Polynomials of degree 4 defining units

Osnel Broche and Ángel del Río

Abstract. If x is the generator of a cyclic group of order n then every
element of the group ring $\mathbb{Z}\langle x \rangle$ is the result of evaluating x at a polyno-
mial of degree smaller than n with integral coefficients. When such an
evaluation result into a unit we say that the polynomial defines a unit on
order n. Marciniak and Sehgal have classified the polynomials of degree at
most 3 defining units. The number of such polynomials is finite. However
the number of polynomials of degree 4 defining units on order 5 is infinite
and we give the full list of such polynomials. We prove that (up to a sign)
every irreducible polynomial of degree 4 defining a unit on an order greater
than 5 is of the form $a(X^4 + 1) + b(X^3 + X) + (1 - 2a - 2b)X^2$ and obtain
conditions for a polynomial of this form to define a unit. As an application
we prove that if n is greater than 5 then the number of polynomials of de-
gree 4 defining units on order n is finite and for $n \leq 10$ we give explicitly
all the polynomials of degree 4 defining units on order n. We also include a
conjecture on what we expect to be the full list of polynomials of degree 4
defining units, which is based on computer aided calculations.

1. Introduction

The study of the group of units $\mathcal{U}(\mathbb{Z}G)$ of an integral group ring of a finite group G
was initiated by Higman in the 1940's [6], [7] and was continued in the 1960's by
Bass and Milnor [1] among others. During the last twenty years quite a number
of results have been obtained in the subject (see e.g. [16], [19], [15], [10], [17], [13],
[4], [5], [11], [12], [8], and [9]).

A fundamental question is how to produce units in $\mathbb{Z}G$. Marciniak and Sehgal
introduced a new point of view in [14] consisting on searching for polynomials in
one variable with integral coefficients which yield a unit in $\mathbb{Z}G$ when evaluated
at a group element. Actually, if $C_n = \langle x \rangle$, the cyclic group of order n generated
by x, then all the elements of $\mathbb{Z}C_n$ are the result of evaluating at x polynomials
in $\mathbb{Z}[X]$, that is, the elements of $\mathbb{Z}C_n$ are of the form $P(x)$ with $P \in \mathbb{Z}[X]$. Note

that that $P(x)$ is a unit in $\mathbb{Z}C_n$ only depends on P and n. In such a case we say that P *defines a unit on order* n. Marciniak and Sehgal showed that if Φ_m denotes the m-th cyclotomic polynomial then Φ_m defines a unit on order n if and only if $m/\gcd(m,n)$ is not a prime power [14]. They also introduced the notion of polynomials defining generic units as the monic polynomials in $\mathbb{Z}[X]$ defining units on all the orders coprime with a given integer. For example, Φ_m defines generic units if and only if m is not a prime power and more generally a polynomial Φ of the form $X^m \Phi_{m_1} \cdots \Phi_{m_k}$, with $m \geq 0$ and $m_1, \ldots, m_k$ positive integers which are not prime powers, defines generic units. Marciniak and Sehgal proved that these polynomials Φ are the only monic polynomials defining generic units [14]. Recently, the authors have shown that these polynomials Φ and their opposites, $-\Phi$, are the only polynomials defining units on infinitely many orders [2].

Marciniak and Sehgal also classified the polynomials of degree at most 3 defining units and the goal of this paper is to continue this work by aiming for the classification of polynomials of degree 4 defining units. Before explaining this we give a "convenient" meaning to "polynomial defining units". Recall that every unit of $\mathbb{Z}G$ has augmentation 1 or -1 and observe that $P(1)$ is the augmentation of $P(x)$. Therefore, if P defines a unit on some order then $P(1) = \pm 1$. Of course the converse is true because if $P(1) = \pm 1$ then P defines a unit on order 1. Hence, to avoid trivialities the "convenient" meaning of "polynomial defining units" should not be "defining unit on some order". On the other hand, P defines a unit on order n if and only if the remainder of P modulo $X^n - 1$ defines a unit on order n. Therefore, we may consider without loss of generality orders greater than the degree of P. More precisely, we say that $P \in \mathbb{Z}[X]$ *defines units* if P defines a unit on some order greater than the degree of P.

Clearly, P defines a unit on order n if and only if so does $-P$. Thus we may only consider polynomials P with $P(1) = 1$. In such a case we say that P is *normalized*. Observe also that P defines a unit on order n if and only if each irreducible factor of f defines a unit on order n. Therefore we may restrict our attention to irreducible polynomials. So the general problem consists in classifying the normalized irreducible polynomials defining units (on some order greater than its degree). Marciniak and Sehgal proved that the only normalized irreducible polynomial of degree 1 defining units is X (which defines units on all orders) and the only one of degree 2 is $\Phi_6 = X^2 - X + 1$ (which defines units on every order coprime with 6) [14]. In the same paper a theorem states that there do not exist irreducible polynomials of degree 3 defining units, but the result is false. This was fixed by Marciniak who proved that there are exactly two normalized irreducible polynomials of degree 3 defining units, namely $X^3 + X^2 - 1$ and $-X^3 + X + 1$ (both define units on order 5, [8], Proposition 8.5.11).

A simple observation shows that the picture of the normalized irreducible polynomials of degree 4 defining units should be richer than the somehow disappointing case of degrees 1, 2 and 3. Indeed, it is well known that $\mathcal{U}(\mathbb{Z}C_5)$ is infinite and every element here is the result of evaluating the generator of C_5 on a polynomial of degree at most 4. So, there are infinitely many normalized irreducible polynomials of degree 4 defining units.

In order to present our results we need to introduce the following polynomials:

$$U_{a,b} = aX^4 + bX^3 + (1 - 2(a + b))X^2 + bX + a,$$

with $a, b \in \mathbb{Z}$, and the following terminology: let P be a polynomial of degree smaller than n. An n-shift of P is a polynomial obtained by permuting cyclically the coefficients of P of degree smaller than n. In other words, if $P = a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ then the n-shifts of P are the polynomials of the form $\sigma_n^i(P) = a_{n-1-i}X^{n-1} + a_{n-2-i}X^{n-2} + \cdots + a_0X^i + a_{n-1}X^{i-1} + \cdots + a_{n-i}$ for $i = 0, \ldots, n - 1$.

Our first result gives a class of polynomials which contains all the normalized irreducible polynomials P of degree 4 defining units.

Theorem 1.1. *If P is an normalized irreducible polynomial of degree 4 of $\mathbb{Z}[X]$ defining a unit on order $n \geq 5$, then one of the following conditions holds:*

(1) *$n = 5$ and P is a 5-shift of $U_{a,b}$ with $a, b \in \mathbb{Z}$;*

(2) *$n = 7$ and P is either $X^4 + X^3 - 1$ or $-X^4 + X + 1$;*

(3) *$n \geq 7$ and $P = U_{a,b}$ with $a, b \in \mathbb{Z}$.*

It is easy to see that $X^4 + X^3 - 1$ and $-X^4 + X + 1$ define units on order 7 (see Section 3). Moreover, if P defines a unit on order n and n is greater than the degree of P then all the n-shifts of P define units on order n. So, to complete the desired goal of classifying the polynomials of degree 4 defining units it remains to give a criterion to decide when $U_{a,b}$ defines a unit on some order greater than 4. Lemma 2.1 gives such a criterion in terms of the norm of some algebraic integers. This reduces the question to solve a system of Diophantine equations in two variables. This is not completely satisfactory because we would like to give explicitly the integers a and b and $n \geq 0$ for which $U_{a,b}$ defines a unit on order n. However this can be used, together with the results by Marciniak and Sehgal mentioned above, to prove that the following polynomials of degree 4 define units:

1. The 5-shifts of $U_{a,b}$ with $a^2 + b^2 + 3ab = a + b$. These polynomials define units on order 5. Moreover $U_{1,0} = \Phi_{12}$ defines a unit on every order which is not multiple of neither 3 nor 4.

2. $\Phi_{10} = U_{1,-1}$. It defines a unit on every order coprime with 10.

3. $X^4 + X^3 - 1$, $-X^4 + X + 1$ and $U_{-1,2} = -X^4 + 2X^3 - X^2 + 2X - 1$. These polynomials define units on order 7.

4. $U_{-1,1} = -X^4 + X^3 + X^2 + X - 1$ and $U_{2,-3} = 2X^4 - 3X^4 + 3X^2 - 3X + 2$. These polynomials define units on order 11.

After a computer assisted calculation, using Lemma 2.1 and Corollary 1.2 below, we have not discovered any other normalized irreducible polynomial of degree 4 defining units. So it seems that the polynomials of the previous list exhausts the list of normalized irreducible polynomials of degree 4 defining units. We have obtained some partial results supporting this. First of all we have classified all the normalized polynomials of degree 4 defining units on some order smaller than 11.

Unfortunately, the Diophantine equation that should be solved to obtain all the normalized irreducible polynomials defining units on order 11 is too complicated. Therefore, other ideas are needed to complete the classification.

On the other hand, we prove the following results.

Corollary 1.2. *Let P be a polynomial of degree 4 defining units and let n be the minimal positive integer greater than 4 such that P defines a unit on order n. Then n is prime.*

Corollary 1.3. *Let n be a positive integer. Then the number of polynomials of degree 4 defining a unit on order n is infinite if and only if $n = 1, 2, 3, 4$ or 5.*

2. Polynomials of degree 4 defining units

The aim of this section is proving Theorem 1.1, Corollary 1.2 and Corollary 1.3.

Proof of Theorem 1.1. Suppose that $P = aX^4 + bX^3 + cX^2 + dX + e$ is a normalized irreducible polynomial of degree 4 in $\mathbb{Z}[X]$. Assume that P defines a unit on order $n > 4$ and let x be a generator of C_n and $u = P(x)$. As the degree of P is 4, $a \neq 0$ and as P is irreducible $e \neq 0$. This implies that $u \notin C_n$ and hence $n \neq 6$, because all the units of $\mathbb{Z}C_6$ are trivial. Let * denote the classical involution of $\mathbb{Z}G$, i.e., * is the linear extension to $\mathbb{Z}G$ of the map $g \mapsto g^{-1}$, for $g \in G$. By Proposition 7.1.8 in [8], $u^* u^{-1}$ is a trivial unit and hence

$$ax^{-4} + bx^{-3} + cx^{-2} + dx^{-1} + e = ax^{j+4} + bx^{j+3} + cx^{j+2} + dx^{j+1} + ex^j,$$

for some integer j with $1 - n \leq j \leq 0$. As $e \neq 0$ and $n \geq 5$, we deduce that $j \in \{-4, -3. -2, -1, 0\}$, and as $a \neq 0$, we have that n divides $j + k$ for some $4 \leq k \leq 8$.

If $j = -4$ then $a = e$ and $b = d$. Moreover $2(a + b) + c = P(1) = 1$. Thus $P = U_{a,b}$ and hence either (1) or (3) holds.

If $j = -3$ then $e = b$, $d = c$, $a = 1 - 2(b + c)$ and n divides either $1, 2, 3, 4$ or 5. Therefore $n = 5$, $P = \sigma_5^2(U_{c,b})$ and condition (1) holds.

Similarly, if $j = -2$ then $c = e$ and n divides $2, 3, 4, 5$ or 6. Thus $n = 5$, $a = b$ and $d = 1 - 2(a + c)$ Hence $P = \sigma_5^4(U_{a,c})$ and condition (1) holds.

Suppose $j = -1$. Then $d = e$ and n divides $3, 4, 5, 6$ or 7. Thus either $n = 5$, $a = c$, and $P = \sigma_5(U_{d,a})$; or $n = 7$ and $b = c = 0$. In the former case condition (1) holds. Otherwise $P = aX^4 + d(X + 1)$. Then $u = ax^{-3} + d(x + 1) \in \mathcal{U}(\mathbb{Z}C_7)$ and hence $x^{-1}u = (1 - 2d)x^3 + d(1 + x^6) = Q(x^3)$ for $Q = dX^2 + (1 - 2d)X + d$. Since $u \notin C_n$, Q is a polynomial of degree 2 defining a unit with $Q(1) = 1$ and $Q \neq X^2$. Thus $Q = X^2 - X + 1$, or equivalently $P = -X^4 + X + 1$.

Finally, suppose that $j = 0$. Arguing as before we deduce that $n = 5$, $n = 7$ or $n = 8$. However, if $n = 8$ then $aX^4 + e$ defines a unit on order 8 and hence $aX + e$ defines a unit on order 2 with $a \neq 0 \neq e$. This contradicts with the fact that all the units of $\mathbb{Z}C_2$ are trivial. Thus $n = 5$ or $n = 7$. If $n = 5$ then $P = \sigma_5^3(U_{b,a})$. If $n = 7$ then $a = b$ and $c = d = 0$. Then $u = P(x) = a(x^4 + x^3) + (1 - 2a)$ is a

non-trivial unit of $\mathbb{Z}C_7$. Then $x^3 u = a(1 + x^6) + (1 - 2a)x^3 = Q(x^3)$ is also a unit of $\mathbb{Z}C_7$ with $Q = aX^2 + (1 - 2a)X + a$. The same argument as in the previous paragraph shows that $P = X^4 + X^3 - 1$. $\qquad\square$

For every positive integer n let ζ_n denote a complex primitive n-th root of unity and let x be a generator of C_n. Let $\mathbb{Q}_n^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ and $\mathbb{Z}_n^+ = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$. Then the map $x \to (\zeta_d)_{d|n}$ defines an isomorphism $\mathbb{Q}\langle x \rangle \to \prod_{d|n} \mathbb{Q}(\zeta_d)$, mapping $\mathbb{Z}\langle x \rangle$ into $\prod_{d|n} \mathbb{Z}[\zeta_d]$. As $\mathbb{Z}\langle x \rangle$ is an order in $\mathbb{Q}\langle x \rangle$ and $\prod_{d|n} \mathbb{Z}[\zeta_d]$ is an order in $\prod_{d|n} \mathbb{Q}(\zeta_d)$, a polynomial P defines a unit on order n if and only if $P(\zeta_d)$ is a unit in $\mathbb{Z}[\zeta_d]$ for every $d \mid n$. Using this it is easy to see that if P defines a unit on order n and d divides n then P also defines a unit on order d. Actually this can be also proved using the ring homomorphism $\mathbb{Z}C_n \to \mathbb{Z}C_d$ mapping a generator x of C_n to $x^{n/d}$.

Let

$$S_{a,b}(\zeta_d) = \zeta_d^{-2} U_{a,b}(\zeta_d) = 1 + a(\zeta_d^2 + \zeta_d^{-2} - 2) + b(\zeta_d + \zeta_d^{-1} - 2).$$

Then $U_{a,b}(\zeta_d)$ is a unit of $\mathbb{Z}[\zeta_d]$ if and only if $S_{a,b}(\zeta_d)$ is a unit of $\mathbb{Z}_d^+$ if and only if $N_{\mathbb{Q}_d^+/\mathbb{Q}}(S_{a,b}(\zeta_d)) = \pm 1$ (see Lemma 4.6 in [17] or Lemma 4.6.9 in [8]). This proves the following.

Lemma 2.1. *The following are equivalent for integers a, b and n with $n \geq 1$:*

1. $U_{a,b}$ *defines a unit on order n.*
2. $S_{a,b}(\zeta_d) = 1 + a(\zeta_d^2 + \zeta_d^{-2}) + b(\zeta_d + \zeta_d^{-1})$ *is a unit of $\mathbb{Z}[\zeta_d + \zeta_d^{-1}]$ for every $d \mid n$.*
3. $N_{\mathbb{Q}_d^+/\mathbb{Q}}(S_{a,b}(\zeta_d)) = \pm 1$ *for every $d \mid n$.*

The following lemma will be used in the proof of Corollary 1.2 and in Section 3.

Lemma 2.2. *Let a and b be integers:*

(1) $U_{a,b}$ *defines a unit on order 3 if and only if $a + b = 0$.*

(2) $U_{a,b}$ *defines a unit on order 9 if and only if $a = -b \in \{0, 1\}$.*

(3) $U_{a,b}$ *defines a unit on order 5 if and only if $a + b = a^2 + b^2 + 3ab$.*

(4) $U_{a,b}$ *defines a unit on order 10 if and only if $b = 0$ and $a \in \{0, 1\}$.*

(5) $U_{a,b}$ *defines a unit on order $4, 6$ or 15 if and only if $a = b = 0$.*

Proof. (1) and the statement (5) for orders 4 or 6 follows easily from the fact that all the units of $\mathbb{Z}C_3$, $\mathbb{Z}C_4$ and $\mathbb{Z}C_6$ are trivial.

By Lemma 2.1, $U_{a,b}$ defines a unit on order 9 if and only if it defines a unit on order 3 and $N_{\mathbb{Q}_9^+/\mathbb{Q}}(S_{a,b}(\zeta_9)) = \pm 1$. A straightforward calculation shows that

(2.1) $N_{\mathbb{Q}_9^+/\mathbb{Q}}(S_{a,b}(\zeta_9)) = 1 + 3(-a^3 - 9a^2b - 6ab^2 - b^3 + 3a^2 + 9ab + 3b^2 - 2a - 2b).$

Hence, using (1) and (2.1), we deduce that $U_{a,b}$ defines a unit on order 9 if and only if $a = -b \in \{0, 1\}$. This proves (2).

(3) is a consequence of Lemma 2.1 and the following equality, that can be checked by straightforward calculations:

$$(2.2) \qquad N_{\mathbb{Q}_5^+/\mathbb{Q}}(S_{a,b}(\zeta_5)) = 1 + 5(a^2 + 3ab + b^2 - a - b).$$

By (1) and (3), if $U_{a,b}$ defines a unit on order 15 then $a = -b$ and $a^2 + b^2 + 3ab = a + b$. This implies $a = b = 0$. This finishes the proof of (5).

(4) Using $N_{\mathbb{Q}_2^+/\mathbb{Q}}(S_{a,b}(\zeta_2)) = 1 - 4b$,

$$N_{\mathbb{Q}_{10}^+/\mathbb{Q}}(S_{a,b}(\zeta_{10})) = 1 + 5(a^2 + ab - a) + b^2 - 3b,$$

and the expression of $N_{\mathbb{Q}_5^+/\mathbb{Q}}(S_{a,b}(\zeta_5))$ in (2.2), we deduce that $U_{a,b}$ defines a unit on order 10 if and only if $b = 0$ and $a \in \{0, 1\}$. □

Proof of Corollary 1.2. Let P be a polynomial in $\mathbb{Z}[X]$ of degree 4 defining units and let n be the smallest integer greater than 4 on which P defines a unit. We may assume without loss of generality that $P(1) = 1$. If P is reducible then, by the classification of the irreducible polynomials of degree at most 3 defining units, P is either X^4, $X^2\Phi_6$, Φ_6^2, $X(X^3 + X^2 - 1)$ or $X(-X^3 + X + 1)$. All these polynomials define units on order 5 and hence $n = 5$.

Suppose that P is irreducible and by means of contradiction assume that n is not prime. Then P is one of the polynomials of Theorem 1.1, and as n is not prime, $P = U_{a,b}$, with $a \neq 0$. If n is divisible by a prime p then $U_{a,b}$ defines a unit on order p and hence the result is obvious if n is divisible by a prime greater than 3. Therefore, we may assume that n is not divisible by any prime greater than 3. By statement (5) of Lemma 2.2, n is not divisible by neither 4 nor 6. Therefore $n = 9$. By statement (2) of Lemma 2.2, $(a, b) = (1, -1)$ i.e., $U_{a,b} = U_{1,-1} = X^4 - X^3 + X^2 - X + 1 = \Phi_{10}$. Then $U_{1,-1}$ defines a unit on order m if and only if $\gcd(10, m) = 1$ and hence $n = 7$, a contradiction. □

Let $P_d(a, b) = N_{\mathbb{Q}_d^+/\mathbb{Q}}(S_{a,b}(\zeta_d))$. Observe that $S_{a,b}(\zeta_d)$ belongs to the principal ideal of $\mathbb{Z}[\zeta_d]$ generated by $1 - \zeta_d$. This implies that $P_d(a, b)$ belongs to the ideal of $\mathbb{Z}$ generated by $N_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(1 - \zeta_d)$. In case d is a power of a prime p, we have $N_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(1 - \zeta_d) = p$ and therefore, in this case, $S_{a,b}(\zeta_d)$ is a unit in $\mathbb{Z}_d^+$ if and only if $P_d(a, b) = 1$. In particular, if p is an odd integer then $U_{a,b}$ defines a unit on order p if and only if $P_p(a, b) = 1$. This is a polynomial on a and b of degree $(p - 1)/2$ with coefficients in $\mathbb{Z}$. Thus, in principal one can calculate all the integers a and b for which $U_{a,b}$ defines a unit on order p by solving the Diophantine equation $P_p(a, b) = 1$. This is what we have done to prove statement (3) of Lemma 2.2. Observe that the relation $a + b = a^2 + b^2 + 3ab$ is equivalent to $(5(a + b) - 2)^2 - 5(a - b)^2 = 4$. Therefore the integers a and b satisfying this condition are given by

$$a = \frac{x + 2 + 5y}{10}, \quad b = \frac{x + 2 - 5y}{10}$$

with (x, y) an integral solutions of the Pell equation $X^2 - 5Y^2 = 4$ such that $x \equiv -2 \mod 5$.

Proof of Corollary 1.3. All the polynomials of the form $1 + a - aX^4$ define units on order 2 and 4, and all the polynomials of the form $1 + aX - aX^4$ define units on order 3. Therefore there infinitely many polynomials of degree 4 defining units on order $1, 2, 3$ or 4. Moreover, $\mathbb{Z}C_5$ has infinitely many units and all the elements in $\mathbb{Z}C_5$ are the result of evaluating a polynomial of degree at most 4 in one generator of C_5. Therefore there are also infinitely many polynomials of degree 4 defining units on order 5.

By Theorem 1.1, to finish the proof it is enough to show that if $n \geq 6$ then there are only finitely many polynomials of the form $U_{a,b}$ defining a unit on order n. We first prove the result under the assumption that n is divisible by d with d a power of an odd prime p such that $\varphi(d) \geq 6$. If $U_{a,b}$ defines a unit on order n then $U_{a,b}$ defines a unit on order d and hence one may assume without lost of generality that $n = d$. Assume that $U_{a,b}$ defines a unit on order n. Then $P_n(a, b) = \pm 1$. Let $U_n = \mathcal{U}(\mathbb{Z}/n\mathbb{Z})/(-1)$ and for every $i \in U_n$ let $\alpha_i = \zeta_n^i + \zeta_n^{-i} - 2$. Then $P_n(a, b) = \prod_{i \in U_d}(1 + \alpha_{2i}a + \alpha_i b)$. Since $\alpha_2 a + \alpha b$ belongs to the ideal of $\mathbb{Z}[\zeta_n]$ generated by $1 - \zeta_n$, we have that $P_n(a, b)$ is an integer congruent with 1 modulo $N(1 - \zeta_n) = p$. Therefore $P_n(a, b) = 1$. We claim that $Q(a, b) = P_n(a, b) - 1$ is irreducible in $\mathbb{C}[a, b]$. Indeed, after a change of variable, the polynomial takes the form $X \prod_{i=1}^{n}(P_i + b_i Y) - 1$ where each $b_i \in \mathbb{C}$ and $P_i \in \mathbb{C}[X]$ with P_i of degree 1 and not multiple of X. Then Eisenstein's irreducibility criterion applies to prove the irreducibility of $Q(a, b)$. The projective curve defined by $Q(a, b) = 0$ contains $\varphi(d)/2$ points at infinity (namely the points $(\alpha_i, -\alpha_{2i}, 0)$). If $\varphi(d) \geq 6$ then, by Siegel's theorem ([3], Theorem 3.2), $Q(a, b)$ has finitely many integral zeros and hence the equation $P_p(a, b) = \pm 1$ has finitely many integral solutions. This gives the desired conclusion.

So it remains to prove the result under the assumption that n is not divisible by any odd prime power d with $\varphi(d) \geq 6$. In particular n is not divisible by any prime greater than 5 and it is not divisible by 9 nor 25. Moreover, the result follows if n is multiple of 4, or multiple of 6 or multiple of 10 or multiple of 15, by Lemma 2.2. Thus the results follows for every $n \geq 6$. $\qquad\square$

3. Polynomials of degree 4 defining units on order ≤ 10

In this section we give explicitly the polynomials of degree 4 defining units on order n for every $n \leq 10$.

If $n = 1, 2, 3, 4$ or 6 then all the units of $\mathbb{Z}C_n$ are trivial. Using this it easy to describe the polynomials of degree 4 defining units on these orders. For example, the normalized polynomials $P \in \mathbb{Z}[X]$ of degree 4 defining units on order 3 are those of one of the following forms: $a + bX + X^2 - aX^3 - bX^4$, $a + (1+b)X - aX^3 - bX^4$, $1 + a + bX - aX^3 - bX^4$.

By Theorem 1.1 and statement (5) in Lemma 2.2, there are no irreducible polynomials of degree 4 defining units on order 8. By Lemma 2.2, if $P \in Z[X]$ is irreducible and normalized of degree 4 then

- P defines a unit on order 5 if and only if P is a 5-th shift of the polynomials $U_{a,b}$ with $a^2 + b^2 + 3ab = a + b$;

- P defines a unit on order 9 if and only if $P = U_{1,-1} = \Phi_{10}$; and

- P defines a unit on order 10 if and only if $P = U_{1,0} = \Phi_6(X^2)$.

In order to classify the polynomials of degree 4 defining units on order 7 we first prove that the two polynomials in statement (2) of Theorem 1.1 define units on order 7. Indeed, if m is relatively prime with n then P defines a unit on order n if and only if so does $P(X^m)$. As Φ_6 defines units on order 7 then so does $\sigma_7(\Phi_6(X^3)) = -X^4 + X + 1$ and $\sigma_7^4(\Phi_6(X^3)) = X^4 + X^3 - 1$. To consider the polynomials of the form $U_{a,b}$ we need the following lemma.

For a prime integer p and an integer n let $v_p(n)$ denote the multiplicity of p as a divisor of n.

Lemma 3.1. *If x, y and z are positive integers satisfying* $\gcd(2x, y) = 1$,

$$(3.1) \qquad\qquad 8x^4 + 4y^4 - 11x^2y^2 = z^2$$

then $x = y = z = 1$.

Proof. Let x, y and z satisfy the hypothesis of the lemma. Then $\gcd(y, z) = 1$ and $\gcd(x, z)|4$.

We claim that if x is odd then there are positive integers r and s satisfying $x = rs$ and $16y^2 - 22r^2s^2 = r^4 - 7s^4$. First of all, by the previous paragraph $\gcd(x, z) = 1$. Multiplying by 16 in (3.1) and completing squares we obtain

$$(8y^2 - 11x^2)^2 + 7x^4 = (4z)^2$$

or equivalently

$$7x^4 = (4z + 8y^2 - 11x^2)(4z - 8y^2 + 11x^2).$$

If p is a prime divisor of $\gcd(8y^2 - 11x^2, 4z)$ then p is an odd divisor of z and p^2 divides $7x^4$. Then $p \mid \gcd(x, z) = 1$, a contradiction. Thus $\gcd(8y^2 - 11x^2, 4z) = 1$ and hence $\gcd(4z + 8y^2 - 11x^2, 4z - 8y^2 + 11x^2) = 1$. Therefore $\{4z + 8y^2 - 11x^2, 4z - 8y^2 + 11x^2\} = \pm\{r^4, 7s^4\}$ for some relatively odd prime positive integers r and s such that $x = rs$. Moreover, $4z + 8y^2 - 11x^2 \equiv r^4 \equiv 1 \mod 4$ and $4z - 8y^2 + 11x^2 \equiv 7s^4 \equiv -1 \mod 4$. Thus, either $4z + 8y^2 - 11x^2 = r^4$ and $4z - 8y^2 + 11x^2 = 7s^4$, or $4z + 8y^2 - 11x^2 = -7s^4$ and $4z - 8y^2 + 11x^2 = -r^4$. In both cases $16y^2 - 22r^2s^2 = r^4 - 7s^4$, as desired.

If $x = 1$ then $r = s = 1$ and the last equality implies that $y = 1$ and hence $z = 1$, as desired. Hence it only remains to prove that $x = 1$ and for that we argue by contradiction. Therefore, we suppose that x is the minimum integer greater than 1 with x, y and z satisfying the hypothesis of the lemma.0

Suppose first that x is odd. By the claim $x = rs$ for some positive integers r and s satisfying $16y^2 - 22r^2s^2 = r^4 - 7s^4$. If $r = 1$ then $s = x$ and, by the previous paragraph, $0 < 16y^2 - 1 = x^2(22 - 7x^2) < 0$, a contradiction. Thus $r > 1$. Rewriting the above equality we have $(r^2 + 11s^2)^2 - 128s^4 = 16y^2$ and hence $8s^4 = (\frac{r^2 + 11s^2}{4} + y)(\frac{r^2 + 11s^2}{4} - y)$. Moreover, $\gcd\left(\frac{r^2+11s^2}{4} + y, \frac{r^2+11s^2}{4} - y\right) = 2$ and thus there are positive integers x_1 and y_1 such that $\left\{\frac{r^2+11s^2}{4} + y, \frac{r^2+11s^2}{4} - y\right\} =$

$\{4x_1^4, 2y_1^4\}$ with $s = x_1 y_1$ and $\gcd(x_1, y_1) = 1$. Then $8x_1^4 + 4y_1^4 - 11x_1^2 y_1^2 = r^2$. Therefore (x_1, y_1, r) is a solution of the equation and $x_1 \leq s < x$. By the minimality of x we deduce that $x_1 = 1$, and hence $(1, s, r)$ is a solution of the equation. By the above paragraph, we deduce that $r = 1$, which yields the desired contradiction.

Secondly suppose that x is even. We claim that $v_2(x) \geq 3$ and $v_2(z) = 1$. Indeed, if $v_2(x) = 1$ then $y^4 - 11 \left(\frac{x}{2}\right)^2 y^2 \equiv 2 \mod 4$. Then $z^2 = 8x^4 + 4y^4 - 11x^2 y^2 \equiv 4\left(y^4 - 11\left(\frac{x}{2}\right)^2 y^2\right) \equiv 8 \mod 16$, a contradiction. Therefore, $v_2(x) \geq 2$ and hence $2v_2(z) = v_2(8x^4 + 4y^4 - 11x^2 y^2) = 2$. This proves that $v_2(z) = 1$. If $v_2(x) = 2$ then $-3 \equiv 2^9 \left(\frac{x}{4}\right)^4 + y^4 - 44 \left(\frac{x}{4}\right)^2 y^2 = \left(\frac{z}{2}\right)^2 \equiv 1 \mod 8$, again a contradiction. This proves the claim.

Let $\overline{x} = x/8$ and $\overline{z} = z/2$. These are odd coprime integers, by the last claim. Moreover, $2^{13}\overline{x}^4 + y^4 - 2^4 \cdot 11\overline{x}^2 y^2 = \overline{z}^2$. Hence $7 \cdot 2^6 \overline{x}^4 = (\overline{z} + y^2 - 88\overline{x}^2)(\overline{z} - y^2 + 88\overline{x}^2)$. If p is an odd common prime divisor of $\overline{z} + y^2 - 88\overline{x}^2$ and $\overline{z} - y^2 + 88\overline{x}^2$ then $p \mid \gcd(\overline{x}, \overline{z}) = 1$. Thus $\gcd(\overline{z} + y^2 - 88\overline{x}^2, \overline{z} - y^2 + 88\overline{x}^2) = 2$. This implies that there are positive integers r and s such that $\overline{x} = rs$ and $\{\overline{z} + y^2 - 88\overline{x}^2, \overline{z} - y^2 + 88\overline{x}^2\}$ is either $\pm\{14r^4, 2^5 s^4\}$ or $\pm\{2r^4, 2^5 \cdot 7s^4\}$.

Assume that $\{\overline{z} + y^2 - 88\overline{x}^2, \overline{z} - y^2 + 88\overline{x}^2\} = \pm\{2^5 s^4, 14r^4\}$. Then $1 \equiv y^2 - 88\overline{x}^2 = \pm(2^4 s^4 - 7r^4) \equiv \pm 1 \mod 8$ and therefore $y^2 - 88r^2 s^2 = 2^4 s^4 - 7r^4$. Hence $128r^4 = (4s^2 + 11r^2)^2 - y^2$. As $\gcd(y, rs) = 1$ we deduce that $\gcd(4s^2 + 11r^2, y) = 1$ and $\gcd(4s^2 + 11r^2 + y, 4s^2 + 11r^2 - y) = 2$. Thus there are relatively prime positive integers u, v such that $r = uv$ and $\{4s^2 + 11r^2 + y, 4s^2 + 11r^2 - y\} = \{2u^4, 2^6 v^4\}$ and $\gcd(2, uv) = 1$. Then $3 \equiv 4s^2 + 11u^2 v^2 = u^4 + 2^5 v^4 \equiv 1 \mod 4$, a contradiction.

Therefore $\{\overline{z} + y^2 - 88\overline{x}^2, \overline{z} - y^2 + 88\overline{x}^2\} = \pm\{2r^4, 2^5 \cdot 7s^4\}$. Then $1 \equiv y^2 - 88\overline{x}^2 = \pm(r^4 - 2^4 \cdot 7s^4) \equiv \pm 1 \mod 8$, and hence $2^{11} s^4 = (r^2 + 44s^2)^2 - y^2$. As in the previous case we deduce that $\{r^2 + 44s^2 + y, r^2 + 44s^2 - y\} = \{2u^4, 2^{10} v^4\}$ and $s = uv$ for some relatively prime positive integers u and v with $\gcd(2, u) = 1$. Thus $r^2 + 44u^2 v^2 = u^4 + 2^9 v^4$. Setting $x_1 = 4v$, $y_1 = u$ and $z_1 = 2r$ we have $8x_1^4 + 4y_1^4 - 11x_1^2 y_1^2 = z_1^2$ and $1 < x_1 \leq 4s \leq 4\overline{x} < x$, in contradiction with the minimality of x. □

Proposition 3.2. *The normalized irreducible polynomials P of degree 4 defining units on order 7 are $X^4 + X^3 - 1$, $-X^4 + X + 1$ and the polynomials $U_{a,b}$ with $(a, b) \in \{(1, 0), (1, -1), (-1, 2)\}$.*

Proof. By straightforward calculations we have

$$P_7(a, b) = 1 - 7(b(b - 1 + 2a)(b - 1 + 3a) + a(a - 1)^2).$$

Hence, by Lemma 2.1, we only have to prove that $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, -1)$, $(1, -2)$ and $(-1, 2)$ are the only integral solutions (a, b) of the following equation:

(3.2) $$b(b - 1 + 2a)(b - 1 + 3a) + a(a - 1)^2 = 0.$$

(Observe that the solutions $(0, 0)$ and $(0, 1)$ yield polynomials $U_{a,b}$ of degree smaller than 4 and the solution $(1, -2)$ provides the polynomial $U_{1,-2} = (X^2 - X + 1)^2$ which is not irreducible.)

Let a and b be integers satisfying (3.2). If $a = 0$ then $b \in \{0, 1\}$; if $a = 1$ then $b \in \{0, -1, -2\}$; and if $b = 0$ then $a \in \{0, 1\}$. Thus we may assume that $a \notin \{0, 1\}$ and $b \neq 0$ and we have to show that $(a, b) = (-1, 2)$. Furthermore, it is easy to see that $b \neq 1$ and $ab < 0$. Let $d = \gcd(a, b)$, chosen so that d and a have the same sign.

Let p be a prime integer. If $v_p(a), v_p(b) > 0$ then $v_p(a) = v_p(b)$. This implies

$$\gcd\left(\frac{a}{d}, b\right) = \gcd\left(\frac{b}{d}, a\right) = 1.$$

Suppose that p divides a but does not divide b. Then $v_p(a) = v_p(b - 1 + 2a) + v_p(b - 1 + 3a)$ and therefore $v_p(b - 1) > 0$. If $v_p(b - 1) \geq v_p(a)$ then $v_p(a) = v_p(b-1+2a)+v_p(b-1+3a) \geq v_p(2a)+v_p(3a) \geq 2v_p(a)$, a contradiction. Therefore $v_p(b - 1) < v_p(a)$ and thus $v_p(a) = v_p(b - 1 + 2a) + v_p(b - 1 + 3a) = 2v_p(b - 1)$. Thus

(3.3) $a = dx^2 \quad \text{and} \quad b - 1 = xb_1,$

for some integers x and b_1 such that

$$(d, x) = (x, b_1) = 1.$$

Suppose now that p divides b but does not divide a. Then $v_p(b) + v_p(b - 1 + 2a) + v_p(b - 1 + 3a) = 2v_p(a - 1)$. In particular $p \mid a - 1$ and hence $p \nmid b - 1 + 2a$. Therefore $v_p(b) + v_p(b - 1 + 3a) = 2v_p(a - 1)$. If $p \neq 2$ then $p \nmid b - 1 + 3a = b + a - 1 + 2a$ and therefore $v_p(b) = 2v_p(a - 1)$. If $v_2(b)$ is even and positive then $v_2(b - 1 + 3a) = v_2(b + a - 1 + 2a) \geq 2$ and therefore $v_2(a - 1) = 1$. This yields a contradiction. Thus, if $v_2(b) > 1$ then $v_2(b) \geq 3$ and hence $v_2(a - 1) \geq 2$ and $v_2(b - 1 + 3a) = 1$. Therefore $v_2(b) = 2v_2(a - 1) - 1$. This implies that one of the following cases hold:

Case 1. $b = -dy^2$, $a - 1 = a_1 y$, with $\gcd(x, y) = \gcd(2d, y) = \gcd(a_1, y) = 1$.

Case 2. $b = -2dy^2$, $a - 1 = 2^k a_1 y$, with $2 \nmid dy a_1$, $\gcd(x, y) = \gcd(d, y) = \gcd(a_1, y) = 1$ and $k \geq 1$.

Case 3. $b = -2^{2k+1} dy^2$, $a - 1 = 2^{k+1} a_1 y$, with $\gcd(x, y) = \gcd(2d, y) = \gcd(a_1, 2y) = 1$ and $k \geq 1$.

We deal with these three cases separately.

Case 1. Using (3.3) and the hypotheses of Case 1, we obtain

$$dx^2 - a_1 y = 1 = -b_1 x - dy^2.$$

Hence $(dx + b_1)x = (a_1 - dy)y$ and, since $\gcd(x, y) = 1$, there is an integer e such that

$$b_1 = -dx + ye \quad \text{and} \quad a_1 = xe + dy.$$

Thus

$$a = 1 + exy + dy^2 = dx^2 \quad \text{and}$$
$$b = 1 + exy - dx^2 = -dy^2.$$

Combining this with (3.2) we obtain

$$-(ey + dx)(ey + 2dx) + (ex + dy)^2 = 0,$$

or equivalently

(3.4) $$2d^2x^2 + e^2y^2 + dexy = e^2x^2 + d^2y^2.$$

Considering this as a quadratic equation on d we obtain that

$$8x^4 + 4y^4 - 11x^2y^2 = z^2$$

for some integer z. By Lemma 3.1, we deduce that $x = y = 1$. Replacing this in $1 + exy + dy^2 = dx^2$ we deduce that $e = -1$. Replacing in (3.4) we deduce that $d = 1$. Hence $a = 1$, in contradiction with the assumptions.

Case 2. Using (3.3) and the hypothesis of Case 2, we obtain

$$dx^2 - 2^k a_1 y = 1 = -b_1 x - 2dy^2.$$

Then there is an integer e such that

$$b_1 = -dx + ey \quad \text{and} \quad 2^k a_1 = 2dy + ex.$$

Thus

$$a = 1 + exy + 2dy^2 = dx^2 \qquad \text{and}$$
$$b = 1 + exy - dx^2 = -2dy^2.$$

Combining this with (3.2) we obtain

(3.5) $$e^2(2y^2 - x^2) + (2d)exy + (2d)^2(x^2 - y^2) = 0.$$

Considering this as a quadratic equation on $2d$ or e we obtain that

$$4x^4 + 8y^4 - 11x^2y^2 = z^2$$

for some integer z. By Lemma 3.1, we deduce that $x = y = 1$. Replacing this in $1 + exy + 2dy^2 = dx^2$ we deduce that $d = -1 - e$. Replacing in (3.5) we deduce that $(d, e) = (-1, 0)$ or $(d, e) = (1, -2)$. As $a \neq 1$, we deduce that $(a, b) = (-1, 2)$, as desired.

Case 3. Using (3.3) and the hypothesis of Case 3, we obtain

$$dx^2 - 2^{k+1} a_1 y = 1 = -b_1 x - 2^{2k+1} dy^2.$$

Therefore there is an integer e such that

$$b_1 = -dx + ey \quad \text{and} \quad 2^{k+1} a_1 = 2^{2k+1} dy + ex.$$

Thus

$$a = 1 + exy + 2^{2k+1} dy^2 = dx^2 \qquad \text{and}$$
$$b = 1 + exy - dx^2 = -2^{2k+1} dy^2.$$

Combining this with (3.2) we obtain

$$2^{2k+1}(ey + dx)(ey + 2dx) - (ex + 2^{2k+1}dy)^2 = 0,$$

or equivalently

(3.6) $e^2(2^{2k+1}y^2 - x^2) + 2^k(2^{k+1}d)exy + (2^{k+1}d)^2(x^2 - 2^{2k}y^2) = 0.$

Considering this as a quadratic equation on $2^{k+1}d$ or e we obtain that

$$4x^4 + 8(2^k y)^4 - 11x^2(2^k y)^2 = z^2$$

for some integer z. By Lemma 3.1, we deduce that $x = 2^k y = 1$, in contradiction with $k \geq 1$. This finishes the proof of Proposition 3.2.   □

The strategy followed to prove Proposition 3.2 could be repeated to classify the polynomials of degree 4 defining units on order 11. This yields the following Diophantine equation:

$$5a^4 + 35a^3b + 56a^2b^2 + 30ab^3 + 5b^4 + 4a^2 + 9ab + 4b^2$$
$$= a^5 + 15a^4b + 35a^3b^2 + 28a^2b^3 + 9ab^4 + b^5 + 7a^3 + 28a^2b + 27ab^2 + 7b^3 + a + b,$$

which seems too difficult to be solved.

References

[1] Bass, H.: The Dirichlet unit theorem, induced characters, and Whitehead groups of finite groups. *Topology* **4** (1965), 391–410.

[2] Broche, O. and del Río, Á.: Polynomials defining many units. *Math. Z.* **283** (2016), no. 3-4, 1195–1200.

[3] Fuchs, C. and Zannier, U.: Integral points on curves: Siegel's theorem after Siegel's proof. In *On some applications of Diophantine approximations,* 139–177. Quad./Monogr. 2, Ed. Norm. Pisa, 2014.

[4] Hertweck, M.: A counterexample to the isomorphism problem for integral group rings. *Ann. of Math.* **154** (2001), no. 1, 115–138.

[5] Hertweck, M.: On the torsion units of some integral group rings. *Algebra Colloq.* **13** (2006), no. 2, 329–348.

[6] Higman, G.: *Units in group rings.* PhD Thesis, Oxford University, 1940.

[7] Higman, G.: The units of group-rings. *Proc. London Math. Soc. (2)* **46** (1940), 231–248.

[8] Jespers, E. and del Río, Á.: *Group ring groups. Vol. 1: Orders and generic constructions of units.* De Gruyter Textbook, De Gruyter, Berlin, 2015.

[9] Jespers, E. and del Río, Á.: *Group ring groups. Vol. 2: Structure theorems of unit groups.* De Gruyter Textbook, De Gruyter, Berlin, 2015.

[10] Jespers, E. and Leal, G.: Generators of large subgroups of the unit group of integral group rings. *Manuscripta Math.* **78** (1993), no. 3, 303–315.

[11] Jespers, E. Pita, A., del Río, Á., Ruiz, M. and Zalesskii, P. A.: Groups of units of integral group rings commensurable with direct products of free-by-free groups. *Adv. Math.* **212** (2007), no. 2, 692–722.

[12] Kimmerle, W.: Unit groups of integral group rings: old and new. *Jahresber. Dtsch. Math.-Ver.* **115** (2013), no. 2, 101–112.

[13] Marciniak, Z. S. and Sehgal, S. K.: Constructing free subgroups of integral group ring units. *Proc. Amer. Math. Soc.* **125** (1997), no. 4, 1005–1009.

[14] Marciniak, Z. S. and Sehgal, S. K.: Generic units in abelian group rings. *J. Group Theory* **8** (2005), no. 6, 777–799.

[15] Ritter, J. and Sehgal, S. K.: Construction of units in integral group rings of finite nilpotent groups. *Trans. Amer. Math. Soc.* **324** (1991), no. 2, 603–621.

[16] Roggenkamp, K. and Scott, L.: Isomorphisms of p-adic group rings. *Ann. of Math. (2)* **126** (1987), no. 3, 593–647.

[17] Sehgal, S. K.: *Units in integral group rings.* Pitman Monographs and Surveys in Pure and Applied Mathematics 69, Longman Scientific & Technical, Harlow, 1993.

[18] Siegel, C. L.: Uber einige Anwendungen diophantischer Approximationen. In *Gesammelte Abhandlungen. Bände I,* 209–266. Springer-Verlag, Berlin-New York, 1966.

[19] Weiss, A.: Torsion units in integral group rings. *J. Reine Angew. Math.* **415** (1991), 175–187.

Osnel Broche: Departamento de Ciências Exatas, Universidade Federal de Lavras, Caixa Postal 3037, 37200-000, Lavras, Brazil.
E-mail: osnel@dex.ufla.br

Ángel del Río: Departamento de Matemáticas, Universidad de Murcia, Campus Espinardo, 30100, Murcia, Spain.
E-mail: adelrio@um.es