COLLOQUIUM MATHEMATICUM

VOL. LIX 1990 FASC. 1

LENGTHS OF IRREDUCIBLE FACTORIZATIONS IN FIELDS WITH SMALL CLASS NUMBER

BY

DAISY C. McCOY AND CHARLES J. PARRY (BLACKSBURG, VIRGINIA)

1. Introduction. Every nonzero integer of an algebraic number field has a unique factorization into irreducible elements if and only if the field has class number 1. Carlitz [2] has shown that the number of irreducible factors occurring in a factorization is unique if and only if the class number of the field is less than or equal to 2. For fields of class number greater than 2, Narkiewicz [3], Narkiewicz and Śliwa [4], and Allen and Pleasants [1] have obtained asymptotic estimates for the number of different lengths of irreducible factorizations. In this article we obtain explicit formulas for the number of different lengths of irreducible factorizations of an algebraic integer, when the ideal class group of the field has Davenport constant at most four.

2. Notation and terminology.

K: an algebraic number field.

β: nonzero, nonunit integer of K.

$l(\beta)$: number of different lengths of factorizations of β into irreducible elements, where the length of an irreducible factorization is the number of irreducible factors.

h: class number of K.

H: ideal class group of K.

X_i $(0 \leqslant i < h)$: ideal classes of K, where X_0 denotes the principal class.

$o(X_i)$: order of the class X_i.

$\Omega_i(\beta)$: number of prime ideals (counting multiplicities) in X_i which divide β.

$s = \Omega(\beta)$: number of prime ideals (counting multiplicities) which divide β.

$(\beta) = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_s$: factorization of (β) into prime ideals.

$[\mathfrak{p}_i]$: the ideal class of $\mathfrak{p}_i$.

$S = S(\beta)$: the sequence $[\mathfrak{p}_1], [\mathfrak{p}_2], \ldots, [\mathfrak{p}_s]$ of ideal classes determined by β.

Block: a finite sequence of elements of H whose product is X_0.

Block product: if $B = X_0^{b_0}X_1^{b_1}\ldots X_{h-1}^{b_{h-1}}$ and $C = X_0^{c_0}X_1^{c_1}\ldots X_{h-1}^{c_{h-1}}$ are blocks and b_i, c_i are nonnegative integers, then

$$BC = X_0^{b_0+c_0}X_1^{b_1+c_1}\ldots X_{h-1}^{b_{h-1}+c_{h-1}}.$$

Irreducible block: a block which cannot be written as a product of two subblocks.

$D(H)$: the *Davenport constant* of H; i.e., the maximum length of an irreducible block of H.

R: the free commutative semigroup generated by the set of all irreducible blocks of H; the elements of R can be represented as formal linear polynomials $\sum a_i B_i$, where each a_i is a nonnegative integer and B_i ranges over all the irreducible blocks of H.

$w(F)$: if $F \in R$, the *weight* $w(F)$ of F is the sum of the coefficients of F.

3. Preliminary results. Some general observations are made in this section, which apply to any number field K.

LEMMA I. *If* $\beta = \beta_0 \beta_1$, *where* $\Omega_i(\beta_0) = 0$ *for* $1 \leqslant i < h$ *and* $\Omega_0(\beta_1) = 0$, *then* $l(\beta) = l(\beta_1)$.

Proof. Since every prime ideal factor of β_0 is principal, the number of irreducible elements in any factorization of β_0 is $\Omega_0(\beta_0)$. Hence $l(\beta_0) = 1$ and $l(\beta) = l(\beta_1)$.

In view of Lemma I, for the remainder of the article we will assume that $\Omega_0(\beta) = 0$.

There is an obvious one-to-one correspondence between the set of all partitions of S into irreducible blocks and a subset R' of R. The coefficient of an irreducible block B of an F in R' is precisely the number of times the block B occurs in the given partition of S.

LEMMA II. *If F belongs to R' and some terms*

$$G = \sum_{i=1}^{m} b_i B_i$$

of F are replaced with the terms

$$G' = \sum_{j=1}^{m} c_j C_j$$

in R subject to the condition that

$$\prod_{i=1}^{m} B_i^{b_i} = \prod_{j=1}^{n} C_j^{c_j},$$

then the polynomial F' obtained by this substitution also belongs to R'.

Proof. Since F corresponds to a partition of S into irreducible blocks, the product condition insures that F' also corresponds to a partition of S. Thus F' belongs to R'.

The substitution of Lemma II can be considered as a transformation on R'. The notation

$$T\Big(\sum_{i=1}^{m} b_i B_i\Big) = \sum_{j=1}^{m} c_j C_j$$

will be used to denote such transformations.

LEMMA III. *The number of different weights of elements of R' is precisely $l(\beta)$.*

Proof. For any F in R', $w(F)$ is precisely the number of irreducible elements in the factorization of β determined by the partition of S corresponding to F.

Each element F of R' determines a solution to the Diophantine equation

$$(*) \qquad 2y_1+3y_2+\ldots+Dy_{D-1}=s,$$

where y_i is the number of irreducible blocks of length $i+1$ which occur in F and $D=D(H)$. A nonnegative integral solution to $(*)$ will be called an *admissible solution* if it is determined by some F in R'.

LEMMA IV. *$l(\beta)$ is precisely the number of distinct sums of the form $y_1+y_2+\ldots+y_{D-1}$, where $y_1,\ldots,y_{D-1}$ run through the set of admissible solutions to $(*)$.*

Proof. Each F in R' gives an admissible solution to $(*)$ with

$$w(F)=y_1+\ldots+y_{D-1}.$$

Conversely, any admissible solution with $y_1+\ldots+y_{D-1}=t$ corresponds to an F in R' with $w(F)=t$. The result follows from Lemma III.

4. Class groups of order 3 and 4. When H has order 3 or 4, it is shown that $l(\beta)$ is a linear function of $m=\min\{\Omega_i(\beta)\}$ such that $X_i\in H$ has maximum order.

LEMMA V. *If $H=Z_3$, then $l(\beta)$ is the number of solutions to $3x+2y=s$ with $0\leqslant x$ and $0\leqslant y\leqslant m$.*

Proof. The irreducible blocks of H are X_i^3 $(i=1,2)$ and X_1X_2. Hence the number of irreducible blocks of length 2 in any partition of $S(\beta)$ is at most m. Thus $l(\beta)$ is bounded from above by the number of solutions to the equation satisfying the inequalities.

Conversely, let x, y be a solution to the equation which satisfies the inequalities. Since (β) is a principal ideal,

$$\Omega_1(\beta)+2\Omega_2(\beta)\equiv 0 \pmod 3.$$

Thus

$$\Omega_1(\beta)\equiv\Omega_2(\beta)\equiv m \pmod 3,$$

and so

$$2y\equiv s\equiv \Omega_1(\beta)+\Omega_2(\beta)\equiv 2m \pmod 3.$$

Hence

$$F=\tfrac{1}{3}(\Omega_1(\beta)-y)X_1^3+\tfrac{1}{3}(\Omega_2(\beta)-y)X_2^3+yX_1X_2$$

is in R' and corresponds to the solution x, y. Since distinct solutions to $(*)$ give distinct values of $x+y$, the result follows from Lemma IV.

LEMMA VI. *If $H=Z_2\times Z_2$, then $l(\beta)$ is the number of solutions to $3x+2y=s$ with $0\leqslant x\leqslant m$ and $0\leqslant y$.*

Proof. Here the irreducible blocks are X_i^2 $(i = 1, 2, 3)$ and $X_1X_2X_3$. Since x denotes the number of irreducible blocks of length 3 in any partition of S, it is clear that $x \leqslant m$. The remainder of the proof is similar to that of Lemma V.

THEOREM VII. *If* $H = Z_3$, *then*

$$l(\beta) = \frac{m+\varepsilon}{3}, \quad \textit{where } \varepsilon \equiv s \pmod 3 \textit{ and } 1 \leqslant \varepsilon \leqslant 3.$$

Proof. If $3x+2y = s$, then

$$y \equiv 2s \pmod 3,$$

so $y = 2s-3t$ for some integer t, and so $x = 2t-s$. It follows from Lemma V that

$$\frac{2s-m}{3} \leqslant t \leqslant \frac{2s}{3} \quad \text{and} \quad \frac{s}{2} \leqslant t.$$

But $s/2 \leqslant (2s-m)/3$. Note that

$$2s-m \equiv 0 \pmod 3$$

and that

$$2s \equiv 3-\varepsilon \pmod 3 \quad \text{with } 0 \leqslant 3-\varepsilon \leqslant 2,$$

so that

$$t \leqslant \frac{2s-3+\varepsilon}{3} = \frac{2s+\varepsilon}{3} - 1.$$

By Lemma V,

$$l(\beta) = \frac{2s+\varepsilon}{3} - 1 - \frac{2s-m}{3} + 1 = \frac{m+\varepsilon}{3}.$$

THEOREM VIII. *If* $H = Z_2 \times Z_2$, *then*

$$l(\beta) = \frac{m+\varepsilon}{2}, \quad \textit{where } \varepsilon \equiv s \pmod 2 \textit{ and } \varepsilon = 1 \textit{ or } 2.$$

Proof. As in the preceding proof, $y = 2s-3t$ and $x = 2t-s$. From Lemma VI,

$$\frac{s}{2} \leqslant t \leqslant \frac{s+m}{2} \quad \text{and} \quad t \leqslant \frac{2s}{3},$$

but $(s+m)/2 \leqslant 2s/3$. Since (β) is a principal ideal,

$$\Omega_1(\beta) + \Omega_3(\beta) \equiv \Omega_2(\beta) + \Omega_3(\beta) \equiv 0 \pmod 2,$$

so

$$\Omega_1(\beta) \equiv \Omega_2(\beta) \equiv \Omega_3(\beta) \equiv m \pmod 2.$$

In particular, $s \equiv m \pmod 2$. Note that

$$s \equiv 2-\varepsilon \pmod 2 \quad \text{with } 2-\varepsilon = 0 \text{ or } 1,$$

so that

$$t \geqslant \frac{s+2-\varepsilon}{2} = \frac{s-\varepsilon}{2} + 1.$$

By Lemma VI,

$$l(\beta) = \frac{s+m}{2} - \left(\frac{s-\varepsilon}{2}+1\right)+1 = \frac{m+\varepsilon}{2}.$$

We now consider the case $H = Z_4$. Number the ideal classes so that $o(X_1) = o(X_3) = 4$ and $o(X_2) = 2$. Let

$$\Omega_1(\beta) = k, \quad \Omega_2(\beta) = l \quad \text{and} \quad \Omega_3(\beta) = m.$$

With no loss of generality, we may assume that $k \geqslant m$.

LEMMA IX. *If* $H = Z_4$, *then* $l(\beta) \leqslant [m/2]+1$.

Proof. By Lemma IV, $l(\beta)$ is bounded by the number of solutions to

$$4x+3y+2z = s$$

which give distinct values for $x+y+z$. Since $y \equiv s \pmod 2$, $y = s-2u$ for some integer u and

$$2x+z = -s+3u,$$

so

$$z \equiv s+u \pmod 2.$$

Thus

$$z = s+u-2v \quad \text{and} \quad x = -s+u+v,$$

so

$$x+y+z = s-v.$$

Since the irreducible blocks of H are X_i^4 $(i = 1, 3)$, $X_i^2X_2$ $(i = 1, 3)$, X_1X_3 and X_2^2, in any partition of $S(\beta)$ the l X_2 terms occur either as singletons in blocks of length 3 or as pairs in blocks of length 2. Thus $l \leqslant y+2z$, so $v \leqslant (3s-l)/4$. On the other hand,

$$\begin{aligned} z &\leqslant m+\tfrac{1}{2}\,(\text{number of } X_2\text{'s not used in blocks of length 3}) \\ &= m+\tfrac{1}{2}(l-y). \end{aligned}$$

Thus

$$y+2z \leqslant l+2m,$$

and hence

$$\frac{3s-l}{4}-\frac{m}{2} \leqslant v \leqslant \frac{3s-l}{4}.$$

Thus there are at most $[m/2]+1$ distinct values of $x+y+z$, where x, y, z is a solution to (*). This gives the desired bound for $l(\beta)$.

THEOREM X. *If* $H = Z_4$, *then*

$$l(\beta) = \begin{cases} [m/2]+1 & \text{if } l > 0, \\ [m/4]+1 & \text{if } l = 0. \end{cases}$$

Proof. First suppose that $l > 0$. Since (β) is a principal ideal,

$$k+2l+3m \equiv 0 \pmod 4,$$

so $k \equiv m \pmod 2$. Also,

$$k \equiv m+2l \pmod 4 \quad \text{and} \quad s = k+l+m \equiv l \pmod 2.$$

Let $m \equiv \varepsilon \equiv 2\varepsilon_1+\varepsilon_0 \pmod 4$ with $0 \leqslant \varepsilon \leqslant 3$ and $0 \leqslant \varepsilon_0,\ \varepsilon_1 \leqslant 1$. Set

$$v = \frac{3s-l-2\varepsilon_0}{4}$$

and note that

$$\begin{aligned} 4v = 3s-l-2\varepsilon_0 &= 3k+2l+3m-2\varepsilon_0 \\ &\equiv 2(m-\varepsilon_0) \equiv 0 \pmod 4, \end{aligned}$$

so that v is an integer. First, we assume that l (and hence s) is even, so $u = s/2-\varepsilon_1$ is an integer. Using the equations given in the proof of Lemma IX, we obtain

$$x = \left(\frac{k-\varepsilon}{4}\right)+\left(\frac{m-\varepsilon}{4}\right),$$

$$y = 2\varepsilon_1, \qquad z = \frac{l+2\varepsilon_0}{2}-\varepsilon_1.$$

An element of R' corresponding to this solution is

$$F = \left(\frac{k-\varepsilon}{4}\right)X_1^4+\left(\frac{m-\varepsilon}{4}\right)X_3^4+\varepsilon_1X_1^2X_2+\varepsilon_1X_3^2X_2+\left(\frac{l}{2}-\varepsilon_1\right)X_2^2+\varepsilon_0X_1X_3.$$

Since we will need a cubic term with positive coefficient, if $\varepsilon_1 = 0$ apply the transformation

$$T_0(X_1^4+X_2^2) = 2X_1^2X_2$$

to F, giving the polynomial F'. Note that $w(F) = w(F')$.

Define the following transformations on R:

$$T_1(X_1^4+X_3^2X_2) = X_1^2X_2+2X_1X_3,$$

$$T_2(X_3^4+X_1^2X_2) = X_3^2X_2+2X_1X_3,$$

$$T_3(X_1^2X_2+X_3^2X_2) = 2X_1X_3+X_2^2.$$

Note that each T_i increases the weight of a polynomial by 1. Assume for the moment that either $\varepsilon_1 = 1$ or $k > m$. Apply T_2 followed by T_1 to F (F' if $\varepsilon_1 = 0$) $(m-\varepsilon)/4$ times. Then apply T_3 ε_1 times. Since each T_i increases the weight by 1,

$$l(\beta) \geqslant 2\left(\frac{m-\varepsilon}{4}\right)+\varepsilon_1+1 = \frac{m-\varepsilon_0}{2}+1 = \left[\frac{m}{2}\right]+1.$$

If $k = m$ and $\varepsilon_1 = 0$, apply T_2 followed by T_1 to F' $(m-\varepsilon)/4-1$ times, apply T_2 one additional time, and then apply T_3 $\varepsilon_1+1 = 1$ time. As above,

$$l(\beta) \geqslant 2\left(\frac{m-\varepsilon}{4}-1\right)+1+\varepsilon_1+1+1 = \left[\frac{m}{2}\right]+1.$$

Now, assume that l, and hence s, are odd. Note that

$$k \equiv m+2 \equiv 2(1-\varepsilon_1)+\varepsilon_0 \pmod 4$$

with $0 \leqslant 2(1-\varepsilon_1)+\varepsilon_0 \leqslant 3$. Set

$$u = \frac{s-1}{2} \quad \text{and} \quad v = \frac{3s-l-2\varepsilon_0}{4},$$

so

$$\begin{aligned} x &= \frac{k+m-2-2\varepsilon_0}{4} = \frac{k+m-(2-2\varepsilon_1+\varepsilon_0+2\varepsilon_1+\varepsilon_0)}{4} \\ &= \frac{k-(2(1-\varepsilon_1)+\varepsilon_0)}{4}+\frac{m-\varepsilon}{4} = \frac{k+4\varepsilon_1-(\varepsilon+2)}{4}+\frac{m-\varepsilon}{4}, \end{aligned}$$

$$y = 1, \quad z = \frac{l-1+2\varepsilon_0}{2}.$$

An element of R corresponding to this solution is

$$F = \left(\frac{k+4\varepsilon_1-(\varepsilon+2)}{4}\right)X_1^4+\left(\frac{m-\varepsilon}{4}\right)X_3^4+(1-\varepsilon_1)X_1^2X_2+\varepsilon_1X_3^2X_2 +\left(\frac{l-1}{2}\right)X_2^2+\varepsilon_0X_1X_3.$$

Apply T_1 followed by T_2 or T_2 followed by T_1, according as $\varepsilon_1 = 1$ or 0, to F $(m-\varepsilon)/4$ times. Apply T_1 ε_1 times, obtaining

$$l(\beta) \geqslant 2\left(\frac{m-\varepsilon}{4}\right)+\varepsilon_1+1 = \left[\frac{m}{2}\right]+1.$$

The first result is now immediate from Lemma IX.

Now assume that $l = 0$. Here $s = k+m$ with $k \equiv m \pmod 4$. Moreover, any admissible solution of the Diophantine equation $4x+3y+2z = s$ must have $y = 0$. The Diophantine equation reduces to

$$2x+z = \frac{k+m}{2}$$

which has solution $z = (k+m)/2-2x$ with $0 \leqslant z \leqslant m$. Hence

$$(k-m)/4 \leqslant x \leqslant (k+m)/4.$$

However, each admissible solution must correspond to an element of R' of the form

$$aX_1^4+bX_3^4+cX_1X_3$$

with $x = a+b$ and $z = c$. Therefore, $4b+c = m$, so

$$z = c \equiv m \pmod 4.$$

Thus

$$2x = \frac{k+m}{2}-z \equiv \frac{k-m}{2} \pmod 4 \quad \text{or} \quad x \equiv \frac{k-m}{4} \pmod 2.$$

Thus at most $[m/4]+1$ of the solutions to the Diophantine equation are admissible, so

$$l(\beta) \leqslant \left[\frac{m}{4}\right]+1.$$

On the other hand,

$$F = \left(\frac{k-\varepsilon}{4}\right)X_1^4+\left(\frac{m-\varepsilon}{4}\right)X_3^4+\varepsilon X_1X_3$$

corresponds to the solution

$$x = \frac{k+m-2\varepsilon}{4}, \qquad z = \varepsilon.$$

Let T_4 denote the transformation $T_4(X_1^4+X_3^4) = 4X_1X_3$. Note that T_4, which increases the weight of a polynomial by 2, can be applied to F $(m-\varepsilon)/4$ times. Hence

$$l(\beta) \geqslant \frac{m-\varepsilon}{4}+1,$$

and so equality must hold.

5. Elementary class group of order 8. When H is an elementary abelian 2-group of rank 3, $D(H) = 4$ (see [5]), so the Diophantine equation becomes

$$(**) \qquad 4x+3y+2z = s.$$

Here, it will be shown that $l(\beta)$ is a linear function in x_0 and y_0, where (x_0, y_0, z_0) is an admissible solution to $(**)$ with $x = x_0$ maximal and $y = y_0$ maximal subject to $x = x_0$.

Each element of H has a unique expression in the form

$$X_\alpha = X_1^i \times X_2^j \times X_3^k \qquad \text{with } 0 \leqslant i, j, k \leqslant 1,$$

where X_1, X_2 and X_3 generate H. Denote α using the 3 digits $1\cdot i$, $2\cdot j$, $3\cdot k$, and then omit any zero digits. Thus, for example,

$$X_{13} = X_1 \times X_2^0 \times X_3.$$

There are 21 irreducible blocks of H, 7 of each length 2, 3, and 4. Those of length 2 are simply the squares of the non-identity elements of H. The irreducible blocks of length 3 and 4 are

$$X_1X_2X_{12},\ X_1X_3X_{13},\ X_1X_{23}X_{123},\ X_2X_3X_{23},\ X_2X_{13}X_{123},\ X_3X_{12}X_{123},$$
$$X_{12}X_{13}X_{23},\ X_1X_2X_3X_{123},\ X_1X_2X_{13}X_{23},\ X_1X_3X_{12}X_{23},$$
$$X_1X_{12}X_{13}X_{123},\ X_2X_3X_{12}X_{13},$$
$$X_2X_{12}X_{23}X_{123}, \quad \text{and} \quad X_3X_{13}X_{23}X_{123}.$$

Let $k_\alpha = \Omega(X_\alpha)$. Since any three non-identity elements, not contained in a proper subgroup, generate H, we may choose X_1 and X_2 so that $k_1 \leqslant k_2 \leqslant k_\alpha$ for $\alpha \neq 1, 2$. Then choose $X_3 \neq X_{12}$ so that k_3 is minimal among the remaining k_α.

LEMMA XI. *Assume that* (x_0, y_0, z_0) *is an admissible solution to* (**) *with* $y = y_0$ *maximal for* $x = x_0$. *If* $x = x_1 = x_0 - 1$, $y = y_1$ *and* $z = z_1$ *is another admissible solution, then* $y_1 \leqslant y_0 + 2$.

Proof. Let F_1 in R' correspond to the solution (x_1, y_1, z_1). Suppose $y_1 > y_0 + 2$. If F_1 contains two different blocks of length 3, say $X_1X_2X_{12}$ and $X_1X_3X_{13}$, then applying

$$T_0(X_1X_2X_{12} + X_1X_3X_{13}) = X_2X_3X_{12}X_{13} + X_1^2$$

gives an F corresponding to an admissible solution with $x = x_0$ and $y = y_1 - 2 > y_0$, contradicting the choice of y_0. Hence we may assume that F_1 contains only one type of irreducible block of length 3, say $X_1X_2X_{12}$.

Suppose now that F_1 contains at least two types of square terms disjoint from $X_1X_2X_{12}$, say X_{13}^2 and X_{23}^2. Applying

$$T_1(X_1X_2X_{12} + X_{13}^2 + X_{23}^2) = X_1X_2X_{13}X_{23} + X_{12}X_{13}X_{23}$$

gives an admissible solution with $x = x_0$ and $y = y_1 > y_0$, again contradicting the choice of y_0. Therefore we may assume that F_1 contains at most one such square term, say X_{23}^2.

If F_1 contains the block $X_3X_{13}X_{23}X_{123}$, then applying

$$T_2(X_3X_{13}X_{23}X_{123} + X_1X_2X_{12}) = X_1X_2X_3X_{123} + X_{12}X_{13}X_{123}$$

yields an element of R' with two types of blocks of length 3 corresponding to the admissible solution (x_1, y_1, z_1) which was seen to give a contradiction.

Now suppose that F_1 contains the block X_{23}^2 and a block of length 4 which does not contain X_{23}, say $X_1X_2X_3X_{123}$. Applying

$$T_3(X_1X_2X_3X_{123} + 2X_1X_2X_{12} + X_{23}^2)$$
$$= X_2X_{12}X_{23}X_{123} + X_1X_3X_{12}X_{23} + X_1^2 + X_2^2$$

gives an admissible solution with $x = x_0$ and $y = y_1 - 2 > y_0$, again contradicting the maximality of y_0. Thus F_1 can contain only one type of block of length 3, one type of block of length 2 which is disjoint from the block of length 3, and no block of length 4 disjoint from either. Therefore, if F_1 contains an X_{23}^2 term, the only blocks of length 4 which can occur are

$$X_1X_2X_{13}X_{23},\quad X_1X_3X_{12}X_{23},\quad X_2X_{12}X_{23}X_{123}.$$

Since X_3, X_{13} and X_{123} can occur only in blocks of length 4, we have

$$x_1 = k_{13} + k_3 + k_{123}.$$

But every irreducible block of length 4 must contain at least one element of $\{X_{13}, X_3, X_{123}\}$, in particular,

$$x_0 \leqslant k_{13} + k_3 + k_{123} = x_1 = x_0 - 1.$$

Thus we may assume that F_1 contains no X_{23}^2 block as well as no $X_3X_{13}X_{23}X_{123}$ block.

Now every block of length 4 in F_1 contains exactly two of the elements X_3, X_{13}, X_{23} and X_{123}. Moreover, since these elements can occur only in blocks of length 4,

$$x_1 = \tfrac{1}{2}(k_3+k_{13}+k_{23}+k_{123}).$$

Label the irreducible blocks of length 4 as $A_1, \ldots, A_7$, and let a_i denote the maximum number of A_i which can occur in a partition of S. Then

$$\begin{aligned}
a_1+a_2+a_3+a_7 &\leqslant k_3,\\
a_3+a_4+a_5+a_7 &\leqslant k_{13},\\
a_2+a_4+a_6+a_7 &\leqslant k_{23},\\
a_1+a_5+a_6+a_7 &\leqslant k_{123},
\end{aligned}$$

where the blocks are labelled so that X_α for $\alpha \in \{3, 13, 23, 123\}$ occurs in block A_i if and only if a_i occurs in the inequality for k_α. Thus

$$2(a_1+\ldots+a_6+2a_7) \leqslant k_3+k_{13}+k_{23}+k_{123}.$$

In particular,

$$x_0 \leqslant a_1+\ldots+a_7 \leqslant \tfrac{1}{2}(k_3+k_{13}+k_{23}+k_{123}) = x_1,$$

a contradiction. Thus no F_1 can exist with $y_1 > y_0+2$.

Let $x = -s+u+v$, $y = s-2u$ and $z = s+u-2v$ be a parametrization of the solutions to (**) as in the proof of Lemma IX.

LEMMA XII. *Suppose $x = x_0$, $y = y_0$ and $z = z_0$ is an admissible solution to (**) with x_0 maximal and y_0 maximal with $x = x_0$. If $u = u_0$ and $v = v_0$ are the values of the parameters corresponding to this solution, then $v \leqslant v_0$ for all admissible solutions to (**).*

Proof. Let (x_1, y_1, z_1) be an admissible solution with $x_0-x_1 = t$. It follows from Lemma XI that $y_1 \leqslant y_0+2t$ so that

$$u_0-u_1 = \tfrac{1}{2}(y_1-y_0) \leqslant t.$$

Thus

$$t = x_0-x_1 = (u_0-u_1)+(v_0-v_1) \leqslant t+v_0-v_1,$$

and so $v_1 \leqslant v_0$.

LEMMA XIII. *If $x = x_1$, $y = y_1$ and $z = z_1$ is an admissible solution with z_1 maximal, then the corresponding $v = v_1$ is minimal for the set of all admissible solutions.*

Proof. Clearly,

$$z_1 \leqslant \sum_\alpha [k_\alpha/2] = \sigma.$$

Since (β) is principal,

$$\begin{aligned}
k_1+k_{12}+k_{13}+k_{123} &\equiv 0 \pmod 2,\\
k_2+k_{12}+k_{23}+k_{123} &\equiv 0 \pmod 2,\\
k_3+k_{13}+k_{23}+k_{123} &\equiv 0 \pmod 2,
\end{aligned}$$

and so, exactly 0, 3, 4 or 7 of the k_α are even (odd). Moreover, if exactly 3 or 4 of the k_α are odd, the corresponding X_α's form an irreducible block of length 3 or 4, respectively. If all 7 of the k_α are odd, then clearly they can be partitioned into one block of length 3 and one of length 4. Hence there exists an admissible solution with $x_1 \leqslant 1$, $y_1 \leqslant 1$ and $z_1 = \sigma$. Since $y_1 = s-2u_1$ and $x_1 = -s+u_1+v_1$ with x_1 and y_1 minimal, u_1 maximizes u and v_1 minimizes v.

LEMMA XIV. *Let $x = x_0$, $y = y_0$ and $z = z_0$ be the admissible solution to* (**) *with $x = x_0$ maximal and $y = y_0$ maximal with $x = x_0$. Let $x = x_1$, $y = y_1$ and $z = z_1$ be the admissible solution to* (**) *with z_1 maximal. Then*

$$l(\beta) \leqslant x_0 - x_1 + \frac{y_0 - y_1}{2} + 1.$$

Moreover, $x_1 \leqslant 1$, $y_1 \leqslant 1$ and $x_1 = 1$ exactly when 4 or 7 of the k_α are odd and $y_1 = 1$ exactly when 3 or 7 of the k_α are odd.

Proof. Let $f = x+y+z$, where $4x+3y+2z = s$. Then

$$f = \frac{s-y}{2} - x = s - v.$$

If (x, y, z) is an admissible solution to (**), then f is the weight of a corresponding F in R'. Now $l(\beta)$ is the number of weights of F in R'. Since $f = s-v$, the maximal and minimal weights are obtained when v is minimal and maximal, respectively. From Lemmas XII and XIII, these values are given by $v = v_1$ and $v = v_0$, respectively. Hence

$$l(\beta) \leqslant 1 + f_1 - f_0 = 1 + \frac{s-y_1}{2} - x_1 - \frac{s-y_0}{2} + x_0$$

$$= 1 + x_0 - x_1 + \frac{1}{2}(y_0 - y_1).$$

The exact values of x_1 and y_1 were determined in the proof of Lemma XIII.

In order to determine x_0 and y_0, we construct an element F in R' of the form

$$F = m_1A_1 + m_2A_2 + m_3A_3 + m_4B + n_1C_1 + n_2C_2 + n_3C_3,$$

where the A's, B's and C's represent blocks of length 4, 3 and 2, respectively. Choose the A_i and m_i as follows:

$$A_1 = X_1X_{12}X_{13}X_{123}, \quad m_1 = k_1, \quad A_2 = X_2X_{12}X_{23}X_{123}$$

and

$$m_2 = \min\{k_2, k_{12} - m_1, k_{123} - m_1\}.$$

If $m_2 = k_{123} - m_1$, then

$$A_3 = X_2X_3X_{12}X_{13} \quad \text{and} \quad m_3 = \min\{k_2 - m_2, k_3, k_{12} - (m_1 + m_2), k_{13} - m_1\},$$

otherwise
$A_3 = X_3X_{13}X_{23}X_{123}, \quad m_3 = \min\{k_3, k_{13}-m_1, k_{23}-m_2, k_{123}-(m_1+m_2)\}.$

The choice for B depends on m_2 and m_3 as follows:

If $m_2 = k_2$ and $m_3 = k_3$ or $m_3 = k_{123}-(m_1+m_2)$, then

$$B = X_{12}X_{13}X_{23}$$

and

$$m_4 = \min\{k_{12}-(m_1+m_2), k_{13}-(m_1+m_3), k_{23}-(m_2+m_3)\}.$$

If $m_2 = k_2$ and $m_3 = k_{13}-m_1$ or $m_3 = k_{23}-m_3$, then

$$B = X_3X_{12}X_{123}$$

and

$$m_4 = \min\{k_3-m_3, k_{12}-(m_1+m_2), k_{123}-(m_1+m_2+m_3)\}.$$

If $m_2 = k_{12}-m_1$ and $m_3 = k_{13}-m_1$ or $m_3 = k_{123}-(m_1+m_2)$, then

$$B = X_2X_3X_{23}$$

and

$$m_4 = \min\{k_2-m_2, k_3-m_3, k_{23}-(m_2+m_3)\}.$$

If $m_2 = k_{12}-m_1$ and $m_3 = k_{23}-m_2$ or $m_3 = k_3$, then

$$B = X_2X_{13}X_{123}$$

and

$$m_4 = \min\{k_2-m_2, k_{13}-(m_1+m_3), k_{123}-(m_1+m_2+m_3)\}.$$

If $m_2 = k_{123}-m_1$ and $m_3 = k_2-m_2$ or $m_3 = k_3$, then

$$B = X_{12}X_{13}X_{23}$$

and

$$m_4 = \min\{k_{12}-(m_1+m_2+m_3), k_{13}-(m_1+m_3), k_{23}-m_2\}.$$

If $m_2 = k_{123}-m_1$ and $m_3 = k_{12}-(m_1+m_2)$ or $m_3 = k_{13}-m_1$, then

$$B = X_2X_3X_{23}$$

and

$$m_4 = \min\{k_2-(m_2+m_3), k_3-m_3, k_{23}-m_2\}.$$

The C_i represent the remaining X_α in $S(\beta)$ which must occur in pairs.

LEMMA XV. *The polynomial F defined above has minimal weight in R'.*

Proof. In each case F corresponds to an admissible solution of $4x+3y+2z = s$ with x maximal and y maximal for the value of x. By Lemma XII, the corresponding $v = v_0$ is maximal. Since $w(F) = x+y+z = s-v$ is minimal when v is maximal, the result follows.

Set $\varepsilon_i \equiv m_i \pmod 2$, $\varepsilon_i = 0$ or 1 for $1 \leqslant i \leqslant 4$. By Lemma XIII,

$$F' = \varepsilon A + \varepsilon_4 B + \text{squares}$$

has maximal weight in R', where $\varepsilon = 1$ if exactly 4 or 7 of the k_α are odd and $\varepsilon = 0$ if exactly 4 or 7 of the k_α are even, $\varepsilon_4 = 1$ if exactly 3 or 7 of the k_α are odd and $\varepsilon_4 = 0$ if exactly 3 or 7 of the k_α are even.

LEMMA XVI. *Let F and F' be as above. If $k_{12} \neq 0$, then for any integer γ with $w(F) \leqslant \gamma \leqslant w(F')$ there exists an element F_1 in R' with $w(F_1) = \gamma$.*

Proof. Suppose there is a series of transformations, which when applied to F yields F'. If each of these transformations increases the weight by at most one, then there is an F_1 with $w(F_1) = \gamma$. Thus we must show that such a series exists.

First assume that $m_1 = m_2 = m_3 = 0$. Here $F = m_4 B + \text{squares}$. If $m_4 \leqslant 1$, then $F = F'$ and the lemma is trivially true. If $m_4 > 1$, then apply

$$T_4(2B) = C_1 + C_2 + C_3$$

$(m_4 - \varepsilon_4)/2$ times. Observe that each application of T_4 increases the weight by one.

Now suppose that at least two of m_1, m_2 and m_3 are positive, say $m_2 > 0$ and $m_1 > 0$ or $m_3 > 0$. Define

$$T_7(A_i + A_j) = A_{ij} + C + C';$$

e.g.,

$$T_7(A_1 + A_2) = X_1 X_2 X_{13} X_{23} + X_{12}^2 + X_{123}^2.$$

Note that $T_7(A_i + A_{ij}) = A_j + \text{squares}$ and that T_7 increases the weight by one. One sequence of transformations taking F to F' is as follows:

Apply T_7 to $A_1 + A_2$ and then to $A_1 + A_{12}$ $(m_1 - \varepsilon_1)/2$ times, followed by T_7 to $A_2 + A_3$ and then to $A_2 + A_{23}$ $(m_2 + \varepsilon_2)/2 - 1$ times, and finally apply T_7 to $A_2 + A_3$ and $A_3 + A_{23}$ $(m_3 - \varepsilon_3)/2$ times. This yields

$$F_2 = \varepsilon_1 A_1 + (2 - \varepsilon_2) A_2 + \varepsilon_3 A_3 + m_4 B + \text{squares}.$$

If $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = 0$, then $F_2 = 2A_2 + m_4 B + \text{squares}$ and this can be dealt with as in the case of exactly one of m_1, m_2 or m_3 being positive. Otherwise, at least one $\varepsilon_i \neq 0$ for some $i \leqslant 3$. Apply T_7 $\varepsilon_1 + \varepsilon_3 + 1 - \varepsilon_2$ more times yielding $F_3 = A + m_4 B + \text{squares}$, where A, the remaining block of length 4, depends on m_1, m_2, m_3. Next apply T_4 $(m_4 - \varepsilon_4)/2$ times yielding $F_4 = A + \varepsilon_4 B + \text{squares}$. If $\varepsilon_4 = 0$ or A and B are disjoint, then no further transformations are possible. Otherwise,

$$T_6(A + B) = B' + \text{squares}$$

can be applied one time. If $m_2 = 0$ and $m_1 > 0$, $m_3 > 0$, then interchanging A_2 and A_1 in the above sequence of transformations yields the desired result.

Now suppose that exactly one of m_1, m_2 or m_3 is not zero, call it m. Then

$$F = mA + m_4 B + \text{squares}.$$

If $m = m_3$ and $m_4 = 0$, then since $k_{12} > 0$, F contains an X_{12}^2 term, so the transformation

$$T_5(A_3 + X_{12}^2) = X_3 X_{12} X_{123} + X_{12} X_{13} X_{23}$$

can be applied. If $m_4 = 0$ and $m \neq m_3$, then $k_2 > 0$, so $k_\alpha > 0$ for $\alpha > 2$. If $m_1 \neq 0$, then apply

$$T_5(A_1 + X_{23}^2) = X_1 X_{23} X_{123} + X_{12} X_{13} X_{23} = B' + B.$$

If $m_2 \neq 0$, then apply

$$T_5(A_2 + X_{13}^2) = X_2 X_{13} X_{123} + X_{12} X_{13} X_{23} = B' + B.$$

Thus there is always a polynomial F_2 in R' such that $w(F) = w(F_2)$ and F_2 contains a block of length 3. In fact,

$$F_2 = (m - \varepsilon_5)A + (m_4 + \varepsilon_5)B + \varepsilon_5 B' + \text{squares},$$

where $\varepsilon_5 = 1$ if $m_4 = 0$ and $\varepsilon_5 = 0$ otherwise. Now suppose that A and B are not disjoint. We can apply $T_6(A+B) = B' + \text{squares}$ followed by $T_6(A+B') = B + \text{squares}$ for a total of $m - \varepsilon_5$ transformations. Next apply

$$T_4(2B) = C_1 + C_2 + C_3 \quad \text{and} \quad T_4(2B') = C_1' + C_2' + C_3'$$

as many times as necessary to get a polynomial F_3 with the coefficients of the B and B' terms to be 0 or 1. If $F_3 = B + B' + \text{squares}$, then by applying the inverse of T_5 we get $F_4 = A + \text{squares}$. Since T_5 does not change the weight of a polynomial, $w(F_3) = w(F_4) = w(F')$.

Now we must consider the case where the A and B are disjoint. This can occur only when

$$A = A_1 = X_1 X_{12} X_{13} X_{123} \quad \text{and} \quad B = X_2 X_3 X_{23}.$$

If $m_1 = 1$, then 4 or 7 of the k_α are odd and $x_0 = x_1 = 1$. Thus no transformation involving A will increase $w(F)$ and applying T_4 $(m_4 - \varepsilon_4)/2$ times will yield F' as in the case $m_1 = m_2 = m_3 = 0$. If $m_1 > 1$, then applying

$$T_2(A+B) = A_2 + B_1 = X_2 X_{12} X_{23} X_{123} + X_1 X_3 X_{13}$$

to F gives

$$F_2 = (m_1 - 1)A_1 + A_2 + (m_4 - 1)B + B_1 + \text{squares}.$$

This is similar to the case where at least two of m_1, m_2 or m_3 are positive.

THEOREM XVII. *If $k_{12} \neq 0$, then*

$$l(\beta) = m_1 + m_2 + m_3 + \frac{m_4 - \varepsilon_4}{2} + \delta,$$

where $\delta = 1$ if 0 or 3 of the k_α are odd and $\delta = 0$ if 4 or 7 of the k_α are odd.

If $k_{12} = 0$, then

$$l(\beta) = \frac{m_3 - \varepsilon_3}{2} + 1.$$

Proof. By Lemma XIV,

$$l(\beta) \leqslant x_0 - x_1 + \frac{y_0 - y_1}{2} + 1.$$

By Lemma XVI, factorizations of all lengths between $w(F)$ and $w(F')$ occur when $k_{12} \neq 0$ and equality holds. By our choice of F, $x_0 = m_1+m_2+m_3$ and $y_0 = m_4$. By Lemma XIV, $x_1 = 1$ when 4 or 7 of the k_α are odd and $x_1 = 0$ otherwise, so $\delta = 1-x_1$. Since $y_1 = \varepsilon_4$,

$$l(\beta) = m_1+m_2+m_3+\frac{m_4-\varepsilon_4}{2}+\delta.$$

Since $k_1 \leqslant k_2 \leqslant k_{12}$, $k_1 = k_2 = 0$ and $m_1 = m_2 = 0$ when $k_{12} = 0$. Also

$$B = X_{12}X_{13}X_{23},$$

so $m_4 = 0$. Thus $F = m_3A_3+\text{squares}$ and the only transformation possible is

$$T_8(2A_3) = \text{squares}.$$

T_8 increases the weight by two and can be applied $(m_3-\varepsilon_3)/2$ times. Thus there are $(m_3-\varepsilon_3)/2+1$ weights of polynomials in R'.

COROLLARY XVIII. *If $k_{12} \neq 0$, then $l(\beta) = 1$ if and only if one of the following is true*:

(a) *Either* 0 *or* 3 *of the k_α are odd, $k_1 = k_2 = k_3 = 0$ and* $\min\{k_{12}, k_{13}, k_{23}\} \leqslant 1$.

(b) *Exactly* 4 *of the k_α are odd, $k_1 = k_2 = 0$, $k_3 = 1$ and either $k_{13} = 1$ or $k_{23} = 1$.*

(c) *All* 7 *of the k_α are odd, $k_1 = k_2 = k_3 = 1$ and at least two of k_{12}, k_{13} or k_{123} are* 1.

Proof. (a) From Theorem XVII we have $l(\beta) = m_1+m_2+m_3+(m_4-\varepsilon_4)/2 +1$ when 0 or 3 of the k_α are odd. Thus, if $l(\beta) = 1$, $m_1 = m_2 = m_3 = 0$, and so $k_1 = k_2 = k_3 = 0$. Also

$$m_4 = \varepsilon_4 \quad \text{and} \quad B = X_{12}X_{13}X_{23},$$

so $\min\{k_{12}, k_{13}, k_{23}\} \leqslant 1$.

Conversely, if no k_α are odd with $k_1 = k_2 = k_3 = 0$, then m_4 is even and

$$\min\{k_{12}, k_{13}, k_{23}\} = 0.$$

Thus $m_1 = m_2 = m_3 = m_4 = 0$ and $l(\beta) = 1$. If exactly 3 of the k_α are odd and $k_1 = k_2 = k_3 = 0$, then

$$\min\{k_{12}, k_{13}, k_{23}\} = 1.$$

Thus $m_1 = m_2 = m_3 = 0$ and $m_4 = \varepsilon_4 = 1$, and so $l(\beta) = 1$.

(b) Here Theorem XVII shows that $l(\beta) = m_1+m_2+m_3+(m_4-\varepsilon_4)/2$. If $l(\beta) = 1$, then $m_1 = m_2 = 0$, $m_3 = 1$ and $m_4 = \varepsilon_4 = 0$. Since

$$A_3 = X_3X_{13}X_{23}X_{123} \quad \text{and} \quad B = X_{12}X_{13}X_{23},$$

it follows that $k_1 = k_2 = 0$, $k_3 = 1$ and $k_{13} = 1$ or $k_{23} = 1$. Conversely, the given conditions force $l(\beta) = 1$.

(c) As above, $l(\beta) = m_1+m_2+m_3+(m_4-\varepsilon_4)/2$. If $l(\beta) = 1$, then

$$F = A_1+B+\text{squares}.$$

Thus $k_1 = 1$. Because

$$A_1 = X_1X_{12}X_{13}X_{123} \quad \text{and} \quad m_2 = m_3 = 0,$$

at least two of k_{12}, k_{13} and k_{123} are one. Since $k_2 \leqslant k_3 \leqslant k_\alpha$ for $\alpha = 13$ or 123, $k_2 = k_3 = 1$. Conversely, the given conditions force $l(\beta) = 1$.

COROLLARY XIX. *If* $k_{12} = 0$, *then* $l(\beta) = 1$ *if and only if* $k_3 \leqslant 1$.

Proof. $l(\beta) = 1$ if and only if $m_3 = \varepsilon_3$. Since $k_1 = k_2 = 0$, $m_3 = k_3$ and $k_3 = 0$ or $k_3 = 1$. Conversely, suppose that $k_3 \leqslant 1$. Then $m_3 \leqslant 1$ and $m_3 = \varepsilon_3$.

REFERENCES

[1] S. Allen and P. A. B. Pleasants, *The number of different lengths of irreducible factorization of a natural number in an algebraic number field*, Acta Arith. 36 (1980), pp. 59–86.

[2] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. 11 (1960), pp. 391–392.

[3] W. Narkiewicz, *On algebraic number fields with non-unique factorization*, Colloq. Math. 12 (1964), pp. 59–68.

[4] — and J. Śliwa, *Normal orders for certain functions associated with factorizations in number fields*, ibidem 38 (1978), pp. 323–328.

[5] J. E. Olson, *A combinatorial problem on finite abelian groups*, J. Number Theory 1 (1969), pp. 8–10.

DEPARTMENT OF MATHEMATICS
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
BLACKSBURG, VA 24061, U.S.A.

Reçu par la Rédaction le 28.4.1988;
en version modifiée le 5.10.1988