ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

HANS PETER REHM

Prime factorization of integral Cayley octaves

Annales de la faculté des sciences de Toulouse 6^e série, tome 2, n° 2 (1993), p. 271-289

<http://www.numdam.org/item?id=AFST_1993_6_2_2_271_0>

Annales de la Faculté des Sciences de Toulouse Vol. II, n° 2, 1993

Prime factorization of integral Cayley octaves(*)

HANS PETER REHM (1)

RÉSUMÉ. — La factorisation unique en irréductibles existe dans l'ordre maximal de Coxeter de l'algèbre (non associative) des octaves de Cayley-Dickson sur les rationnels. On en déduit une notion de factorialité pour les algèbres alternées p-adiques sur $\mathbf{Q}_p$. La factorisation en irréductibles d'un octave primitif entier se calcule à partir d'un facteur irréductible de la norme en utilisant un algorithme effectif. Enfin, on obtient une démonstration purement algébrique du théorème de Jacobi sur les sommes de huit carrés.

ABSTRACT. — A theorem about unique prime factorization holds in Coxeter's (nonassociative) maximal order of the algebra of Cayley Dickson octaves over rational numbers. This implies a prime factorization theory also for p-adic alternative algebras over $\mathbf{Q}_p$. The prime factorization of a primitive integral octave can be found by factorizing the norm and repeated division with residue. By counting octaves one gets a purely algebraic proof of Jacobi's theorem about sums of eight squares.

1. Introduction

This paper develops a kind of "elementary number theory" for integral Cayley octaves, that is the properties connected with divisibility. I took Hurwitz's *number theory of quaternions*, *cf.* [3], as a model, since the technics developed later for the number theory of associative algebras cannot be adapted easily to this nonassociative case. So I do not know whether the prime factorization theory for p-adic alternative algebras can be extended to the case of general local base fields.

(*) Reçu le 6 octobre 1992

(1) Mathematisches Institut II der Universität, 75 Karlsruhe 1, Englerstr. 2

The technics of associative number theory break down even at the most elementary level: the divisor relation is not transitive and all left ideals of the maximal order are, by a result of Mahler, generated by rationals hence useless for a factorization theory of octaves. But using the results of Coxeter one has division with residue. Unfortunately, Euclid's division algorithm, executed formally, does not always compute common right divisors of two integral octaves in contrast to the associative case of Hurwitz quaternions. Nevertheless, the division with residue can be used to obtain an algorithm computing a right divisor of norm p of a primitive octave. The theorem about unique prime factorization follows. (Uniqueness is proved by global geometric arguments for which I could not find a local replacement. Hence I do not know a direct local proof for the theorem obtained by localization.)

Following a suggestion in [1] I chose Jacobi's formula describing in how many ways an integer can be written as a sum of eight squares as a test for the power of prime factorization. Known proofs use series identities from the theory of elliptic functions or Siegel's analytic theory of forms. The proof exposed here is elementary (adding a few pages from [1], [2], and [8] would make it self contained), and provides more detailed algebraic information. Earlier papers on octaves, for example [7], [6] or [5], use Jacobi's formula or the theory of quadratic forms in order to find the number of integral octaves of given norm and prove other properties of integral octaves. Here I want to demonstrate that the arithmetics of octaves is enough to do this job.

The paper is organized as follows: section 2 and 3 introduce the notations and cite (rather generously) known facts about alternative and octave algebras. Sections 4-6 contain the factorization algorithm, theorems about unique prime factorization, and information about prime octaves. In section 7 we get a prime factorization theory for alternative p-adic algebras by localization. In section 8 the theory is applied to count the number of octaves of given norm.

The main results of the paper have been presented already at the Oberwolfach number theory meeting in 1988.

Finally I want to state my obligation to the late Hans Zassenhaus who aroused my interest in octave algebras.

2. Integral octaves

For the convenience of the reader I collect the few results about octaves needed later from [1], [2] and [8]. As usual, $\mathbb{Q}$, $\mathbb{R}$ is the field of rational

resp. real numbers, $\mathbb{Z}$ the ring of integers, and $\mathbb{N} = \{1, 2, 3, \ldots\}$. Following Coxeter [2] the Cayley Dickson octave algebra $\mathcal{A}$ over $\mathbb{Q}$ is defined by the incomplete multiplication table of a $\mathbb{Q}$-base $e_0, \ldots, e_7$:

- $e_0 e_i = e_i e_0 = e_i$ $(i = 0, \ldots, 7)$
- $e_0 = -e_i^2$ $(i = 1, \ldots, 7)$
- $e_{\pi 1} = e_{\pi 2} e_{\pi 4} = -e_{\pi 4} e_{\pi 2}$.

Here π is any power of the cyclic permutation (1234567). The other relations are easily deduced, e.g. $e_5 = e_6 e_1$ hence $e_5 e_1 = e_6 e_1^2 = -e_6$.

$\mathcal{A}$ is the unique alternative division algebra over $\mathbb{Q}$ with center $\mathbb{Q}$ up to isomorphism.

e_0 is the unit element and we indentify $q \in \mathbb{Q}$ and qe_0 throughout. In particular we write $e_0 = 1$.

An octave

$$\alpha = \sum_{i=0}^{7} x_i e_i \quad (x_0, \ldots, x_7 \in \mathbb{Q})$$

which we sometimes denote by

$$\alpha = (x_0, \ldots, x_7)$$

has the *trace*

$$\mathrm{tr}(\alpha) = 2x_0$$

and the *norm*

$$\mathrm{n}(\alpha) = \sum_{i=0}^{7} x_i^2 .$$

The conjugate octave is

$$\alpha^* = \mathrm{tr}(\alpha) - \alpha ,$$

and from $\mathrm{n}(\alpha) = \alpha\alpha^* = \alpha^*\alpha$ we see that α is a zero of the polynomial

$$(X - \alpha)(X - \alpha^*) = X^2 - \mathrm{tr}(\alpha)X + \mathrm{n}(\alpha) \in \mathbb{Q}[X] .$$

The map $\alpha \mapsto \alpha^*$ is an *antiautomorphism* of $\mathcal{A}$, the trace a linear form, and the norm multiplicative, that is a *homomorphism* of (multiplicative) loops. Note $\alpha^{-1} = \mathrm{n}(\alpha)^{-1}\alpha^*$, if $\mathrm{n}(\alpha) \neq 0$, that is $\alpha \neq 0$. Sometimes the formula $\mathrm{n}(\alpha + \beta) = \mathrm{n}(\alpha) + \mathrm{n}(\beta) + \mathrm{tr}(\alpha\beta^*)$ is useful.

An important tool is the theorem 2.1.

THEOREM 2.1 (Artin). — *Subalgebras of alternative algebras are associative if they can be generated by two elements (and the center).*

This implies that there are only 4 types of subalgebras of $\mathcal{A}$ namely $\mathbb{Q}$, imaginary quadratic number fields, generalized definite quaternion division algebras over $\mathbb{Q}$ (all of them can be embedded) and $\mathcal{A}$. We do not need this fact but use Artin's result in order to save brackets writing $\alpha(\beta\gamma)\alpha^*$ instead of $\big(\alpha(\beta\gamma)\big)\alpha^* = \alpha\big((\beta\gamma)\alpha^*\big)$, for example. Note α^* is in the subalgebra generated by α (and $\beta\gamma$).

Finally I mention *Ruth Moufang's rules* which hold for all α, β, γ in an alternative algebra:

$$\begin{aligned} \alpha(\beta\gamma)\alpha &= (\alpha\beta)(\gamma\alpha) \\ \alpha\big(\beta(\alpha\gamma)\big) &= (\alpha\beta\alpha)\gamma \\ \big((\gamma\alpha)\beta\big)\alpha &= \gamma(\alpha\beta\alpha)\,. \end{aligned}$$

It is useful to equip $\mathcal{A}$ (or $\mathcal{A}\otimes\mathbb{R}$) with the *metric* defined by the positive definite bilinear form

$$\langle \alpha\,,\,\beta\rangle := \frac{1}{2}\,\mathrm{tr}(\alpha\beta^*)\,.$$

The absolute value (or length) of α in this metric is

$$|\alpha| = \sqrt{\langle \alpha\,,\,\alpha\rangle} = \sqrt{\mathrm{n}(\alpha)}\,.$$

We will have to use the *Schwarz* and *triangle inequalities*

$$\begin{aligned} \big|\langle \alpha\,,\,\beta\rangle\big| &\le |\alpha|\cdot|\beta| \\ |\alpha+\beta| &\le |\alpha| + |\beta|\,. \end{aligned}$$

If $|\alpha| = |\beta|$ then $\big|\langle \alpha\,,\,\beta\rangle\big| = |\alpha|\cdot|\beta|$ if and only if $\alpha = \beta$ or $\alpha = -\beta$.

$\alpha \in \mathcal{A}$ is called *integral* if $\mathrm{tr}(\alpha) \in \mathbb{Z}$ and $\mathrm{n}(\alpha) \in \mathbb{Z}$. Obviously

$$\mathcal{C}_0 := \sum_{i=0}^{7} \mathbb{Z}e_i$$

is an alternative ring of (integral) octaves and a $\mathbb{Z}$-lattice of rank 8 (that is, an *order* of $\mathcal{A}$). We will reserve henceforth the adjective *integral* for octaves in the maximal order $\mathcal{C}$ of $\mathcal{A}$ given by Coxeter's $\mathbb{Z}$-base $(1, e_1, e_2, e_3, h, e_1h, e_2h, e_3h)$ where $h = 1/2\,(e_1 + e_2 + e_3 - e_4)$. (In fact

Coxeter uses $-e_4$ and $-e_4h$ instead of e_3 and e_3h.) By exhibiting a fundamental domain of small diameter for the lattice $\mathcal{C}$ Coxeter [2] proves theorem 2.2 (see [2]).

THEOREM 2.2. — *For every $\lambda \in \mathcal{A}$ there is a $\gamma \in \mathcal{C}$ such that*

$$\mathrm{n}(\lambda - \gamma) \leq \frac{1}{2}.$$

We will use this in form of the corollary (apply the theorem to $\lambda = \alpha\beta^{-1}$).

COROLLARY 2.3. — *If $\alpha, \beta \in \mathcal{C}$ and $\beta \neq 0$ then there exist $\gamma, \rho \in \mathcal{C}$ such that $\alpha = \gamma\beta + \rho$ and $\mathrm{n}(\rho) \leq 1/2\,\mathrm{n}(\beta)$.*

This says that $\mathcal{C}$ is kind of (non associative) Euclidean domain. One could hope that the usual division algorithm computes common right divisors of α and β of maximal norm, as it does in associative Euclidean domains. But I have examples $\alpha = \alpha_0\pi$, $\beta = \beta_0\pi$ with $\alpha_0, \beta_0, \pi \in \mathcal{C}$, $\mathrm{n}(\pi) = 11$ where the algorithm stops at an element ρ_N of norm 1, or (for different α_0, β_0) with $\mathrm{n}(\rho_N) = 11$ but ρ_N is a right divisor of neither α nor β. The reason for this behaviour is that from $\rho = \alpha_0\pi - \gamma(\beta_0\pi)$ we cannot conclude $\rho = \rho_0\pi$ for some $\rho_0 \in \mathcal{C}$ because $\mathcal{C}$ is not associative. Nevertheless, in section 4 the reader will find an algorithm based on the corollary computing left or right factors of α and prescribed norm dividing $\mathrm{n}(\alpha)$.

3. Lattices and reduction mod p

A lattice M in $\mathcal{A}$ is, by definition, a rank 8 $\mathbb{Z}$-submodule of $\mathcal{A}$. For example, $\mathcal{C}_0$ and the maximal order $\mathcal{C}$ are lattices. If M is a lattice, and $0 \neq \alpha \in \mathcal{A}$, so is $M\alpha := \{\mu\alpha \mid \mu \in M\}$.

Many elementary properties of lattices in associative algebras hold for our lattices. In this paper lattices are only used to find the number of prime octaves of given norm p by reduction mod p. I give here only what is needed for this purpose.

LEMMA 3.1. — *If M is a lattice, $0 \neq \alpha \in \mathcal{C}$, and $M\alpha \subseteq M$ then the index (of Abelian groups) is*

$$(M : M\alpha) = \mathrm{n}(\alpha)^4.$$

Proof.— If $\alpha \in \mathbb{Q}$ then $\alpha \in \mathbb{Z}$, $\mathrm{n}(\alpha) = \alpha^2$, and $(M : M\alpha) = \alpha^8$. If $\alpha \notin \mathbb{Q}$ the minimal polynomial of the linear map $\mu \mapsto \mu\alpha$ is $f(X) = X^2 - \mathrm{tr}(\alpha)X + \mathrm{n}(\alpha)$ (use Artin's theorem to see this). The characteristic polynomial is $f(X)^4$. The determinant of the map is $\pm(M : M\alpha)$ by elementary divisor theory. This determinant is (up to a sign) the absolute term of the characteristic polynomial which is $\mathrm{n}(\alpha)^4$. □

This lemma will be applied to *principal lattices*, that is, the lattices $\mathcal{C}\alpha$, $0 \neq \alpha \in \mathcal{C}$. Since α, α^* and any third element generate an associative algebra one has $\mathcal{C}\mathrm{n}(\alpha) = \mathcal{C}(\alpha\alpha^*) = (\mathcal{C}\alpha)\alpha^*$ hence $(\mathcal{C}\alpha : \mathcal{C}\mathrm{n}(\alpha)) = (\mathcal{C} : \mathcal{C}\alpha) = \mathrm{n}(\alpha)^4$.

For most $\alpha \notin \mathbb{Q}$ the lattice $\mathcal{C}\alpha$ is not a left ideal of $\mathcal{C}$ since by a theorem of Mahler, van der Blij and Springer [1] the only left ideals of $\mathcal{C}$ are the $\mathcal{C}m$ with $m \in \mathbb{Z}$. However, for $m \in \mathbb{Z}$ the principal lattice $\mathcal{C}m$ is a twosided ideal and reduction mod m is a surjective homomorphism of alternative rings $\mathcal{C} \to \mathcal{C}/\mathcal{C}m := \overline{\mathcal{C}}$. In particular, for a prime number p, $\mathcal{C}/\mathcal{C}p := \overline{\mathcal{C}}$ is a simple alternative algebra over the Galois field $\mathbf{F}_p = \mathbb{Z}/\mathbb{Z}p$ hence isomorphic to Zorn's *vector matrix algebra* over $\mathbb{F}_p$. (See [1]; of course $\overline{\mathcal{C}}$ is a composition algebra with respect to the quadratic form

$$Q(\overline{\alpha}) := \overline{\mathrm{n}(\alpha)}$$

where overlining means forming classes mod p.)

Zorn's algebra consists of the *vector matrices*

$$A = \begin{pmatrix} a & \mathbf{b} \\ \mathbf{c} & d \end{pmatrix}, \quad a,\ d \in \mathbb{F}_p,\ \mathbf{b} = (b_1, b_2, b_3),\ \mathbf{c} = (c_1, c_2, c_3) \in \mathbb{F}_p^3.$$

Addition is as expected. The norm of A is $\mathrm{n}(A) = ad + \mathbf{bc}$. Here $\mathbf{bc} = b_1c_1 + b_2c_2 + b_3c_3$ is the usual scalar product of vectors. (In [1] and [9] the sign in the formula for $\mathrm{n}(A)$ is given as $-$, but only with $+$ this norm is multiplicative and the formula $A^2 - \mathrm{tr}(A)A + \mathrm{n}(A) = 0$ holds. I believe that there is a misprint in [9] copied in [1] since Zorn uses his formula later with the correct sign.)

For the multiplication which is not used in the proofs of this paper I refer to [1] or [9].

To count prime octaves we need lemma 3.2.

LEMMA 3.2.— *If p is a prime number then there are $(p^4 - 1)(p^3 + 1)$ classes $\overline{\alpha} \in \overline{\mathcal{C}} = \mathcal{C}/\mathcal{C}p$ such that $\overline{\alpha} \neq 0$ and $\overline{\mathrm{n}(\alpha)} = 0$.*

Proof. — Using the isomorphism between $\overline{\mathcal{C}}$ and the vector matrix algebra which respects norm and trace one sees that it is enough to count the vector matrices $A \neq 0$ such that $\mathrm{n}(A) = 0$ or the $0 \neq (a, d, \mathrm{b}, \mathrm{c}) \in \mathbb{F}_p^8$ such that $ad = -\mathrm{bc}$ which is easy. □

Finally I cite some properties of the *unit loop*

$$\mathcal{C}^\times := \{\varepsilon \in \mathcal{C} \mid \varepsilon^{-1} \in \mathcal{C}\} = \{\varepsilon \in \mathcal{C} \mid \mathrm{n}(\varepsilon) = 1\}.$$

PROPOSITION 3.3. — *There are* 240 *unit octaves. The following sequence of loops is exact:*

$$1 \to \{1, -1\} \to \mathcal{C}^\times \to (\mathcal{C}/\mathcal{C}2)^\times \to 1.$$

Proof. — See [1] or section 6.

COROLLARY 3.4. — *Let* $\omega \in \mathcal{C}$ *and* $\mathrm{n}(\omega)$ *odd. Then there is exactly one pair* $\pm\varepsilon$ *such that* $\varepsilon \in \mathcal{C}^\times$ *and* $\omega \equiv \varepsilon \bmod 2$ *(that is* $\omega - \varepsilon \in \mathcal{C} \cdot 2$*).*

Now the tools we need are ready, and we can start with our *elementary number theory of octaves*.

4. Right and left divisors

An integral octave $\mu \in \mathcal{C}$, $\mu \neq 0$, is called a *right (left) divisor* of $\alpha \in \mathcal{C}$ if $\alpha\mu^{-1} \in \mathcal{C}$ ($\mu^{-1}\alpha \in \mathcal{C}$, respectively). For *right* divisors, I use the notation $\mu \mid \alpha$. Unfortunately, this relation is not transitive. Because of $\mathcal{C}^* = \mathcal{C}$ conjugation furnishes a right-left duality, and every proposition about right divisors has a dual about left ones.

Units $\varepsilon \in \mathcal{C}^\times$ are characterized by dividing every $\alpha \in \mathcal{C}$. If $\beta = \varepsilon\alpha$, $\varepsilon \in \mathcal{C}^\times$, then $\mathcal{C}^\times\alpha \cap \mathcal{C}^\times\beta$ is not empty, but it may happen that $\mathcal{C}^\times\alpha \neq \mathcal{C}^\times\beta$.

By Artin's theorem (2.1), $\mu \mid \alpha$ if and only if $\mathrm{n}(\mu) \mid \alpha\mu^*$. If $\mu \mid \alpha$ and $\beta \in \mathcal{C}$ it may happen that μ is neither a right nor a left divisor of $\alpha\beta$ and $\beta\alpha$, even for units β. But a straightforward application of Moufang's identities establishes that for $\varepsilon \in \mathcal{C}^\times$, $\alpha, \beta \in \mathcal{C}$, $\alpha \neq 0$ the following relations are equivalent:

$$\alpha \mid \beta, \quad \varepsilon^*\alpha \mid \varepsilon\beta, \quad \alpha\varepsilon \mid \varepsilon\beta\varepsilon, \quad \varepsilon\alpha\varepsilon \mid \beta\varepsilon.$$

Similarly, if ρ, π, $\beta \in \mathcal{C}$, $\mathrm{n}(\pi) = p$ is a prime, and $\mathrm{n}(\rho) \not\equiv 0 \bmod p$ then the following congruences are equivalent:

$$\pi^*\beta \equiv 0 \bmod p, \quad (\rho\pi^*)(\beta\rho) \equiv 0 \bmod p, \quad (\rho\pi)^*(\rho\beta\rho) \equiv 0 \bmod p.$$

If we define, as usual, the *content* $c(\alpha)$ of $\alpha \in \mathcal{C}$ to be the largest rational integer dividing α then $c(\alpha)$ is the greatest common divisor of the coefficients of α in some $\mathbb{Z}$-base of $\mathcal{C}$. Then $\mu \mid \alpha$ is equivalent to the divisibility relation of rational integers $\mathrm{n}(\mu) \mid c(\alpha\mu^*)$.

$\beta \in \mathcal{C}$ is called *primitive* if $c(\beta) = 1$. We can write $\alpha \in \mathcal{C}$ uniquely in the form $\alpha = m\alpha_0$ such that α_0 is a primitive integral octave and m a natural number. (Of course $m = c(\alpha)$ does the job.) Since m is in the nucleus $\mathbb{Q}$ of $\mathcal{A}$ (that is, commutes and associates with everything) right and left divisors of α_0 are also right resp. left divisors of α.

$\pi \in \mathcal{C}$ is called a *prime* octave if $\mathrm{n}(\pi) = p$ is a prime number. If $p \mid \mathrm{n}(\alpha)$ for a primitive octave α we wish to find right prime divisors $\pi \mid \alpha$ with $\mathrm{n}(\pi) = p$. The formal Euclid division algorithm started at p, α need not end with such a π. But it can be replaced by the efficient algorithm described in the proof of proposition 4.1.

PROPOSITION 4.1. — *Let* $0 \neq \alpha \in \mathcal{C}$, $m \in \mathbb{N}$ *such that* $m \mid \mathrm{n}(\alpha)$. *Then there exist at least* 240 *right and* 240 *left divisors* μ *of* α *such that* $\mathrm{n}(\mu) = m$.

Proof. — First we prove the existence of μ, μ', α_1, $\alpha_1' \in \mathcal{C}$ such that $\alpha = \alpha_1\mu = \mu'\alpha_1'$ and $\mathrm{n}(\mu) = m = \mathrm{n}(\mu')$ by induction. For $m = 1$ we may use $\mu = \mu' = 1$. If $m > 1$ division of α by m gives γ, $\rho \in \mathcal{C}$ such that $\alpha = \gamma m + \rho$ and $\mathrm{n}(\rho) \leq (1/2)\,\mathrm{n}(m) = (1/2)\,m^2$ (see 2.3). If $\rho = 0$, we find an integral octave μ such that $m = \mathrm{n}(\mu) = \mu\mu^* = \mu^*\mu$ since, by a well known theorem of Lagrange's, every natural number is a sum of 4 squares. Then, by Artin's theorem 2.1, $\alpha = \gamma(\mu^*\mu) = (\gamma\mu^*)\mu$ and $\alpha = (\mu\mu^*)\gamma = \mu(\mu^*\gamma)$. If $\rho \neq 0$ then $1 \leq \mathrm{n}(\rho)$ and, because of $\mathrm{n}(\alpha) \equiv \mathrm{n}(\rho) \bmod m$, $\mathrm{n}(\rho) = m'm$ with $m' \in \mathbb{N}$ and $m' \leq (1/2)\,m < m$. By the induction hypothesis there exists a *left* divisor λ' of ρ such that $\rho = \lambda'\mu$, $\mu \in \mathcal{C}$, and $\mathrm{n}(\lambda') = m'$. $\mathrm{n}(\mu) = m$ follows. Now

$$\alpha = \beta(\mu^*\mu) + \lambda'\mu = (\beta\mu^*)\mu + \lambda'\mu = (\beta\mu^* + \lambda')\mu.$$

Hence μ is the desired *right* divisor of α. The left divisor μ' is found similarly.

To get more divisors the procedure in the proof is made a bit more explicit.

We have the following *algorithm*:

Start with $\rho_0 = \alpha$, $m_0 = m$, then compute γ_0, ρ_1 such that $\rho_0 = m_0\gamma_0 + \rho_1$ and $\mathrm{n}(\rho_1) \leq (1/2)\, m_0^2$. Suppose inductively that $\rho_i \in \mathcal{C}$ and $m_i \in \mathbb{N}$ have already been computed such that $m_i \mid \mathrm{n}(\rho_i)$. Stop if $m_i \mid \rho_i$ and set $N := i-1$. Otherwise compute integral γ_i and ρ_{i+1} with $\rho_i = \gamma_i m_i + \rho_{i+1}$ and $\mathrm{n}(\rho_{i+1}) \leq (1/2)\, m_i^2$ and put $m_{i+1} := (1/m_i)\,\mathrm{n}(\rho_{i+1})$. Obviously

$$\mathrm{n}(\rho_{i+1}) = \mathrm{n}(\rho_i) + m_i^2\,\mathrm{n}(\gamma_i) - m_i\,\mathrm{tr}(\gamma_i\rho_i^*) \equiv 0 \bmod m_i\,.$$

Hence m_{i+1} is an integer dividing $\mathrm{n}(\rho_{i+1})$, and because of $1 \leq m_{i+1} \leq (1/2)\, m_i < m_i$ the algorithm will terminate at some m_{N+1}. If now

$$\rho_{N+1} = \tau'_N\tau_{N+1} = \tau'_{N+1}\tau_N$$

such that τ'_N, τ_{N+1}, τ'_{N+1} and $\tau_N \in \mathcal{C}$ and $\mathrm{n}(\tau_{N+1}) = m_{N+1} = \mathrm{n}(\tau'_{N+1})$ we may obtain (recursively down) sequences $\tau_{N+1}, \tau_N, \ldots, \tau_0, \tau_{-1}$ and $\tau'_{N+1}, \tau'_N, \ldots, \tau'_0, \tau'_{-1}$ by defining

$$\begin{aligned}\tau_{i-1} &= (\tau'_i)^*\gamma_i + \tau_{i+1}\\ \tau'_{i-1} &= \tau_i^*\gamma_i + \tau'_{i+1}\,.\end{aligned}$$

By an easy induction (using Artin's theorem 2.1), we see that $\rho_i = \tau'_{i-1}\tau_i = \tau'_i\tau_{i-1}$ and $\mathrm{n}(\tau_i) = m_i = \mathrm{n}(\tau'_i)$ (for $i = N+1, \ldots, 0$). But note that the ρ_i and γ_i do not depend on the choice of τ_{N+1}, τ'_{N+1}. The formula $\rho_i = \tau'_{i-1}\tau_i$ shows that different τ_i force different τ'_{i-1}. Hence we will find at least as many different right (left) divisors τ_0 (resp. τ'_0) of $\alpha = \tau'_{-1}\tau_0 = \tau'_0\tau_{-1}$ with norm $m = m_0$ as we can find suitable τ_{N+1} and τ'_{N+1}. Now $\rho_{N+1} = \sigma m_{N+1}$, $\sigma \in \mathcal{C}$, by construction. There are at least 240 octaves $\lambda \in \mathcal{C}$ such that $m_{N+1} = \mathrm{n}(\lambda) = \lambda^*\lambda$ (take one and multiply it with units). We conclude $\rho_{N+1} = \sigma(\lambda^*\lambda) = (\sigma\lambda^*)\lambda$. Hence the $\tau_{N+1} := \lambda$ and $\tau'_N := \sigma\lambda^*$ will do the job. The τ'_{N+1} are found similarly. □

Remark.— If $m_{N+1} > 1$ the procedure gives more than 240 right and left divisors of α with norm m. If α is primitive and $m = p$ is an odd prime or if m and $\mathrm{n}(\alpha)/m$ are relatively prime then there are exactly 240 right divisors of this kind as will be shown in section 5. Hence in these cases the algorithm must stop at $m_{N+1} = 1$. For finding the right (left) prime divisors of a primitive α we simply use a table of the 240 units and need not solve equations of type $\mathrm{n}(\lambda) = \ell$ for $\ell > 1$.

Obviously the proposition (and the algorithm) can be used to factorize $\alpha \in \mathcal{C}$. Let us write

$$\prod_{i=0}^{n} \gamma_i = \left(\cdots\left((\gamma_0\gamma_1)\gamma_2\right)\cdots\right)\gamma_n\,.$$

Then we have (by induction on n) the corollary 4.2.

COROLLARY 4.2.— *Let* $\alpha \in \mathcal{C}$, $\mathrm{n}(\alpha) = m_1 \cdots m_n$, $m_1, \ldots, m_n \in \mathbb{N}$. *Then there are integral octaves* $\mu_1, \ldots, \mu_n$ *such that*

$$\alpha = \prod_{i=1}^{n} \mu_i \quad \textit{and} \quad \mathrm{n}(\mu_i) = m_i \quad (i = 1, \ldots, m)\,.$$

In fact one could prescibe any way of bracketing the product.

5. Unique factorization

The prime octave factors π of a prime number p are rather arbitrary and any π such that $\mathrm{n}(\pi) = p$ will do. On the other hand there holds proposition 5.1.

PROPOSITION 5.1.— *Let* τ, τ', μ, $\mu' \in \mathcal{C}$ *such that* $\alpha = \tau\mu = \tau'\mu'$, $\mathrm{n}(\mu) = \mathrm{n}(\mu')$ *is odd, and* $\mathrm{n}(\tau)$ *and* $\mathrm{n}(\mu)$ *are relatively prime. Then* $\mu \equiv \mu' \bmod 2$ *implies* $\mu = \mu'$ *or* $\mu = -\mu'$.

Proof.— Suppose the contrary. Then the Schwarz inequality says

$$\left|\langle \mu, \mu' \rangle\right| < \mathrm{n}(\mu)\,.$$

From $\mathrm{n}(\mu' - \mu) = 2\mathrm{n}(\mu) - \mathrm{tr}(\mu'\mu^*) = 2\big(\mathrm{n}(\mu) - \langle \mu', \mu \rangle\big)$ we conclude $0 < \mathrm{n}(\mu' - \mu) < 4\mathrm{n}(\mu)$, or $0 < \mathrm{n}(\beta) < \mathrm{n}(\mu)$ where $\beta := (1/2)\,(\mu' - \mu)$. Note $\beta \in \mathcal{C}$.

On the other hand $\tau\mu = \tau'\mu' = \tau'(2\beta + \mu)$ implies $(\tau - \tau')\mu = 2\tau'\beta$, and $\mathrm{n}(2\tau')$ divides $\mathrm{n}(\tau - \tau')\,\mathrm{n}(\mu)$. Since $\mathrm{n}(\mu)$ is odd and relatively prime to $\mathrm{n}(\tau') = \mathrm{n}(\tau)$ we see that $\mathrm{n}(2\tau')$ divides $\mathrm{n}(\tau - \tau')$. The equation $(\tau - \tau')\mu = 2\tau'\beta$ implies also

$$\mathrm{n}\big((\tau - \tau')\mu\big) = \mathrm{n}(2\tau')\,\mathrm{n}(\beta) < \mathrm{n}(2\tau')\,\mathrm{n}(\mu)\,,$$

that is $\mathrm{n}(\tau - \tau') < \mathrm{n}(2\tau')$, a contradiction since $\tau \neq \tau'$ and

$$\mathrm{n}(2\tau') \mid \mathrm{n}(\tau - \tau')\,. \;\square$$

Once for all we fix a *total ordering* of $\mathcal{C}$ making $\mathcal{C}$ an ordered additive group (e.g. lexicographic with respect to the coordinates in a fixed $\mathbb{Z}$-base of $\mathcal{C}$).

COROLLARY 5.2. — *Let* $\alpha \in \mathcal{C}$, $\mathrm{n}(\alpha) = um$, $u, m \in \mathbb{N}$ *relatively prime, and* m *odd. Then there are exactly* 240 *right divisors* $\mu \in \mathcal{C}$ *of* α *such that* $\mathrm{n}(\mu) = m$. *Exactly one of these divisors is* $\equiv 1 \bmod 2$ *and* > 0.

Proof. — Decompose the set $M = \{\mu \in \mathcal{C} \mid \mathrm{n}(\mu) = m,\ \mu \mid \alpha\}$ into classes mod 2. By proposition 5.1 and 4.1 every class contains 2 elements and there are at least 120 classes mod 2 represented by M. Because of $m = \mathrm{n}(\mu) \equiv 1 \bmod 2$ these correspond to elements of the loop $(\mathcal{C}/\mathcal{C}2)^\times$ which has, by proposition 3.3, exactly 120 elements. Hence $\{\overline{\mu} \mid \mu \in M\} = (\mathcal{C}/\mathcal{C}2)^\times$ and $\overline{1} = \overline{\mu}$ has a solution in M which can be made unique by requiring $\mu > 0$. □

COROLLARY 5.3 (Unique primary factorization). — *Let* $\alpha \in \mathcal{C}$,

$$\mathrm{n}(\alpha) = 2^{r_0} \cdot p_1^{r_1} \cdot \ldots \cdot p_t^{r_t}$$

with prime numbers $2 = p_0 < p_1 < \ldots < p_t$ *and* $r_0, \ldots, r_t \in \mathbb{N} \cup \{0\}$. *Then there exists exactly one "vector"*

$$(\omega_0, \ldots, \omega_t) \in \mathcal{C}^{t+1}$$

such that

1) $\alpha = \prod_{i=0}^{t} \omega_i$;

2) $\mathrm{n}(\omega_i) = p_i^{r_i}$ $(i = 0, \ldots, t)$;

3) $\omega_i \equiv 1 \bmod 2$ $(i = 1, \ldots, t)$;

4) $\omega_i > 0$ $(i = 1, \ldots, t)$.

Surprisingly there is also a corollary in the case of norms which are not relatively prime.

PROPOSITION 5.4. — *Let* p *be an odd prime number, and* $\alpha \in \mathcal{C}$ *such that* $p \mid \mathrm{n}(\alpha)$ *and* $p \nmid \alpha$. *If* $\tau, \pi, \tau', \pi' \in \mathcal{C}$, $\alpha = \tau\pi = \tau'\pi'$, *and* $\mathrm{n}(\pi) = \mathrm{n}(\pi') = p$, *then* $\pi \equiv \pi' \bmod 2$ *implies* $\pi = \pi'$ *or* $\pi = -\pi'$.

Proof. — By corollary 2.3, there exist $\rho, \gamma \in C$ such that $\alpha = \gamma p + \rho$ and $\mathrm{n}(\rho) \leq (1/2)\, p^2$. Obviously p divides $\mathrm{n}(\rho)$ hence $\mathrm{n}(\rho) = \ell p$. Because of $\ell \leq (1/2)\, p$ the numbers ℓ and p are relatively prime and we can apply proposition 5.1 to factorize ρ. But the right divisors π of α and ρ such that $\mathrm{n}(\pi) = \pi^* \pi = p$ are the same! □

The argument proving corollary 5.2 now yields corollary 5.5.

COROLLARY 5.5. — *Let p, α as in the proposition. Then there are exactly 240 right divisors $\pi \in C$ of α such that $\mathrm{n}(\pi) = p$. Exactly one of these divisors is $\equiv 1 \bmod 2$ and > 0.*

Adding the case $p = 2$ we get proposition 5.6.

PROPOSITION 5.6. — *If p is a prime > 2 then define*

$$\mathcal{P}(p) = \left\{ \pi \in C \mid \mathrm{n}(\pi) = p,\ \pi > 0,\ \pi \equiv 1 \bmod 2 \right\}.$$

Let $\mathcal{P}(2) = \{\pi_1, \ldots, \pi_9\}$ where (coordinates with respect to the base $1, e_1, \ldots, e_7$)

$$\pi_1 = (1,1,0,0,0,0,0,0)$$

$$\pi_2 = \frac{1}{2}(2,1,1,1,1,0,0,0)$$

$$\pi_3 = \frac{1}{2}(2,1,1,1,-1,0,0,0)$$

$$\pi_4 = \frac{1}{2}(2,1,1,0,0,1,0,1)$$

$$\pi_5 = \frac{1}{2}(2,1,1,0,0,1,0,-1)$$

$$\pi_6 = \frac{1}{2}(2,1,0,1,0,1,1,0)$$

$$\pi_7 = \frac{1}{2}(2,1,0,1,0,1,-1,0)$$

$$\pi_8 = \frac{1}{2}(1,2,1,1,0,1,0,0)$$

$$\pi_9 = \frac{1}{2}(1,2,-1,-1,0,-1,0,0).$$

If $\alpha \in C$, α is primitive, and $p \mid \mathrm{n}(\alpha)$ then there is exactly one right divisor π of α in $\mathcal{P}(p)$.

Proof. — It remains to check only the case $p = 2$. If $\alpha = 2\gamma + \rho$, $\mathrm{n}(\rho) \leq 2$, then $\rho \neq 0$ and $2 \mid \mathrm{n}(\rho)$, hence $\mathrm{n}(\rho) = 2$. The right divisors π of α and ρ such that $\mathrm{n}(\pi) = 2$ are the same. $\mathcal{P}(2)$ has the property that the set of all prime octaves of norm 2 is the disjoint union of the $C^{\times} \pi_i$ $(i = 1, \ldots, 9)$. □

Remark. — If $\pi, \pi' \in \mathcal{C}$, $\mathrm{n}(\pi) = \mathrm{n}(\pi') = 2$, and $\pi' \notin \mathcal{C}^\times \pi$, it may happen that $\mathcal{C}^\times \pi$ and $\mathcal{C}^\times \pi'$ are not disjoint since there is a loop not a group acting on the set of all primes of norm 2. The search for $\mathcal{P}(2) = \{\pi_1, \ldots, \pi_9\}$ is more difficult than in associative algebras. In fact it was done with the help of a computer. I do not know theorems describing in which cases (nonassociative) actions of loops decompose the set acted on in disjoint orbits as is customary in group theory. Here this is established for the unit loop acting on the set of all prime octaves of norm p, p a prime.

By induction one gets at once theorem 5.7.

THEOREM 5.7 (Unique prime factorization). — *Let α be a primitive integral octave with norm $\mathrm{n}(a) = p_1 \cdot \ldots \cdot p_r$ and $p_1, \ldots, p_r$ prime numbers (not necessarily different). Then there exists a unit $\varepsilon = \pi_0 \in \mathcal{C}^\times$ and prime octaves $\pi_i \in \mathcal{P}(p_i)$ (the sets of primes defined in the previous proposition) such that*

$$\alpha = \prod_{i=0}^{r} \pi_i .$$

$(\pi_0, \ldots, \pi_r)$ is uniquely determined by α.

Remark. — The prime factors π_i depend heavily on the sequel of the p_i chosen, and also on the bracketing of the product. Another unique factorization of α can be obtained by refining the primary decomposition from corollary 5.3:

$$\alpha = \omega_0 \cdots \omega_t .$$

Here $\alpha \equiv \omega_0 \bmod 2$ and $\omega_i \equiv 1 \bmod 2$. Applying our theorem to $\omega = \omega_j$ $(j = 1, \ldots, t)$, we have $1 \equiv \omega \equiv \pi_0 \bmod 2$ hence only a sign $\pi_0 = -1$ might be needed writing ω_j as a product of primes in $\mathcal{P}(p_j)$.

6. Prime octaves

In this section we want to find the number of prime octaves of given norm (without using Jacobi's formula).

LEMMA 6.1. — *Let $\alpha, \beta \in \mathcal{C}$, $m \in \mathbb{N}$ and $\mathrm{n}(\alpha) = \mathrm{n}(\beta) < (1/4)\, m^2$. Then $\alpha \equiv \beta \bmod m$ implies $\alpha = \beta$.*

Proof. — If $\beta = \alpha + m\gamma$ then $\gamma \neq 0$ would imply $\mathrm{n}(\gamma) \geq 1$. Considering

$$\mathrm{n}(\alpha + m\gamma) = \mathrm{n}(\alpha) + m^2\,\mathrm{n}(\gamma) + m\,\mathrm{tr}(\alpha\gamma^*)$$

our hypotheses imply that $m\mathrm{n}(\gamma) = \left|2\langle\alpha,\gamma\rangle\right| \leq 2\sqrt{\mathrm{n}(\alpha)}\sqrt{\mathrm{n}(\gamma)}$ contradicting $\mathrm{n}(\alpha) < (1/4)\,m^2$. □

Remark. — These methods furnish also a proof of proposition 3.3 shorter than that given in [1]. An element ε in the kernel of $\mathcal{C}^\times \mapsto (\mathcal{C}/\mathcal{C}2)^\times$ has the form $\varepsilon = 1 + 2\gamma$. The formula $m\mathrm{n}(\gamma) = \left|2\langle\alpha,\gamma\rangle\right|$ for $m = 2$ and $\alpha = 1$ and the Schwarz inequality imply $\mathrm{n}(\gamma) = \left|\langle 1,\gamma\rangle\right| \leq \sqrt{\mathrm{n}(1)}\sqrt{\mathrm{n}(\gamma)}$. If $\gamma \neq 0$, this is only possible if $\mathrm{n}(\gamma) = 1$ and the inequality is an equality. But this forces $\gamma = -1$ and $\varepsilon = -1$. Zorn's vector matrix algebra over $\mathbb{F}_2$ has 120 units. Hence reduction mod 2 of units must be surjective.

COROLLARY 6.2. — *For $m > 2$ reduction $\mathcal{C}^\times \mapsto (\mathcal{C}/\mathcal{C}m)^\times$ is an injective loop homomorphism.*

Proof. — $1 < \dfrac{1}{4}\,m^2$. □

COROLLARY 6.3. — *If $m \in \mathbb{N}$, $m > 4$, and $M := \{\alpha \in M \mid n(\alpha) = m\}$, then the reduction map $M \to \mathcal{C}/\mathcal{C}m$ is injective.*

Proof. — $m < \dfrac{1}{4}\,m^2$. □

Now we can deduce the proposition 6.4.

PROPOSITION 6.4

i) If p is an odd prime number then there are exactly p^3+1 prime octaves π such that $\mathrm{n}(\pi) = p$, $\pi \equiv 1 \bmod 2$, and $\pi > 0$.

ii) If p is any prime number then there are exactly $240(p^3+1)$ prime octaves of norm p.

Proof. — For $p = 2, 3$ this can be established easily by explicit enumeration (*cf.* [2] or use a computer). Let $p > 3$. We denote reduction mod p by overlining. Then $\mathcal{P}(p) = \mathcal{P}$ can be indentified (by the last corollary) with the subset $\overline{\mathcal{P}}$ of $N := \{\overline{\alpha} \in \overline{\mathcal{C}} \mid \overline{\mathrm{n}(\alpha)} = 0,\ \overline{\alpha} \neq 0\}$. For $\overline{\alpha}$ and $\overline{\beta}$ define $\overline{\alpha} \sim \overline{\beta}$ if there exists a $\pi \in \mathcal{P}$ such that $\overline{\alpha\pi^*} = 0 = \overline{\beta\pi^*}$. This means that π is a right divisor of representatives α, β of the classes $\overline{\alpha}$, resp. $\overline{\beta}$. Since $p \nmid \alpha$ but $p \mid \mathrm{n}(\alpha)$ we have, by proposition 5.6, a *unique* $\pi \in \mathcal{P}$ which is a

right divisor of α. This implies the transitivity of the relation $\sim$ which is therefore an equivalence relation. Obviously $\overline{\alpha} \sim \overline{\pi}$ hence we may take $\overline{\mathcal{P}}$ as a full set of representatives of the equivalence classes. The classes are $\overline{\mathcal{C}\pi}\setminus\{0\}$ and contain p^4-1 elements because $\left|\overline{\mathcal{C}\pi}\right| = (\mathcal{C}\pi : \mathcal{C}p) = \mathrm{n}(\pi)^4 = p^4$ (see lemma 3.1). Using the isomorphism between $\mathcal{C}/\mathcal{C}p$ and the Zorn algebra over $\mathbf{F}_p$ we conclude from lemma 3.2 that N contains $(p^4-1)(p^3+1)$ elements. Hence $\overline{\mathcal{P}}$ and $\mathcal{P}$ contain p^3+1 elements. ii) follows easily by applying theorem 5.7 to prime α.

7. Arithmetics in p-adic vector matrix algebras

Let p be a prime number, $\mathbb{Q}_p$ the p-adic completion of $\mathbb{Q}$ and $\mathbb{Z}_p$ that of $\mathbb{Z}$. The unit group of $\mathbb{Z}_p$ is denoted by $\mathbb{Z}_p^\times$. Then $\mathcal{A}_p = \mathcal{A}\otimes\mathbb{Q}_p$ is an alternative algebra and $\mathcal{C}_p := \mathcal{C}\otimes\mathbb{Z}_p$ a maximal order. If $\alpha\in\mathcal{A}$ and $\alpha\otimes 1$ are identified then $\mathcal{A}$ is dense in $\mathcal{A}_p$, and $\mathcal{C}$ in $\mathcal{C}_p$ with respect to the topology given by the filtration $\mathcal{C}_p p^n$, $n\in\mathbb{N}$. But $\mathcal{A}_p$ splits hence is isomorphic to the Zorn vector matrix algebra (see section 2) over $\mathbb{Q}_p$ (we denote it by $\mathcal{Z}(\mathbb{Q}_p)$), and the isomorphism may be chosen such that it identifies $\mathcal{C}_p$ with the ring $\mathcal{Z}(\mathbb{Z}_p)$ of vector matrices with p-integral entries (*cf.* [1]). The idea is now that embedding the special set of prime octaves $\mathcal{P}(p)$ one gets a prime factorization theory in $\mathcal{C}_p$.

THEOREM 7.1. — *Let* $0\neq\alpha\in\mathcal{C}_p$, $\mathrm{n}(\alpha)\in\mathbb{Z}_p^\times p^n$, *and* $\alpha\notin\mathcal{C}_p p$. *Then*

$$\alpha = \prod_{i=0}^{t}\pi_i\,,$$

where $\pi_0\in\mathcal{C}_p^\times = \{\varepsilon\in\mathcal{C}_p \mid \mathrm{n}(\varepsilon)\in\mathbb{Z}_p^\times\}$, *and* $\pi_i\in\mathcal{P}(p)$ *for* $i=1,\ldots,n$, *and* $(\pi_0,\ldots,\pi_n)$ *is uniquely determined by* α.

Proof. — The case $n=0$ is trivial. Suppose $n>0$. By density $\alpha\equiv\beta \bmod p^{n+1}$ for some $\beta\in\mathcal{C}$. Because there is a unique right divisor $\pi_n\in\mathcal{P}(p)$ of β (see proposition 5.6) the same holds for α. Induction concludes the proof. □

Remark. — The theorem yields a similar theorem for the Zorn vector matrix algebra over $\mathbb{Q}_p$. But $\mathcal{P}(p)$ is described globally by a condition mod 2 which is not natural in $\mathcal{C}_p$. For a purely local proof we need a set of vector matrices $\mathcal{P}$ defined locally such that

$$N := \{\gamma\in\mathcal{Z}(\mathbb{Z}_p) \mid \mathrm{n}(\gamma)\equiv 0 \bmod p,\ p\nmid\gamma\}$$

is the disjoint union of the $\mathcal{Z}(\mathbb{Z}_p)\pi \setminus \mathcal{Z}(\mathbb{Z}_p)p$, $\pi \in \mathcal{P}$. From

$$\alpha_1\pi_1 = \alpha_2\pi_2 \not\equiv 0 \bmod p \quad \text{and} \quad \pi_1,\ \pi_2 \in \mathcal{P}\,,$$

we should be able to conclude $\pi_1 = \pi_2$. Inspired by matrix algebras one would perhaps expect that the set of vector matrices

$$\left\{ \begin{pmatrix} 1 & \mathbf{x} \\ 0 & p \end{pmatrix}, \begin{pmatrix} p & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \right\}$$

(where $\mathbf{x} \in \mathbb{Z}_p^3$ form a set of representatives of $\mathbb{F}_p^3$) will do the job. However, if $\mathbf{yx} = 0$ and $\mathbf{y}$ is primitive in $\mathbb{Z}_p^3$ then

$$\begin{pmatrix} p & -\mathbf{x} \\ \mathbf{y} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{x} \\ 0 & p \end{pmatrix} = \begin{pmatrix} p & \mathbf{0} \\ \mathbf{y} & p \end{pmatrix}$$

shows that the primitive vector matrix on the right side has p^2 right divisors in the set suggested. Since this defect is visible $\bmod p$ the main difficulty seems to be at work already $\bmod p$.

I mention (without the straightforward proofs) that the units behave rather as expected. The unit loop $H_0 := \mathcal{Z}(\mathbb{Z}_p)^\times$ has a filtration by normal subloops $H_n := 1 + \mathcal{Z}(\mathbb{Z}_p)p^n$ and the sequences of loops

$$1 \to H_1 \to H_0 \to \big(\mathcal{Z}(\mathbb{F}_p)\big)^\times \to 1$$
$$1 \to \mathcal{Z}(\mathbb{Z}_p)p^{n+1} \to \mathcal{Z}(\mathbb{Z}_p)p^n \to H_n/H_{n+1} \to 1 \quad (n \geq 1)$$

are exact. H_n/H_{n+1} is isomorphic to the additive group $\mathbb{F}_p^8$ hence commutative and associative. Trying to approximate $\bmod p^n$ nonassociativity will be felt most at the first step.

8. Counting integral octaves

Most of the results in this section are not new. They are easily proved by using Jacobi's formula about sums of 8 squares. Here we do the converse: Using only the arithmetic of octaves a new proof of Jacobi's formula is possible.

PROPOSITION 8.1

i) If $m \in \mathbb{N}$ and $m = \prod_{p|m} p^{n_p}$ is the prime factorization of m then the number of primitive octaves $\mu \in \mathcal{C}$ such that $\mathrm{n}(\mu) = m$ is

$$\mathrm{pr}(m) := 240 \prod_{p|m} (p^3+1)p^{3(n_p-1)}\,.$$

ii) If $2 \nmid m$ *then are* $(1/240)\,\mathrm{pr}(m)$ *primitive octaves* $\mu \in \mathcal{C}$ *such that* $\mathrm{n}(\mu) = m$, $\mu \equiv 1 \bmod 2$ *and* $\mu > 0$.

Proof.— If α, $\beta \in \mathcal{C}$, $\beta \neq 0$ the coordinates of $\alpha\beta$ are obtained from those of α by means of a linear transformation with integral coefficients. Hence, for the contents, $\mathrm{c}(\alpha) \mid \mathrm{c}(\alpha\beta)$. Obviously, $\mathrm{c}(\alpha) = \mathrm{c}(\alpha^*)$, and $\mathrm{c}(\alpha)^2 \mid \mathrm{n}(\alpha)$. If in addition $\mathrm{n}(\alpha)$ and $\mathrm{n}(\beta)$ are relatively prime and $\mathrm{c}(\alpha) = \mathrm{c}(\beta) = 1$ we conclude $\mathrm{c}(\alpha\beta) \mid \mathrm{c}(\alpha\beta\beta^*) = \mathrm{n}(\beta)\mathrm{c}(\alpha) = \mathrm{n}(\beta)$. Similarly $\mathrm{c}(\alpha\beta) \mid \mathrm{n}(\alpha)$, therefore $\mathrm{c}(\alpha\beta) = 1$. Hence, in the unique primary factorization of α (see corollary 5.3) the factors ω_i are primitive if and only if α is primitive. If follows that $\mathrm{pr}(m)$ is the product of factors c_p, where c_p is the number of primitive ω such that $\mathrm{n}(\omega) = p^{n_p}$, $\omega \equiv 1 \bmod 2$, and $\omega > 0$ if p is an odd prime divisor of m, and $c_2 = \mathrm{pr}(2^{n_2})$. Now factorize ω uniquely according to theorem 5.7:

$$\omega = \prod_{i=0}^{n_p} \pi_i\,, \quad \mathrm{n}(\pi_i) = p \quad (i > 0)\,.$$

Note $\pi_0 = 1$ or -1 and just one of the signs makes $\omega > 0$ if $(\pi_1, \ldots, \pi_r)$ is given. If now γ is a primitive octave and π a prime octave with $\mathrm{n}(\pi) = p$ then $\mathrm{c}(\gamma\pi) \mid \mathrm{c}(\gamma\pi\pi^*) = p$. Hence $\gamma\pi$ remains primitive if and only if π^* is not a right divisor of γ. To obtain all primitive ω we may chose π_1 arbitrary in $\mathcal{P}(p)$ (p^3+1 possibilities), and for the following π_i the one prime octave in $\mathcal{P}(p)$ making the product imprimitive has to be excluded (p^3 possibilities). In total there are $(p^3+1)p^{3(n_p-1)}$ ω's. The same reasoning for $p = 2$ (but now $\pi_0 \in \mathcal{C}^\times$ is arbitrary) yields $\mathrm{pr}(2^r) = 240 \cdot 9 \cdot 8^{r-1}$. □

COROLLARY 8.2.— *If* $\tau_3(m)$ *denotes the sum of the third powers of the natural divisors* d *of* $m \in \mathbb{N}$ *then the number* $\mathrm{oct}(m)$ *of* $\alpha \in \mathcal{C}$ *such that* $\mathrm{n}(\alpha) = m$ *is*

$$\mathrm{oct}(m) = 240 \cdot \tau_3(m)\,.$$

Proof.— Since $\alpha = \mathrm{c}(\alpha)\alpha_0$, α_0 primitive, and $\mathrm{n}(\alpha) = \mathrm{c}(\alpha)^2\,\mathrm{n}(\alpha_0)$ we see

$$\mathrm{oct}(m) = \sum_{d^2 \mid m} \mathrm{pr}\Big(\frac{m}{d^2}\Big)\,.$$

By the proposition evidently $(1/240)\,\mathrm{pr}(m)$ is a (weakly) multiplicative number theoretical function and by Möbius summation so are $\tau_3(m)$ (as

is well known) and $(1/240)\,\mathrm{oct}(m)$. Hence it is sufficient to prove the corollary for $m = p^r$, p a prime. Since there are $\mathrm{oct}(p^i)$ imprimitive and $\mathrm{pr}(p^{i+2})$ primitive integral octaves of norm p^{i+2} there holds $\mathrm{oct}(p^{i+2}) = \mathrm{oct}(p^i) + \mathrm{pr}(p^{i+2})$. The result follows now from the proposition by an easy induction. □

Finally we want to discuss the consequences for the norm form $\sum_{i=0}^{7} x_i^2$ of the (nonmaximal) order $\mathcal{C}_0$. We begin with the "difficult" prime 2 dividing $(\mathcal{C} : \mathcal{C}_0)$.

PROPOSITION 8.3. — *Let* $\lambda \in \mathcal{C}$, $\mathrm{n}(\lambda) = 2^t$, $t \in \mathbb{N}$.

i) λ *is primitif if and only if* $\lambda \equiv \pi \bmod 2$ *for some* $\pi \in \mathcal{C}$ *such that* $\mathrm{n}(\pi) = 2$.

ii) If $\pi \in \mathcal{C}$, $\mathrm{n}(\pi) = 2$, *then the number of elements* $\lambda \in \mathcal{C}$ *such that* $\mathrm{n}(\lambda) = 2^t$ *and* $\lambda \equiv \pi \bmod 2$ *is* $2 \cdot 8^t$.

Proof. — i) is seen by dividing λ by 2 with residue π. ii) is correct for $t = 1$ as can be established by explicitely writing down the λ for any π. (Even if it is enough to take $\pi \in \mathcal{P}(2)$ from proposition 5.6 one better uses a computer to do this since there are $240 \cdot 9$ octaves λ to consider.)

Let $t > 1$. $\overline{\lambda} = \overline{\pi}$ and $\mathrm{n}(\lambda) = 2^t$ implies $\lambda = \tau\pi$ with a unique primitive $\tau \in \mathcal{C}$, and $\mathrm{n}(\tau) = 2^{t-1}$. By i), $\overline{\tau} = \overline{\alpha}$ for some $\alpha \in \mathcal{C}$ such that $\mathrm{n}(\alpha) = 2$. Now $\overline{\lambda} = \overline{\pi}$ is equivalent to $(\overline{\alpha} - 1)\overline{\pi} = 0$. This is again a statement about elements of norm 2 only. By explicit enumeration using a computer one sees that for every π there are exactly 8 such classes $\overline{\alpha} \in \mathcal{C}/\mathcal{C}2$ such that $(\overline{\alpha} - 1)\overline{\pi} = 0$. The induction hypothesis says that there exist exactly $2 \cdot 8^{t-1}$ octaves $\alpha \in \mathcal{C}$ such that $\overline{\tau} = \overline{\alpha}$, and $\mathrm{n}(\tau) = 2^{t-1}$. This number must be multiplied by 8 to find then number of λ's. This completes the induction. □

COROLLARY 8.4. — *The number of primitive* $\lambda \in \mathcal{C}_0$ *such that* $\mathrm{n}(\lambda) = 2^t$, $t \in \mathbb{N}$ *is* $7 \cdot 2 \cdot 8^t$.

Proof. — $\lambda \in \mathcal{C}_0$ is equivalent to $\overline{\lambda} \subset \mathcal{C}_0$. Exactly 112 of the $\pi \in \mathcal{C}$ such that $\mathrm{n}(\pi) = 2$ belong to $\mathcal{C}_0$. Hence exactly 7 of the classes $\overline{\pi}$ are in $\mathcal{C}_0$. By the proposition, each of these classes contains $2 \cdot 8^t$ of the λ's. □

Note $2\mathcal{C} \subset \mathcal{C}_0$. Hence $\mathrm{n}(\lambda) = 2^t$, $\lambda \in \mathcal{C}_0$, and λ imprimitive is equivalent to $(1/2)\,\lambda \in \mathcal{C}$. The number of these λ is the number of all $\tau \in \mathcal{C}$ such that $\mathrm{n}(\tau) = 2^{t-2}$ which we found (in corollary 8.2) to be $240 \cdot \tau_3(2^{t-2})$. Adding the number of primitive λ one gets corollary 8.5.

COROLLARY 8.5. — *Denote the number of* $\lambda \in \mathcal{C}_0$ *such that* $\mathrm{n}(\lambda) = m$ *by* $\mathrm{oct}_0(m)$. *Then* $\mathrm{oct}_0(1) = 16$, $\mathrm{oct}_0(2) = 14 \cdot 8$ *and, for* $t > 1$, $t \in \mathbb{N}$

$$\mathrm{oct}_0(2^t) = 14 \cdot 8^t + 240 \cdot \tau_3(2^{t-2}) .$$

Discussing general $\lambda \in \mathcal{C}_0$, $\mathrm{n}(\lambda) = 2^t \cdot m$, $2 \nmid m$ we factorise λ uniquely:

$$\lambda = \gamma\mu,\ \gamma, \mu \in \mathcal{C}, \quad m = \mathrm{n}(\mu) \equiv 1 \bmod 2,\ \mu > 0 .$$

Because of $\gamma \equiv \lambda \bmod 2$ the octave λ is in $\mathcal{C}_0$ if and only if γ is in $\mathcal{C}_0$. Since the number of such μ (they are automatically in $\mathcal{C}_0$) is, by corollary 8.2, $\tau_3(m)$ we have shown proposition 8.6.

PROPOSITION 8.6. — *Let* $m \in \mathbb{N}$, $2 \nmid m$, $t \in \mathbb{N}$ *or* $t = 0$. *Then* $\mathrm{oct}_0(2^t \cdot m) = \mathrm{oct}_0(2^t) \cdot \tau_3(m)$ *(for the first factor see the previous corollary).*

Obviously, $\mathrm{oct}_0(2^t m)$ is the number of representations of $2^t m$ as a sum of 8 squares which is known to be

$$\frac{16}{7}\,\tau_3(m)\left|8^{t+1} - 15\right| \quad \text{(Jacobi's formula)} .$$

Summing the series on sees $\tau_3(2^{t-2}) = (1/7)\,(8^{t-1} - 1)$, so the formula in the proposition and Jacobi's say the same.

References

[1] VAN DER BLIJ (F.) and SPRINGER (T. A.) . — *The arithmetics of octaves and the group* G_2, Proc. Nederl. Akad. Wet. 1959, pp. 406-418.

[2] COXETER (H. S. M.) . — *Integral Cayley numbers*, Duke math. J. **13** (1946), pp. 561-578.

[3] HURWITZ (A.) . — *Über die Zahlentheorie der Quaternionen*, Math. Werke, Bd. **2**, pp. 303-330.

[4] JACOBI (C. B.) Ges. Werke, Bd. **1**.

[5] LAMONT (P. J. C.) . — *The number of Cayley integers of given norm*, Proc. Edinburgh Math. Soc. **25** (1982).

[6] PALL (G.) and TAUSSKY (O.) . — *Factorization of Cayley numbers*, J. Number Theory **2** (1970), pp. 74-90.

[7] RANKIN (R. A.) . — *A certain class of multiplicative functions*, Duke Math. J. **13** (1946), pp. 281-306.

[8] SCHAFER (R. D.) . — *An Introduction to Nonassociative Algebras*, Academic Press, New York and London (1966).

[9] ZORN (M.) . — *Alternativkörper und quadratische Systeme*, Abh. Math. Sem. Hamburg Univ. **9** (1933), pp. 393-402.