degree over Q is the obvious generalization of this formula.) It can be shown that $\Delta = f^2 d$ where $f = f(\theta) \in Z$ is called the conductor. Moreover it can be shown that the elements of J are all of the form $\alpha = r + s\theta + t\theta^2$ where $r, s, t \in Q$ and the denominators of r, s, t, when written in reduced form, are all divisors of f. (There are further restrictions on r, s, t.*)

* Cf. the quadratic case: there $f = 1$ or 2 and when $f = 2$ we were allowed denominators of 2 provided both the numerators were odd. Also $f = 2$ if and only if $m \equiv 1 \bmod 4$. There is no such simple criterion in the cubic case although the following facts are useful [3]: (i) $\Delta \geq 49$, or $\Delta \leq -23$; (ii) $\Delta \equiv 0$ or $1 \bmod 4$.

Without going into further detail we give the following consequence of proposition 1.

PROPOSITION 6. Let $Q(\theta)$ be simple; let $p > 2$ be a rational prime such that $p \equiv 2 \bmod 3$, $-3d$ is a quadratic residue mod p, and $p \nmid$ g.c.d. (a, b). Then p is a cubic residue mod q for every rational prime divisor q of g.c.d. (a, b) such that $q \nmid f$.

Proof: Noting that $\theta^{(1)} + \theta^{(2)} + \theta^{(3)} = 0$, $\theta^{(1)}\theta^{(2)} + \theta^{(2)}\theta^{(3)} + \theta^{(3)}\theta^{(1)} = a$, $\theta^{(1)}\theta^{(2)}\theta^{(3)} = -b$, direct calculation shows that

$$N(r+s\theta+t\theta^2) = (r+s\theta^{(1)}+t\theta^{(1)2})\,(r+s\theta^{(2)}+t\theta^{(2)2})\,(r+s\theta^{(3)}+t\theta^{(3)2})$$

$$= r^3-2ar^2t+ars^2+art^2-bs^3-abst^2+b^2t^3+3brst.$$

Hence $N(r-\theta) = r^3+ar+b$.

Now the conditions on p ensure the solubility of $x^3 + ax + b \equiv 0 \bmod p$. For by Cardan's formula [13] we must first be able to extract the square root $\sqrt{-3d}$; that is, $-3d$ must be a quadratic residue mod p. Secondly, we must be able to extract two certain cube roots. But since $p \equiv 2 \bmod 3$ all residues mod p are cubic residues so that every residue has a unique cube root.

Thus $x^3 + ax + b \equiv 0 \bmod p$ is soluble and we wish to show that it has a non-repeated root $x = r$, i.e., one for which the derivative $3r^2 + a \not\equiv 0$. Clearly this is true if there is just one root. If there are three roots and every root is repeated we have $x^3 + ax + b \equiv (x - r)^3$ whence $0 \equiv -3r$, $a \equiv 3r^2$, $b \equiv -r^3$, and since $p \neq 3$, $a \equiv b \equiv 0$; but this contradicts $p \nmid$ g.c.d. (a, b).

Thus for some r we have $r^3 + ar + b = kp$, $p \nmid (3r^2 + a)$. We may assume $p \nmid k$; for if $p \mid k$ replace r by $r + p$ to get a new k not divisible by p: $(r + p)^3 + a(r + p) + b = p(k + 3r^2 + a + 3rp + p^2) = pk'$, $p \nmid k'$. Hence p occurs to the first power in the norm $N(r - \theta) = r^3 + ar + b = kp$ and by proposition 1, $N\pi = N(r' + s'\theta + t'\theta^2) = p$ is soluble. (Since $N(-\alpha) = -N(\alpha)$ we need consider only the positive sign.) Now

https://doi.org/10.4153/CMB-1962-017-5 Published online by Cambridge University Press

$q|a$, $q|b$, $q \nmid f$ so that $N\pi \equiv r'^3 \equiv p \bmod q$ where $r' = u/v$, $u, v \in Z$ and $q \nmid v$. This implies that $x^3 \equiv p \bmod q$ is soluble and that p is a cubic residue mod q. Q. E. D.

In the important case $a = 0$ we can give a more specific result. Since $\sqrt[3]{-b} = -\sqrt[3]{b}$ and $Q(-\sqrt[3]{b}) = Q(\sqrt[3]{b})$, we may restrict ourselves to $Q(\sqrt[3]{b})$ where b is a positive cube-free integer. Write $b = hk^2$ where hk is square-free. Then an integral basis for J is ([8], vol. 2, p. 104):

$$\{1, \alpha = \sqrt[3]{hk^2}, \beta = \sqrt[3]{h^2k}\} \quad \text{if } 9 \nmid (h^2 - k^2),$$

and $\{\gamma = \frac{1}{3}(1 + h\alpha + k\beta), \alpha, \beta\}$ if $9 \mid (h^2 - k^2)$.

Thus the only prime occurring in a denominator is 3.

COROLLARY: If $Q(\sqrt[3]{b})$ is simple then b has no prime factor $\equiv 1 \bmod 3$.

Proof: The only properties of q used in the preceeding proof were $q|$g. c. d. (a, b) and that q does not occur in a denominator. Thus all we require of q here is that $q|b$ and $q \not\equiv 3$. Thus suppose $q \equiv 1 \bmod 3$ and $q|b$. If $p \nmid b$ and $p \equiv 2 \bmod 3$, by the proposition p is a cubic residue mod q. But only one third of the residues mod q are cubic residues and we will have the required contradiction if we can show that a $p \equiv u \bmod q$ exists for any $u \not\equiv 0 \bmod q$. This follows from the fact that g. c. d. $((2 - u)q + u, q) = 1$ so that there are infinitely many primes in the progression

$$\begin{aligned} p &= 3qx + (2 - u)q + u, \quad x = 1, 2, 3, \ldots \\ &\equiv 2 \bmod 3, \quad \equiv u \bmod q. \end{aligned}$$

For example, $Q(\sqrt[3]{7})$ is not simple. See [10] for a table of data relating to cubic fields.

7. An inequality for the class number. Here we must assume a knowledge of ideal theory and the definition of the class number $h = h(\theta)$ of $Q(\theta)$; ($Q(\theta)$ is simple if and only if $h = 1$). Our reason for including this section in the present note, which up till now has been on a completely elementary level, is that

https://doi.org/10.4153/CMB-1962-017-5 Published online by Cambridge University Press

proposition 1 which gave criteria for $h > 1$ is susceptible of a rather obvious generalization which gives criteria for $h > 2$, $h > 3$, etc. We recall that $n = (Q(\theta):Q)$; $\{w_1, \ldots, w_n\}$ will denote an integral basis.

PROPOSITION 7. Let the rational prime p split completely in $Q(\theta)$ and let $p^{s_o} > 1$ be the minimum power of p such that

$$N(a_1 w_1 + \ldots + a_n w_n) = \pm p^{s_o}, \quad \text{g.c.d.}\{a_i\} = 1 .$$

Then $h \geq s_o$ and if $n = 2$, $s_o | h$.

Proof: We have

$$(p) = \wp_1 \wp_2 \ldots \wp_n$$

where no two of the prime ideals $\wp_i$ are equal. Taking norms,

$$p^n = N\wp_1 N\wp_2 \ldots N\wp_n$$

so that

$$N\wp_1 = N\wp_2 = \ldots = N\wp_n = p .$$

Let $\wp$ be one of the $\wp_i$ and let

$$\wp^s = (\beta) = (b_1 w_1 + \ldots + b_n w_n)$$

be the least power of $\wp$ which is principal. Then $\wp, \wp^2, \ldots, \wp^s \sim (1)$ give rise to distinct classes and the class group has a subgroup of order s ; hence $s|h$. If $g = \text{g.c.d.}\{b_i\}$ and $b_i = gc_i$, taking norms we have $N\wp^s = p^s = g^n N(c_1 w_1 + \ldots)$ and therefore $g = 1$ or $g = p$. If $g = p$, $\wp^s = (p)(c_1 w_1 + \ldots)$ contradicting $(p) = \wp_1 \ldots \wp_n$. Thus $g = 1$, $N\beta = \pm p^s$ and by the definition of s_o we have $s_o \leq s \leq h$.

Now let $n = 2$. The only prime ideals whose norms are powers of p are $\wp_1$ and $\wp_2$. Hence

https://doi.org/10.4153/CMB-1962-017-5 Published online by Cambridge University Press

$$(\alpha) = (a_1w_1 + a_2w_2) = \wp_1^{t_1}\,\wp_2^{t_2}\ , \quad (p) = \wp_1\,\wp_2$$

where we may assume $t_1 \geq t_2 \geq 0$. Thus $(\alpha) = (p)^{t_2}\wp_1^{t_1-t_2}$ and

$$((a_1w_1 + a_2w_2)/p^{t_2}) = \wp_1^{t_1-t_2}$$

is an integral ideal so that $(a_1w_1 + a_2w_2)/p^{t_2}$ must be an integer. Hence $t_2 = 0$, $(\alpha) = \wp_1^{t_1}$ and therefore $t_1 \geq s$. Taking norms, $p^{s_o} = p^{t_1}$ so that $s_o = t_1 \geq s$; from above $s_o \leq s$; thus $s_o = s$ and since $s|h$, $s_o|h$.

We now give only the simplest corollaries which relate to $Q(\sqrt{m})$, $m < 0$.

COROLLARY 1. Let $m < 0$, $m \equiv 1 \bmod 4$ and let p be the smallest rational prime such that* $\left(\frac{m}{p}\right) = 1$. Then $h(\sqrt{m}) > \frac{\log(-m/4)}{\log p}$.

Proof: The condition $\left(\frac{m}{p}\right) = 1$ means that p splits in $Q(\sqrt{m})$. Solving $a^2 + |m|b^2 = p^{s_o}$ or $4p^{s_o}$ for minimal s_o with g.c.d.$(a,b) = 1$, we see that $b \neq 0$ and $p^{s_o} \geq (|m|+1)/4$. Thus

$$h \geq s_o \geq \frac{\log\{(|m| + 1)\ 4\}}{\log p} > \frac{\log(-m\ \ 4)}{\log p} .$$

COROLLARY 2. Let $m < 0$ and $m \equiv 1 \bmod 4$ and let p be the smallest rational prime > 2 such that $\left(\frac{m}{p}\right) = 1$. Then $h(\sqrt{m}) > (\log|m|)/\log p$.

* $\left(\frac{m}{2}\right) = (-1)^{(m^2-1)/8}$; as usual, m is assumed square-free.

Proof: We must exclude $p = 2$ since it is now ramified. Again p splits and solving $a^2 + |m|b^2 = p^{s_0}$ we see $p^{s_0} > |m|$ (strict inequality since $\left(\frac{m}{p}\right) \neq 0$, i.e., $p \nmid m$) and the result follows.

Since $\left(\frac{m}{2}\right) = 1$ if $m = 1 \bmod 8$, $h \to \infty$ as $m \to -\infty$ through values $\equiv 1 \bmod 8$, by corollary 1. Similarly corollary 2 gives various arithmetical progressions of m such that $h \to \infty$. Thus

COROLLARY 3. $h(\sqrt{m})$ is unbounded as $m \to -\infty$.

This result is obviously not deep and is not to be compared with Heilbronn's theorem [5] that $h \to \infty$ as $m \to -\infty$ (through all values).

* * *

The author would like to thank Doctors J. Lambek, C. Riehm, and D. Sussman for their help during the preparation of this note.

REFERENCES

1. G. Frobenius, Über quadratische Formen, die viele Primzahlen darstellen, Sitz. Akad. Wissen., Berlin, 1912, pp. 966-80,

2. H. Hancock, Foundations of the theory of algebraic numbers, 2 vols., 1931.

3. H. Hasse, Zahlentheorie, 1949.

4. ________, Vorlesungen über Zahlentheorie, 1950.

5. H. Heilbronn, On the class number in imaginary quadratic fields, Quart. J. Math., Oxford, 1934, pp. 150-60.

6. ________, and E.H. Linfoot, On the imaginary quadratic corpora of class number one, Quart. J. Math., Oxford, 1934, pp. 293-301.

7. D.H. Lehmer, On imaginary quadratic fields whose class number is unity, Bull. Amer. Math. Soc., 1933, p. 360.

8. W.J. Leveque, Topics in number theory, 2 vols., 1956.

9. H. Pollard, The theory of algebraic numbers, Carus monograph no. 9, Math. Assoc. Amer., 1950.

10. L.W. Reid, A table of class numbers for cubic number fields, Amer. J. Math., 1901, pp. 68-84.

11. ________, The elements of the theory of algebraic numbers, 1910.

12. J. Sommer, Vorlesungen über Zahlentheorie, 1907.

13. B.L. van der Waerden, Modern algebra, vol. 1 (revised English translation), 1953.

14. H. Weyl, Algebraic theory of numbers, Annals of Math. studies, no. 1, 1940.

McGill University

https://doi.org/10.4153/CMB-1962-017-5 Published online by Cambridge University Press