Jordanizing Discriminant forms

Fabian Werner

September 2, 2013

Abstract

We show that every discriminant form $\mathcal{D} = (D, Q)$ possesses a Jordan decomposition, i.e. can be almost diagonalized, see Thm. 1.

Let D be a finite abelian group. A finite quadratic form is a map $Q : D \to \mathbb{Q}/\mathbb{Z}$ such that

(i) $(\gamma, \delta) := Q(\gamma + \delta) - Q(\gamma) - Q(\delta)$ is a (symmetric!) $\mathbb{Z}$-bilinear map that is non-degenerate in the sense that $D^\perp = \{0\}$.

(ii) $Q(a\gamma) = a^2 Q(\gamma)$ for all $a \in \mathbb{Z}, \gamma \in D$.

A touple $\mathcal{D} = (D, Q)$ consisting of a finite abelian group D (written additively) and a finite quadratic form $Q : D \to \mathbb{Q}/\mathbb{Z}$ is called a discriminant form. Every finite abelian group is isomorphic to a finite direct product of copies of cyclic groups $\mathbb{Z}_{p^e}$ for primes p and exponents e. A finite basis of D is a set $\gamma_1, ..., \gamma_n$ such that

(i) The γ_i generate D as a $\mathbb{Z}$-module, i.e. for every element $\mu \in D$ there are $\lambda_1, ..., \lambda_n \in \mathbb{Z}$ such that

$$\mu = \sum_{i=1}^{n} \lambda_i \gamma_i$$

(ii) The γ_i are 'linearely independent' meaning that whenever $\sum_{i=1}^n \lambda_i \gamma_i = 0$ for some $\lambda_i \in \mathbb{Z}$, then

$$\lambda_i \equiv 0 \mod \operatorname{ord}(\gamma_i)$$

where $\operatorname{ord}(\delta)$ is the (additive) order of the element δ.

In this short note we want to show the following:

Theorem 1. *For every discriminant form $\mathcal{D} = (D, Q)$ there exists a Jordan splitting. That means that D is the* ***orthogonal*** *direct sum over components C where C is one of the following:*

1. *$C \cong \mathbb{Z}_{p^e}$ for some odd prime p and C is generated by a single element γ with $(\gamma, \gamma) = \frac{a}{p^e}$ where $a \in \mathbb{Z}, \gcd(a, p) = 1$ and $Q(\gamma) = \frac{2^{-1}a}{p^e} + \mathbb{Z}$ where the inversion of 2 takes place in $\mathbb{Z}_{p^e}$.*

2. *$C \cong \mathbb{Z}_{2^e}$ is generated by a single element γ with $(\gamma,\gamma) = \frac{a}{2^e}$ where $a \in \mathbb{Z}, \gcd(a,2) = 1$ and $Q(\gamma) = \frac{a+v2^e}{2^{e+1}} + \mathbb{Z}$ where v is either 0 or 1.*

3. *$C \cong \mathbb{Z}_{2^e} \times \mathbb{Z}_{2^e}$ is generated by two elements γ, δ such that the Gram matrix of pairings of γ and δ is given by*

$$2^{-e}\begin{pmatrix} x & 1 \\ 1 & x \end{pmatrix}$$

where x is either 0 or 2. If $x = 0$ then $Q(\gamma) = Q(\delta) = 0 + \mathbb{Z}$. We say that this is a block of type (A). If $x = 2$ then $Q(\gamma) = Q(\delta) = \frac{1}{2^e} + \mathbb{Z}$. We say that this is a block of type (B).

Proof. Throughout, $\mathbf{Q}_p$ will denote the p-adic numbers, $\mathbf{Z}_p$ will denote the p-adic integers and $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$.
Every $\alpha \in \mathbf{Q}_p$ can be written uniquely as a p-adic expansion of the form

$$\alpha = \alpha_N p^N + \alpha_{N+1} p^{N+1} + \alpha_{N+2} p^{N+2} + ... = \sum_{n=N}^{\infty} \alpha_n p^n$$

for some $N \in \mathbb{Z}$ and $\alpha_n \in \{0, 1, ..., p-1\}$. Furthermore,

$$\alpha \in \mathbf{Z}_p \iff N \geq 0$$

and

$$\alpha \in \mathbf{Z}_p^\times \iff \alpha \in \mathbf{Z}_p \text{ and } \alpha_0 \neq 0$$

For $\alpha = \sum_{n=0}^{\infty} \alpha_n p^n \in \mathbf{Z}_p$ and $e \in \mathbb{N}$ we define

$$R_{p^e}(\alpha) := \alpha_0 p^0 + ... + \alpha_{e-1} p^{e-1}$$

Depending on the context, we view $R_{p^e}(\alpha)$ as an element in $\mathbb{Z}$ or as an element in $\mathbb{Z}_{p^e}$. If we view R_{p^e} as a map from $\mathbf{Z}_p$ to $\mathbb{Z}_{p^e}$, i.e. it can be considered to take α modulo p^e, then some straightforward computations (that just involve the p-adic expansions of the elements) show that it is a ring homomorphism. Let $\mathcal{D} = (D, Q)$ be a discriminant form. By basic algebra (see e.g. [1], Satz 5.16), we can write $D \cong \oplus_{p \in \mathbb{P}} D_p$ and every p-part of D is of the form $D_p \cong \oplus_{e \in \mathbb{N}} (\mathbb{Z}_{p^e})^{r(e)}$ with almost all $r(e) \in \mathbb{N}$ being zero. We concentrate on one single p-part D_p. Let $\gamma_1, ..., \gamma_n$ be a basis in the sense that

$$\Phi_p : X := \mathbb{Z}_{p^{e_1}} \times ... \times \mathbb{Z}_{p^{e_n}} \to D_p, \quad (a_1, ..., a_n) \mapsto \sum a_i \gamma_i$$

is an isomorphism. Let E be the maximum of all e_i. We choose fixed representatives $(\gamma_i, \gamma_j) = a_{ij}/p^E + \mathbb{Z}$ (some of the integers a_{ij} may be divisiple by p). We choose them in such a way that $a_{ij} = a_{ji}$. This is possible as $(\gamma_i, \gamma_j) = (\gamma_j, \gamma_i)$. We define $G := (a_{ij})_{i,j=1,...,n} \in \mathbb{Z}^{n \times n}$. We claim that this matrix is non-degenerate over $\mathbf{Q}_p$:

Assume there was a vector $\tilde{v} \in \mathbf{Q}_p^n$ such that $\tilde{v} \neq 0$ and $G\tilde{v} = 0$. By multiplying $\tilde{v}$ with a certain p-power if necessary, we may assume that $\tilde{v} \in \mathbf{Z}_p^n$

and there is one entry $\tilde{v}_{i_0} \in \mathbf{Z}_p^\times$ (here we need $v \neq 0$!). Let $v_i := R_{p^E}(\tilde{v}_i) \in \mathbb{Z}_{p^E}$ and put $v := (R_{p^{e_i}}(v_i))_{i=1,\ldots,n}) \in X$. Put

$$\delta := \Phi_p(v) = \sum_i v_i \gamma_i$$

then we claim that $\delta \in D^\perp$:

$$(\delta, \gamma_j) = \sum_i v_i(\gamma_i, \gamma_j) = p^{-E} \sum_i v_i \underbrace{a_{ij}}_{=a_{ji}}$$

As the reduction maps are ring (and therefore $\mathbb{Z}$-module-)homomorphisms,

$$\begin{aligned} 0 = (G\tilde{v})_j &= \sum_i a_{ji}\tilde{v}_i \\ \Rightarrow 0 \equiv R_{p^E}(0) &\equiv R_{p^E}(\sum_i a_{ji}\tilde{v}_i) \\ &\equiv \sum_i a_{ji} R_{p^E}(\tilde{v}_i) \equiv \sum_i a_{ji} v_i \mod p^E \end{aligned}$$

Hence,

$$(\delta, \gamma_j) = p^{-E} \underbrace{\sum_i a_{ji} v_i}_{\equiv 0 \mod p^E} + \mathbb{Z} = 0 + \mathbb{Z}$$

therefore, $\delta \in D^\perp$. By assumption on discriminant forms, this means $\delta = 0$ in D. As Φ_p was an isomorphism (i.e. injective) this means that in particular $v_{i_0} \equiv 0 \mod p^{e_{i_0}}$ but v_{i_0} is not divisible by p as $\tilde{v}_{i_0} \in \mathbf{Z}_p^\times$. Contradiction.
Considering G as a (nonsingular!) symmetric matrix in $\mathbf{Z}_p^{n\times n}$, we can apply the machinery in [2] Chapter 15, §4.4, pp. 396-397. Therefore, we get a matrix $S \in \mathrm{GL}_n(\mathbf{Z}_p)$ with the property that $S^T G S$ is diagonal (if p was odd) or $S^T G S$ is almost diagonal if $p = 2$ meaning that it consists ("diagonally") of matrices

$$2^\nu(a), a \in \mathbf{Z}_2^\times \quad \text{or} \quad 2^\nu \begin{pmatrix} a & b \\ b & c \end{pmatrix}, 2|a, 2|c, 2 \nmid b, 2 \nmid ac - b^2$$

In fact, one can do even better: These 2-by-2-blocks are isomorphic over $\mathbf{Z}_2$ to

$$\text{either } 2^\nu \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ or } 2^\nu \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \tag{1}$$

see [3]. Let

$$S = \begin{pmatrix} s_{11} & s_{12} & \ldots \\ s_{21} & s_{22} & \ldots \\ \vdots & & \\ s_{n1} & s_{n2} & \ldots \end{pmatrix}$$

the we set

$$\begin{aligned}\delta_1 &:= s_{11}\gamma_1 + s_{21}\gamma_2 + ... + s_{n1}\gamma_n\\ \delta_2 &:= s_{12}\gamma_1 + s_{22}\gamma_2 + ... + s_{n2}\gamma_n\\ &\vdots\\ \delta_n &:= s_{1n}\gamma_1 + s_{2n}\gamma_2 + ... + s_{nn}\gamma_n\end{aligned}$$

i.e. the new coordinates are the columns of S. A straightforward matrix multiplication gives

$$(\delta_i, \delta_j) = \frac{R_{p^E}((S^TGS)_{ij})}{p^E} + \mathbb{Z}$$

For the sake of readability, we choose fixed representatives $a'_{ij} \in \mathbb{Z}$ of $R_{p^E}((S^TGS)_{ij})$. Now, because of the simple structure of S^TGS, if we write down the matrix (we do not want to call it Gram matrix as we do not know yet whether and in which sense the δ_i form a "basis") $H := ((\delta_i, \delta_j))_{i,j=1,...,n}$ then H is an orthogonal sum of matrices of type $(a/p^E), a \in \mathbb{Z}$ (if p is odd) or of matrices of the type $(a/2^E), a \in \mathbb{Z}$ or $2^{-E+\nu}\begin{pmatrix} a & b \\ b & c \end{pmatrix}, 2|a, 2|c, 2 \nmid b, 2 \nmid ac - b^2, a, b, c \in \mathbb{Z}$ if $p = 2$ (and we can assume $b = 1$ and $a = c = 0$ or $a = c = 2$ if we wish, see (1)). Now we kill all p-divisors in the diagonal blocks, i.e. we rewrite (a/p^E) to (a'/p^e) where now, e varies but $\gcd(a', p) = 1$. We also rewrite $2^{-E+\nu}\left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ just to $2^{-\nu'}\left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$. Now we resort the δ_i in a way such that the exponents e or ν' are ordered, i.e. $H + \mathbb{Z}$ becomes a matrix which consists of (almost) diagonal blocks $H_e + \mathbb{Z}$ and $H_e + \mathbb{Z}$ is $p^{-e}H'_e + \mathbb{Z}$ and $H'_e + \mathbb{Z}$ is either a diagonal matrix with $\gcd(\det(H'_e), p) = 1$ (if p is odd) or a matrix that consists of either odd diagonal entries or 2-by2-blocks $A = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ with $2|a, 2|c, 2 \nmid c, 2 \nmid \det(A)$. Remember that after the simplification as in equation (1) we can even assume $b = 1$ and $a = c = 0$ or $a = c = 2$ but in order to avoid unnecessary case distinctions we will still view them as blocks with arbitrary a, b, c like in A above from time to time.
In the case that p is odd, let us rename $\delta_1, ..., \delta_n$ to $\delta_{1,1}, ..., \delta_{1,n_1}, \delta_{2,1}, ..., \delta_{2,n_2}, ...\delta_{e,j}$ according to their exponents e (and j runs from 1 to n_e for every fixed e). If $p = 2$ and e is fixed, then we fix the order such that the 2-by-2-blocks come first (hence, two δ's) and then there is some diagonal part where we rename the δ's to α's, so $\delta_1^{(e)}, \mu_1^{(e)}, \delta_2^{(e)}, \mu_2^{(e)}, ...\delta_r^{(e)}, \mu_r^{(e)}, \alpha_1^{(e)}, ..., \alpha_s^{(e)}$, $e = e_1, e_2, ..., e_A$. The set of all these vectors will now be referred to as the 'selected' vectors. Their pairings are given by / will be denoted by the following:

If p is odd, then $\delta_{e_i,j}$ is orthogonal to all other selected vectors and

$$(\delta_{e_i,j}, \delta_{e_i,j}) = \frac{a_{e_i,j}}{p^{e_i}} + \mathbb{Z}$$

with $\gcd(a_{e_i,j}, p) = 1$.
If $p = 2$ then

1. δ_i, μ_i are orthogonal to all the other selected vectors.
2. $(\delta_i, \delta_i) = a/2^e + \mathbb{Z}, (\delta_i, \mu_i) = b/2^e + \mathbb{Z}, (\mu_i, \mu_i) = c/2^e + \mathbb{Z}$ where $b = 1$ and either $a = c = 0$ or $a = c = 2$.
3. α_i is orthogonal to each other selected vector and $(\alpha_i, \alpha_i) = t_i/2^e$ with $2 \nmid t_i$.

We claim that we can conclude that the δ form a finite basis solely from this information:

Let p be odd. We claim that

$$\Psi : \left(\mathbb{Z}_{p^1}\right)^{n_1} \times ... \times \left(\mathbb{Z}_{p^{e_r}}\right)^{n_r} \to D_p, \quad \Psi\left(\left(a_{e_i,j}\right)_{\substack{i=1,...,r \\ j=1,...,n_i}}\right) = \sum_{i,j} a_{e_i,j}\delta_{e_i,j}$$

is a well defined isomorphism of $\mathbb{Z}$-modules.

First of all we remark that Ψ is surjective. This is due to the fact that $\gcd(\det(S), p) = 1$, i.e. if we operate (in the same way as we did with S on $\delta_1, ..., \delta_n$) on the new basis vectors, we get back $\delta_1, ..., \delta_n$ and those generated D_p by assumption.

We show that Ψ is well defined: Let $\delta := \delta_{e_i,j}$ and $e := e_i$ then $p^e\delta = 0$ because, in fact, $p^e\delta \in D^\perp$: As $D_p \perp D_q$ for different primes $p \neq q$ it suffices to show that $p^e\delta \in (D_p)^\perp$. By the above, D_p is generated by the new basis $\delta_{e_i,j}$ but keep in mind that because of the simple structure of $H + \mathbb{Z}$, $\delta_{e_i,j}$ is orthogonal to $\delta_{e_{i'},j'}$ unless $i = i', j = j'$, so for a general element $\zeta = \sum \lambda_{e_i,j}\delta_{e_i,j} \in D_p$ with $\lambda_{e_i,j} \in \mathbb{Z}$, we have $(\delta, \zeta) = p^e\lambda_{e,j}(\delta_{e,j}\delta_{e,j}) = p^e\lambda_{e,j}a_{e_i,j}/p^e + \mathbb{Z} = 0 + \mathbb{Z}$ as $p^e p^{-e} = 1 \in \mathbb{Z}$.

We show the injectivity of Ψ: Assume there are $\lambda_{e_i,j} \in \mathbb{Z}$ such that

$$\zeta = \sum \lambda_{e_i,j}\delta_{e_i,j} = 0$$

Then we pair ζ with $\gamma_{e_x,y}$ for every x, y and obtain

$$0 + \mathbb{Z} = (0, \gamma_{e_i,j}) = (\zeta, \gamma_{e_i,j}) = \sum \lambda_{e_i,j}(\delta_{e_i,j}, \delta_{e_x,y}) = \lambda_{e_x,y}a_{e_x,y}/p^{e_x} + \mathbb{Z}$$

Hence, $\lambda_{e_x,y}a_{e_x,y}/p^{e_x} \in \mathbb{Z}$ or, phrased differently, $p^{e_x} | \lambda_{e_x,y}a_{e_x,y}$. As $\gcd(a_{e_x,y}, p) = 1$ for all x, y,

$$p^{e_x} | \lambda_{e_x,y}$$

Now if $\Psi((\lambda_{e_i,j})_{i,j}) = 0$ then $(\lambda_{e_i,j})_{i,j} = 0$ in the structure $\oplus_{i,j}(\mathbb{Z}_{p^{e_i}})^j$. Hence, Ψ is injective.

Now let $p = 2$. Here, we put

$$\Psi : \oplus_{e=e_1,...,e_A}(\mathbb{Z}_{2^e} \times \mathbb{Z}_{2^e})^r \oplus (\mathbb{Z}_{2^e})^s \to D_2$$

to be the map

$$\Psi\left[\left(\left(\left((x_j^{(e)}, y_j^{(e)})_{j=1,...,r}, (z_i)_{i=1,...,s}\right)\right)_{e=e_1,...,e_A}\right]$$
$$= \sum_e \left(\sum_j x_j^{(e)}\delta_j^{(e)} + y_j^{(e)}\mu_j^{(e)} + \sum_i z_i\alpha_i\right)$$

As in the case of p odd, the new basis vectors generate D_2 as a $\mathbb{Z}$-module, so the surjectivity is shown. We need to show the injectivity and that Ψ is well defined. We will omit the proof showing that Ψ is well defined because it is completely analogous to the case p odd. On the injectivity: Let

$$v = ((x_j^{(e)}, y_j^{(e)})_{j=1,\ldots,r}, (z_i)_{i=1,\ldots,s})_{e=e_1,\ldots,e_A}$$

and assume

$$\zeta = \Psi(v) = \sum_e \left(\sum_j x_j^{(e)} \delta_j^{(e)} + y_j^{(e)} \mu_j^{(e)} + \sum_i z_i \alpha_i \right) = 0$$

Again, we show that $\zeta \in D^\perp$. As in the case p odd, it suffices to show that ζ is orthgonal to whole D_2. For streamlining the proof we view both types of 2-by2-blocks $A = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ with $2|a, 2|c, 2 \nmid c, 2 \nmid \det(A)$.

$$2^{-e} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \; textor \; 2^{-e} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

just as blocks of the type

$$2^{-e} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \text{ with} 2|a, 2|c, 2 \nmid c, 2 \nmid ac - b^2$$

but for the later use we keep in mind that there are actually only these two types above. We pair ζ with every selected vector for the 2-adic part: Let e be fixed. Let $\delta_j = \delta_j^{(e)}, \mu_j = \mu_j^{(e)}, \alpha_i = \alpha_i^{(e)}$. Rename the results of the pairings to $a_j = a_j^{(e)}, b_j = b_j^{(e)}$ and so forth. We also rename the coefficients $x_j^{(e)}$ to x_j and so forth. Recall that inside D_2, different "e-parts" are orthogonal to each other and inside each e-part, almost all selected vectors are orthogonal to each other (except to itself or its potential partner in a 2-by-2-block). Hence,

$$\begin{aligned} 0 + \mathbb{Z} = (\zeta, \delta_j) &= \underbrace{(\sum_{e' \neq e} ..., \delta_j)}_{=0+\mathbb{Z}} + \sum_j x_j^{(e)} (\delta_j^{(e)}, \delta_j) + y_j^{(e)} (\mu_j^{(e)}.\delta_j) + \sum_i z_i (\alpha_i, \delta_j) \\ &= 2^{-e} (x_j a_j + y_j b_j) \end{aligned}$$

Hence, $x_j a_j + y_j b_j \equiv 0 \mod 2^e$. Pairing ζ with μ_j gives $x_j b_j + y_j c_j \equiv 0 \mod 2^e$. Written in matrix form, this means

$$\begin{pmatrix} a_j & b_j \\ b_j & c_j \end{pmatrix} \begin{pmatrix} x_j \\ y_j \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \mod 2^e$$

As $2 \nmid a_j c_j - b_j^2$ which is the determinant of the matrix, the matrix is invertible over $\mathbb{Z}_{2^e}$. Consequently, $x_j \equiv y_j \equiv 0 \mod 2^e$. This works for all fixed e and j. The diagonal part is handled precisely as in the case where p is odd.

We have obtained a decomposition of D into $D = \bigoplus_{p\in\mathbb{P}} D_p$ where

$$D_2 = \bigoplus_{e=e_1,\dots,e_A} \left(\bigoplus_{j=1,\dots,r} (\mathbb{Z}_{2^e} \oplus \mathbb{Z}_{2^e}) \bigoplus_{i=1,\dots,s} \mathbb{Z}_{2^e} \right)$$

and

$$D_p = \bigoplus_{i=1,\dots,n_1} \mathbb{Z}_{p^1} \oplus \dots \oplus \bigoplus_{i=1,\dots,n_r} \mathbb{Z}_{p^{e_r}}$$

The single parts are generated by elements with bilinear pairing as follows: $\mathbb{Z}_{2^e} \oplus \mathbb{Z}_{2^e}$ is generated by two elements γ, δ of order 2^e with the properties that

$$(\gamma,\gamma) = a/2^e, (\gamma,\delta) = b/2^e, (\delta,\delta) = c/2^e$$

with $b = 1$ and either $a = c = 0$ or $a = c = 2$. The diagonal parts $\mathbb{Z}_{2^e}$ are generated by an element α of order 2^e with $(\alpha,\alpha) = a/2^e$ with $\gcd(a, 2) = 1$. Analogously, the diagonal part in the odd-p-case $\mathbb{Z}_{p^e}$ are generated by a single element α of order p^e with the property that $(\alpha,\alpha) = a/p^e$ with $\gcd(a, p) = 1$. We have obtained a nice orthogonal splitting but so far we have not involved the quadratic form at all. Therefore, our knowledge is yet restructed to the values of the bilinear pairing. We want to change this now. We want to compute the values of the quadratic form Q instead of the values (γ,γ). By definition,

$$(\gamma,\gamma) = Q(\gamma+\gamma) - Q(\gamma) - Q(\gamma) = 4Q(\gamma) - 2Q(\gamma) = 2Q(\gamma)$$

What we can hope for is that we can revert this formula in a certain sense, i.e. we can hope to obtain

$$Q(\gamma) = \frac{(\gamma,\gamma)}{2}$$

This is in line with the initial claim: in the 2-by-2-blocks with Gram matrix $2^{-e}\left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ with $b = 1$ and $a = c = 0$ or $a = c = 2$ we claimed indeed that $Q(\gamma) = \frac{a/2}{2^e} + \mathbb{Z}$ and $Q(\delta) = \frac{c/2}{2^e} + \mathbb{Z}$. However, this formula is **not** satisfied automatically in any sense. For example, if we have some fixed $\gamma \in D$ with $(\gamma,\gamma) = a/b + \mathbb{Z}$ with a even, then it does not follow in general that $Q(\gamma) = \frac{a/2}{b} + \mathbb{Z}$ (cf. the existence of the $(v, w) \neq (0, 0)$ cases below). So we really have to work to make this formula hold. Of course, in the 2-adic part we cannot divide by 2 so there should be some problems coming up. In the odd-adic parts we do not expect problems.
Take concrete representatives $(\gamma,\gamma) = a/b+\mathbb{Z}$ and $Q(\gamma) = c/d+\mathbb{Z}$. By canceling all common divisors, we may assume that $\gcd(a, b) = \gcd(c, d) = 1$. By the equation above we get

$$\frac{a}{b} + \mathbb{Z} = (\gamma,\gamma) = 2Q(\gamma) = \frac{2c}{d} + \mathbb{Z}$$

Hence,

$$\frac{a}{b} - \frac{2c}{d} = \frac{ab - 2cb}{bd} \in \mathbb{Z}$$

or phrased differently, $bd|ad-2cb$. We prove that for every touple $a,b,c,d\in\mathbb{Z}$ with $\gcd(a,b)=\gcd(c,d)=1$ and $bd|ab-2cd$ we have

$$\text{either } d=b \text{ or } d=2b \tag{2}$$

First of all we have $b|bd|ab-2cb$ and $b|-2cb$, hence, $b|ad$. As $\gcd(a,b)=1$, $b|d$. Similarly, $d|db|ad-2cb$ and $d|ad$ hence, $d|2cb$ and as $\gcd(c,d)=1$ we must have $d|2b$. Hence,

$$b|d|2b$$

Now either we use the splitting into prime numbers or, alternatively, we can prove the assertion by induction on the 2-order of d:
First case: $\text{ord}_2(d)=0$: Then $\gcd(2,d)=1$ and hence, $d|2b$ implies $d|b$ so $b|d|b$ and hence, $b=d$.
Induction step: $\text{ord}_2(d)>0$: Then, $d=2d'$ for some $d'\in\mathbb{Z}$. Let first $\text{ord}_2(b)=0$ so $\gcd(2,b)=1$. Then $2d'=d|2b$ hence, $d'|b$. As $b|d=2d'$ and $\gcd(b,2)=1$, $b|d'$. Hence, $b=d'=d/2$ or $2b=d$. Now let $b=2b'$ for some $b'\in\mathbb{Z}$. Then

$$\frac{db}{4}=\frac{d}{2}\frac{b}{2}\Big|\frac{db}{2}\Big|\frac{ad-2bc}{2}=a\frac{d}{2}-2\frac{b}{2}c$$

employing the induction hypothesis we get either $d/2=b/2$ (iff. $d=b$) or $b/2=2d/2=d$ so $b=2d$. Equation (2) is proved.

Now assume $b=d$. Then b must be odd: if b was even, then $a/b\equiv 2c/b \mod \mathbb{Z}$ yields $2|b|a-2c$ and $2|-2c$ so $2|a$ hence, $\gcd(a,b)\neq 1$. Contradiction. On the other hand, if b is odd, then b cannot be equal to $2d$, so $b=d$ must hold in this case. Hence,

$$b=d \iff b \text{ is odd} \quad \text{and} \quad b=2d \iff b \text{ is even} \tag{3}$$

Let γ be a basis element of the odd p-part of D, then $b=p^e$ is odd, hence $b=d$ by equation (3). We know then that $a/p^e=2c/p^e+\mathbb{Z}$ and thus $c\equiv a2^{-1} \mod p^e$. Hence,

$$Q(\gamma)=(a2^{-1} \mod p^e)/p^e+\mathbb{Z}$$

so for the odd-adic parts, knowledge of the values of the bilinear form is the same as knowledge of the values of the quadratic form. Both imply each other. In the case that γ comes from the 2-adic part, then we cannot know the value of Q on γ absolutely: All we can say is that since $b=2d$ by equation (3),

$$Q(\gamma)=\frac{c}{2b}+\mathbb{Z}=\frac{c}{2^{e+1}}+\mathbb{Z}$$

In this sense, the quadratic form is "stronger" (contains more information) than the bilinear form. However we can say a little bit more: In the situation above, $c\equiv a \mod 2^e$ follows directly from $2(\gamma,\gamma)=Q(\gamma)$. As the values of $a/2^e+\mathbb{Z}$ only depends on the value $a \mod 2^e$, we select $a\in\{0,1,...,2^e-1\}$ and analogously $c\in\{0,1,...,2^{e+1}-1\}$. We write a and c 2-adically as

$$a=a_0+a_1 2+a_2 2^2+...+a_{e-1}2^{e-1}$$
$$c=c_0+c_1 2+c_2 2^2+...+c_{e-1}2^{e-1}+c_e 2^e$$

with $a_i, c_i \in \{0,1\}$. Now $a \equiv c \mod 2^e$ means that the first parts up to 2^{e-1} coincide. Hence what is really hidden yet from us is the value of the bit in front of the 2^e. I.e.

$$c = a + v2^e \text{ with } v \in \{0,1\} \tag{4}$$

So in the case of diagonal components C in odd p-parts we have that C is generated by a single element γ of order p^e with $(\gamma,\gamma) = a/p^e + \mathbb{Z}$ with $a \in \mathbb{Z}, \gcd(a,p) = 1$ and $Q(\gamma) = 2^{-1}a/p^e + \mathbb{Z}$ where the inversion takes place in $\mathbb{Z}_{p^e}$. In the case of diagonal entries in the 2-adic part, there are components C generated by a single element γ of order 2^e with $(\gamma,\gamma) = a/2^e + \mathbb{Z}$ with $a \in \mathbb{Z}, \gcd(a,2) = 1$ and $Q(\gamma) = (a + v2^e)/2^{e+1} + \mathbb{Z}$ with $v \in \{0,1\}$ and both cases can exist. Also note that for a 2-adically written $a = a_0 + a_1 2 + a_2 2^2 + ...$, we have $\gcd(a,2) = 1 \iff a_0 = 1$ so since a was a unit in $\mathbb{Z}_{2^e}$, so is $a + v2^e$. Since we did not claim anything apart from that we are done with these diagonal parts. Now what about the 2-by-2-blocks? These are components $C \cong \mathbb{Z}_{2^e} \times \mathbb{Z}_{2^e}$ generated by two elements γ, δ of order 2^e having a Gram matrix

$$(\gamma,\gamma) = a/2^e, (\gamma,\delta) = b/2^e, (\delta,\delta) = c/2^e$$

with $b = 1$ and either $a = c = 0$ or $a = c = 2$. If $a = c = 0$ we call this a block of type I and if $a = c = 2$ we call it of type II. Here the situation with the quadratic form is a little more involved. All we can say after the discussion above so far is that there are $v, w \in \{0,1\}$ with

$$Q(\gamma) = \tfrac{a+v2^e}{2^{e+1}} \text{ and } Q(\delta) = \tfrac{c+w2^e}{2^{e+1}}$$

A natural question is: can all four cases $(v,w) \in \{(0,0),(0,1),(1,0),(1,1)\}$ really occur? If not then we were done more quickly. Unfortunately this is the case as we will show now: Consider the abstract algebraic structure $D := \mathbb{Z}_{2^e} \times \mathbb{Z}_{2^e}$ as above generated by $\gamma \cong (1,0)$ and $\delta \cong (0,1)$. We endow this with a finite bilinear form $(\cdot,\cdot)$ having (more generally speaking) a Gram matrix of the form $2^{-e}\left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ with $a,b,c \in \mathbb{Z}$ arbitrary but satisfying $2|a, 2|c, 2 \nmid b, 2 \nmid ac - b^2$ then this is almost a discriminant form, the quadratic form is still missing. For $v, w \in \{0,1\}$ arbitrary we simply define

$$Q(\gamma) := \tfrac{a+v2^e}{2^{e+1}} \text{ and } Q(\delta) := \tfrac{c+w2^e}{2^{e+1}}$$

i.e. more generally we define for every element $x\gamma + y\delta, x, y \in \mathbb{Z}$

$$Q(x\gamma + y\delta) := x^2 Q(\gamma) + y^2 Q(\delta) + xy(\gamma,\delta)$$

In order to see that this is a well-defined quadratic form having $(\cdot,\cdot)$ as its associated bilinear form we have to verify that

$$Q(\zeta + \omega) = Q(\zeta) + Q(\omega) + (\zeta,\omega) \quad \forall \zeta, \omega \in D$$

Let $\zeta = A\gamma + B\delta, \omega = C\gamma + D\delta$ then

$$\begin{aligned}
Q((A\gamma + B\delta) + (C\gamma + D\delta)) &= Q((A+C)\gamma + (B+D)\delta) \\
&= (A+C)^2 Q(\gamma) + (B+D)^2 Q(\delta) + (A+C)(B+D)(\gamma,\delta) \\
&= \frac{(A+C)^2(a+v2^e)}{2^{e+1}} + \frac{(B+D)^2(c+w2^e)}{2^{e+1}} + \frac{2(A+C)(B+D)b}{2^{e+1}} \\
&= \cancel{\frac{A^2(a+v2^e)}{2^{e+1}}} + \frac{2AC(a+v2^e)}{2^{e+1}} + \cancel{\frac{C^2(a+v2^e)}{2^{e+1}}} \\
&\quad + \cancel{\frac{B^2(c+w2^e)}{2^{e+1}}} + \frac{2BD(c+w2^e)}{2^{e+1}} + \cancel{\frac{D^2(c+w2^e)}{2^{e+1}}} \\
&\quad + \frac{2(A+C)(B+D)b}{2^{e+1}} + \mathbb{Z}
\end{aligned}$$

If we carefully compare this to the expression

$$\begin{aligned}
&Q(A\gamma + B\delta) + Q(C\gamma + D\delta) + (A\gamma + B\delta, C\gamma + D\delta) \\
&\quad = \frac{A^2(a+v2^e)}{2^{e+1}} + \frac{B^2(c+w2^e)}{2^{e+1}} + \frac{2ABb}{2^{e+1}} + \frac{C^2(a+v2^e)}{2^{e+1}} + \frac{D^2(c+w2^e)}{2^{e+1}} + \frac{2CDb}{2^{e+1}} \\
&\qquad + AC(\gamma,\gamma) + (AD+BC)(\gamma,\delta) + BD(\delta,\delta) + \mathbb{Z} \\
&\quad = \cancel{\frac{A^2(a+v2^e)}{2^{e+1}}} + \cancel{\frac{B^2(c+w2^e)}{2^{e+1}}} + \frac{2ABb}{2^{e+1}} + \cancel{\frac{C^2(a+v2^e)}{2^{e+1}}} + \cancel{\frac{D^2(c+w2^e)}{2^{e+1}}} + \frac{2CDb}{2^{e+1}} \\
&\qquad + \frac{2ACa}{2^{e+1}} + \frac{2(AD+BC)b}{2^{e+1}} + \frac{2BDc}{2^{e+1}} + \mathbb{Z}
\end{aligned}$$

then we see that the difference is

$$\begin{aligned}
&\frac{2AC(\cancel{a}+v2^e)}{2^{e+1}} + \frac{2BD(\cancel{c}+w2^e)}{2^{e+1}} + \frac{2(AB+AD+BC+BD)b}{2^{e+1}} \\
&\quad - \frac{2ABb}{2^{e+1}} - \frac{2CDb}{2^{e+1}} - \cancel{\frac{2ACa}{2^{e+1}}} - \frac{2(AD+BC)b}{2^{e+1}} - \cancel{\frac{2BDc}{2^{e+1}}} + \mathbb{Z} \\
&= \underbrace{\frac{2^{e+1}ACv}{2^{e+1}} + \mathbb{Z}}_{=0+\mathbb{Z}} + \underbrace{\frac{2^{e+1}BDw}{2^{e+1}} + \mathbb{Z}}_{=0+\mathbb{Z}} + \frac{2(AB+AD+BC+BD)b}{2^{e+1}} - \frac{2ABb}{2^{e+1}} - \frac{2CDb}{2^{e+1}} - \frac{2(AD+BC)b}{2^{e+1}} \\
&= \frac{2(AB+AD+BC+CD)b}{2^{e+1}} - \frac{2ABb}{2^{e+1}} - \frac{2CDb}{2^{e+1}} - \frac{2(AD+BC)b}{2^{e+1}} + \mathbb{Z} \\
&= 0 + \mathbb{Z}
\end{aligned}$$

What have we seen now? If we just **define** the quadratic form on an abstract algebraic structure as we wish (i.e. with all of the four $v = 0, 1, w = 0, 1$ cases), we get in fact a discriminant form, so all four cases really might appear after we are done with the process as above. Side remark: We have also seen that the finite bilinear form does not fully describe the finite quadratic form, the four forms with $v, w = 0$ or 1 **all** have the same bilinear form as their associated form but they are different! Now the question is the following: We stated in the theorem that we can reduce it to the case $v = w = 0$, so how do we do that? We

show that inside the 2-by-2-blocks, we can choose new bases γ', δ' so that the Gram matrix and quadratic form w.r.t. this new basis becomes equal to a block of type (A) or (B) as announced in the theorem. Before we start the proof we make the following observartion: Let us assume that we have found γ', δ' such that they generate the 2-by-2-block and are $\mathbb{Z}_{2^e}$–linearly independent. Assume further that

$$Q(\gamma') = \frac{a}{2^{e+1}} + \mathbb{Z}, Q(\delta') = \frac{c}{2^{e+1}} + \mathbb{Z} \text{ and } (\gamma', \delta') = (\gamma, \delta) = \frac{1}{2^e} + \mathbb{Z}$$

Then we are done as then the map $\gamma \mapsto \gamma', \delta \mapsto \delta'$ is a map that transfers the quadratic form in total to the form we want. This comes from the fact that all the values

$$Q(A\gamma + B\delta) = A^2 Q(\gamma) + B^2 Q(\delta) + AB(\gamma, \delta)$$

only depend on $Q(\gamma), Q(\delta)$ and (γ, δ).
On Type I: Here D is a discriminant form of the algebraic structure $D = \mathbb{Z}_{2^e} \times \mathbb{Z}_{2^e}$ generated by two elements γ, δ having a Gram matrix of the form $2^{-e} \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) + \mathbb{Z}$ and satisfying $Q(\gamma) = \frac{0+v2^e}{2^{e+1}} + \mathbb{Z} = \frac{v}{2} + \mathbb{Z}$ and $Q(\delta) = \frac{0+w2^e}{2^{e+1}} + \mathbb{Z} = \frac{w}{2} + \mathbb{Z}$.
The Case $v = w = 0$: Here we have nothing to do. The form is as claimed in the theorem.
The cases $v = 1, w = 0$ and $v = 0, w = 1$: If $v = 0, w = 1$ then we first interchange the roles of γ and δ and then proceed as we will do below so we can assume $v = 1, w = 0$. Put $\gamma' := \gamma + 2^{e-1}\delta$ and $\delta' = \delta$. As the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 2^{e-1} & 1 \end{smallmatrix}\right)$ is contained in $\mathrm{GL}_2(\mathbb{Z}_{2^e})$, this really is a new basis for D. We compute

$$\begin{aligned} Q(\gamma') &= Q(\gamma) + 2^{2(e-1)} \underbrace{Q(\delta)}_{=0+\mathbb{Z}} + 2^{e-1}(\gamma, \delta) \\ &= \frac{v}{2} + 2^{e-1}\frac{b}{2^e} + \mathbb{Z} = \frac{1}{2} + \frac{1}{2} + \mathbb{Z} = 0 + \mathbb{Z} \end{aligned}$$

$$Q(\delta') = Q(\delta) = 0 + \mathbb{Z}$$

$$\begin{aligned} (\gamma', \delta') &= (\gamma, \delta) + 2^{e-1}(\delta, \delta) \\ &= (\gamma, \delta) + 0 + \mathbb{Z} = (\gamma, \delta) \end{aligned}$$

So, we are done in this case.
The Case $v = w = 1$: We need to make another case distinction:
The Case $v = w = 1$ and $e = 1$: Here $2^{-1}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) + \mathbb{Z} = 2^{-1}\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right) + \mathbb{Z}$ and $Q(\gamma) = Q(\delta) = \frac{1}{2} + \mathbb{Z}$ is precisely the condition to be of the desired Type (B) [with the correct values of the quadratic form]. So we have nothing to de here.
The Case $v = w = 1$ and $e > 1$: Here we put $\gamma' := \gamma + 2^{e-1}\delta$ and $\delta' := 2^{e-1}\gamma + \delta$. Here, the matrix $\left(\begin{smallmatrix} 1 & 2^{e-1} \\ 2^{e-1} & 1 \end{smallmatrix}\right)$ is contained in $\mathrm{GL}_2(\mathbb{Z}_{2^e})$ (here we already need

$e > 1$!) so this really is a new basis. We compute

$$\begin{aligned} Q(\gamma') &= Q(\gamma) + 2^{2(e-1)}Q(\delta) + 2^{e-1}(\gamma,\delta) \\ &= \frac{1}{2} + \underbrace{2^{2(e-1)}\frac{1}{2}}_{=0+\mathbb{Z}} + \frac{2^{e-1}}{2^e} + \mathbb{Z} \\ &= \frac{1}{2} + 0 + \frac{1}{2} + \mathbb{Z} = 0 + \mathbb{Z} \end{aligned}$$

$$\begin{aligned} Q(\delta') &= 2^{2(e-1)}Q(\gamma) + Q(\delta) + 2^{e-1}(\gamma,\delta) \\ &= \underbrace{2^{2(e-1)}\frac{1}{2}}_{=0+\mathbb{Z}} + \frac{1}{2} + \frac{2^{e-1}}{2^e} + \mathbb{Z} \\ &= 0 + \frac{1}{2} + \frac{1}{2} + \mathbb{Z} = 0 + \mathbb{Z} \end{aligned}$$

$$\begin{aligned} (\gamma',\delta') &= 2^{e-1}\underbrace{(\gamma,\gamma)}_{=0+\mathbb{Z}} + (\gamma,\delta) + 2^{2(e-1)}(\delta,\gamma) + 2^{e-1}\underbrace{(\delta,\delta)}_{=0+\mathbb{Z}} \\ &= (\gamma,\delta) + \frac{2^{2(e-1)}}{2^e} + \mathbb{Z} = (\gamma,\delta) + 0 + \mathbb{Z} \end{aligned}$$

Note that we have used $e > 1$ extensively, namely when concluding that $\frac{2^{2(e-1)}}{2^e} + \mathbb{Z} = 0 + \mathbb{Z}$.

On Type II: Here D is a discriminant form of the algebraic structure $D = \mathbb{Z}_{2^e} \times \mathbb{Z}_{2^e}$ generated by two elements γ, δ having a Gram matrix of the form $2^{-e}\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right) + \mathbb{Z}$ and satisfying $Q(\gamma) = \frac{2+v2^e}{2^{e+1}} + \mathbb{Z} = \frac{v}{2} + \mathbb{Z}$ and $Q(\delta) = \frac{2+w2^e}{2^{e+1}} + \mathbb{Z} = \frac{w}{2} + \mathbb{Z}$.

The Case $v = w = 0$: Here we have nothing to do. The form is as claimed in the theorem.

The cases $v = 1, w = 0$ and $v = 0, w = 1$: If $v = 0, w = 1$ then we first interchange the roles of γ and δ and then proceed as we will do below so we can assume $v = 1, w = 0$.

Assume first that $e = 1$. Here, $2^{-1}\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right) + \mathbb{Z} = 2^{-1}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) + \mathbb{Z}$ and $Q(\gamma) = \frac{2+2^1}{2^2} + \mathbb{Z} = 0 + \mathbb{Z}$ and $Q(\delta) = \frac{2+0}{2^2} + \mathbb{Z} = \frac{1}{2} + \mathbb{Z}$. This is precisely the $v = 0, w = 1$–case of Type I which we have already dealt with above.

We assume now that $e > 1$. Put $\gamma' := \gamma + 2^{e-1}\delta$ and $\delta' = \delta$. As the matrix

$\left(\begin{smallmatrix} 1 & 0 \\ 2^{e-1} & 1 \end{smallmatrix}\right)$ is contained in $\mathrm{GL}_2(\mathbb{Z}_{2^e})$, this really is a new basis for D. We compute

$$\begin{aligned} Q(\gamma') &= Q(\gamma) + 2^{2(e-1)}Q(\delta) + 2^{e-1}(\gamma,\delta) \\ &= \frac{2+2^e}{2^{e+1}} + \underbrace{2^{2(e-1)}\frac{2+0\cdot 2^e}{2^{e+1}}}_{=0+\mathbb{Z}} + 2^{e-1}\frac{1}{2^e} \\ &= \frac{1+2^{e-1}}{2^e} + \frac{1}{2} + \mathbb{Z} \\ &= \frac{1}{2^e} + \frac{1}{2} + \frac{1}{2} + \mathbb{Z} = \frac{1}{2^e} + \mathbb{Z} \\ Q(\delta') &= Q(\delta) = \frac{2+0\cdot 2^e}{2^{e+1}} + \mathbb{Z} = \frac{1}{2^e} + \mathbb{Z} \end{aligned}$$

$$\begin{aligned} (\gamma',\delta') &= (\gamma,\delta) + 2^{e-1}(\delta,\delta) \\ &= (\gamma,\delta) + 0 + \mathbb{Z} = (\gamma,\delta) \end{aligned}$$

Note that we have used $e > 1$ when we concluded that $2^{2(e-1)}$ is divisible by 2^e. We are done in this case.
The Case $v = w = 1$: We need to make another case distinction:
The Case $v = w = 1$ and $e = 1$: Here $2^{-1}\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right) + \mathbb{Z} = 2^{-1}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) + \mathbb{Z}$ and $Q(\gamma) = Q(\delta) = \frac{2+2}{4} + \mathbb{Z} = 0 + \mathbb{Z}$. This is precisely the condition to be of Type (A) as desired.
The Case $v = w = 1$ and $e > 1$: We have $Q(\gamma) = Q(\delta) = \frac{2+2^e}{2^{e+1}} + \mathbb{Z} = \frac{1}{2^e} + \frac{1}{2} + \mathbb{Z}$. Here we put $\gamma' := \gamma + 2^{e-1}\delta$ and $\delta' := 2^{e-1}\gamma + \delta$. The matrix $\left(\begin{smallmatrix} 1 & 2^{e-1} \\ 2^{e-1} & 1 \end{smallmatrix}\right)$ is contained in $\mathrm{GL}_2(\mathbb{Z}_{2^e})$ (here we already need $e > 1$!) so this really is a new

basis of D. We compute

$$\begin{aligned} Q(\gamma') &= Q(\gamma) + 2^{2(e-1)}Q(\delta) + 2^{e-1}(\gamma,\delta) \\ &= \frac{1}{2^e} + \frac{1}{2} + \underbrace{\frac{2^{2(e-1)}(2+2^e)}{2^e}}_{=0+\mathbb{Z}} + \frac{2^{e-1}}{2^e} + \mathbb{Z} \\ &= \frac{1}{2^e} + \frac{1}{2} + \frac{1}{2} + \mathbb{Z} = \frac{1}{2^e} + \mathbb{Z} \end{aligned}$$

$$\begin{aligned} Q(\delta') &= 2^{2(e-1)}Q(\gamma) + Q(\delta) + 2^{e-1}(\gamma,\delta) \\ &= \underbrace{\frac{2^{2(e-1)}(2+2^e)}{2^e}}_{=0+\mathbb{Z}} + \frac{1}{2^e} + \frac{1}{2} + \frac{2^{e-1}}{2^e} + \mathbb{Z} \\ &= \frac{1}{2^e} + \frac{1}{2} + \frac{1}{2} + \mathbb{Z} = \frac{1}{2^e} + \mathbb{Z} \end{aligned}$$

$$\begin{aligned} (\gamma',\delta') &= 2^{e-1}\underbrace{(\gamma,\gamma)}_{=0+\mathbb{Z}} + (\gamma,\delta) + 2^{2(e-1)}(\delta,\gamma) + 2^{e-1}\underbrace{(\delta,\delta)}_{=0+\mathbb{Z}} \\ &= (\gamma,\delta) + \frac{2^{2(e-1)}}{2^e} + \mathbb{Z} = (\gamma,\delta) + 0 + \mathbb{Z} \end{aligned}$$

Note that we have used $e > 1$ extensively, namely when concluding that $\frac{2^{2(e-1)}}{2^e} + \mathbb{Z} = 0 + \mathbb{Z}$. □

References

[1] J.C. Jantzen, J. Schwermer *Algebra.* Springer.

[2] J.H. Conway, N.J. Sloane *Sphere Packings, Lattices and Groups* Springer.

[3] `http://happy-werner.de/uni/sonstiges/miniConway_complete.pdf`