Classification on symmetric non-degenerate bilinear forms on finite Abelian groups, October 23, 2009

Michiel Kosters

Contents

We will follow the proof of Wall in section 5 of [**WA**].

1. General theory and the reduction to p-groups

Lemma 0.1.1. *Let G be a finite Abelian group. Then $G \cong \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$.*

Proof. Since $\mathrm{Hom}(G \oplus H, \mathbf{Q}/\mathbf{Q}) \cong \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z}) \oplus \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$, it is enough (by the structure theorem) to show the lemma for a cyclic group. Say that $G = \mathbf{Z}/n\mathbf{Z}$. Then the image of 1 must be in $\frac{1}{n}\mathbf{Z}/\mathbf{Z} \cong \mathbf{Z}/n\mathbf{Z}$ and such an element determines a morphism. $\square$

Definition 0.1.2. A symmetric blinear map $b : G \times G \to \mathbf{Q}/\mathbf{Z}$ is called non-degenerate if the map

$$\begin{aligned} \varphi : G &\to \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z}) \\ g &\mapsto (h \mapsto b(g, h)) \end{aligned}$$

is an isomorphism. This is equivalent to saying that $b(g, G) = 0 \implies g = 0$ since G is finite.

A pair (G, b) where G is a finite Abelian group and $b : G \times G \to \mathbf{Q}/\mathbf{Z}$ is a symmetric bilinear map is called a metric pair.

Remark 0.1.3. Suppose that (G, b) is a metric pair where $G = \prod_{i=1}^{n} \mathbf{Z}/n_i^{r_i}\mathbf{Z}$. Let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ where the 1 is on the i-th place. Then we can form a matrix $A := (a_{ij})_{i,j=1}^{n}$ where $a_{ij} = b(e_i, e_j) \in \mathbf{Q}/\mathbf{Z}$. This matrix is symmetric and $p^{\min(r_i, r_j)} a_{ij} = 0$. If $x, y \in G$ are notated as vectors, then $b(x, y) = xAy^t$. On the other hand, a matrix $A := (a_{ij})_{i,j=1}^{n}$ which is symmetric and satisfies $p^{\min(r_i, r_j)} a_{ij} = 0$ gives a metric pair (G, b) where $b(x, y) = xAy^t$ for vectors $x, y \in G$.

Definition 0.1.4. Let (G, b) and (H, b') be metric pairs. Then we say that (G, b) is (metrically) isomorphic to (H, b') if there is an isomorphism $\varphi : G \to H$ such that for $x, y \in G$ we have that $b(x, y) = b'(\varphi(x), \varphi(y))$.

Definition 0.1.5. Let (G, b) and (H, b') be metric pairs. We then define the orthogonal sum $(G, b) \oplus (H, b')$ to be the pair $(G \times H, b'')$ where $b''((a, b), (c, d)) = b(a, c) + b'(b, d)$ for $a, c \in G$ and $b, d \in H$.

If $(B, b'') \cong (G, b) \oplus (H, b')$, we say that the decomposition $(G, b) \oplus (H, b')$ splits (B, b'').

Notation 0.1.6. Let G be a group and let $H_1, H_2 \subset G$ be subgroups. If $G = G_1 + G_2$ and $G_1 \cap G_2 = \{0\}$, then we write $G = H_1 \times H_2$.

Notation 0.1.7. Suppose we have a metric pair (G, b). Let H be a subgroup of G. Then $(H, b|_H)$ is a metric pair as well and we will often denote it as H.

The notation for a decomposition can also be cumbersome. Suppose that we have a metric pair (G, b) and we have subgroups H_1, H_2 of G. These H_1 and H_2 become metric pairs by the above remark. If we have $G = H_1 \times H_2$, we can write any element of $g \in G$ uniquely as $g = h_1 + h_2$ where $h_1 \in H_1$ and $h_2 \in H_2$. We have the following map:

$$\varphi : (G, b) \to (H_1, b|_{H_1}) \oplus (H_2, b|_{H_2})$$

If this is a metric isomorphism, we write $G = H_1 \oplus H_2$ (without references to the metrics).

Definition 0.1.8. Let (G, b) be a metric space and $S \subset G$ be a subset of G. Then we say that $x \in G$ is perpendicular to S if $b(x, S) = 0$. The set of all elements in G which are orthogonal to S is denoted by $S^\perp$.

For $S, T \subset G$ we say that S is orthogonal to T if $S \subset T^\perp$ (this relation is symmetric).

Lemma 0.1.9. *Let (G, b) be a metric pair and suppose that $G = G_1 \times G_2$ where $G_1, G_2 \subset G$ are subgroups. Then $G = G_1 \oplus G_2$ iff $G_1 \subset G_2^\perp$ (that is, G_1 and G_2 are orthogonal).*

Proof. $\Longrightarrow$: Let $x \in G_1$, $y \in G_2$. Then:

$$\begin{aligned} b(x, y) &= b|_{H_1}(x, 0) + b|_{H_2}(0, y) \\ &= b(x, 0) + b(0, y) \\ &= 0 \end{aligned}$$

$\Longleftarrow$: Let $g, h \in G$ and write $g = g_1 + g_2$, $h = h_1 + h_2$ where $g_1, h_1 \in G_1$, $g_2, h_2 \in G_2$. Then we have:

$$\begin{aligned} b(g, h) &= b(g_1 + g_2, h_1 + h_2) \\ &= b(g_1, h_1) + b(g_2, h_2) + b(g_1, h_2) + b(g_2, h_1) \\ &= b(g_1, h_1) + b(g_2, h_2) \\ &= b|_{G_1}(g_1, h_1) + b|_{G_2}(g_2, h_2) \end{aligned}$$

This is precisely what we needed. $\square$

Lemma 0.1.10. *Let (G, b) be a metric pair and H a subgroup which is non-degenerate. Then $G = H \oplus H^\perp$ and if $G = H \oplus H'$, then $H' = H^\perp$. If (G, b) is non-degenerate, we have that $H^\perp$ is non-degenerate as well..*

Proof. Consider the following map:

$$\begin{aligned} \varphi : G &\to \mathrm{Hom}(H, \mathbf{Q}/\mathbf{Z}) \\ g &\mapsto (h \mapsto b(g, h)) \end{aligned}$$

By definition, its kernel is $H^\perp$. Let $\psi := \varphi|_H$, then ψ is an isomorphism by non-degeneracy. This shows that $H \cap H^\perp = \{0\}$. Now take $g \in G$. Then $g = \psi^{-1}\varphi(g) + (g - \psi^{-1}\varphi(g))$, and $\psi^{-1}\varphi(g) \in H$ and $g - \psi^{-1}(\varphi(g)) \in H^\perp$ which follows from:

$$\begin{aligned} \varphi(g - \psi^{-1}(\varphi(g))) &= \varphi(g) - \varphi(\psi^{-1}(\varphi(g))) \\ &= \varphi(g) - \varphi(g) \\ &= 0 \end{aligned}$$

Hence $G = H \oplus H^\dagger$.

For the next statement, it follows that $H' \subset H^\perp$ by Lemma 0.1.9, and we see that $\#H \cdot \#H' = \#G = \#H \cdot \#H^\perp$, hence $H' = H^\perp$.

Now suppose that (G, b) is non-degenerate. The natural map $G = H \oplus H^\perp \to \mathrm{Hom}(H, \mathbf{Q}/\mathbf{Z}) \oplus \mathrm{Hom}(H^\perp, \mathbf{Q}/\mathbf{Z})$ respects the decomposition and is an isomorphism, it follows that $H^\perp \to \mathrm{Hom}(H^\perp, \mathbf{Q}/\mathbf{Z})$ is an isomorphism, that is, $H^\perp$ is non-degenerate. $\square$

Lemma 0.1.11. *Let (G, b) and (H, b') be metric pairs. Then $(G, b) \oplus (H, b')$ is non-degenerate iff (G, b) and (H, b') are non-degenerate.*

Proof. By definition $(G,b) \oplus (H,b')$ is non-degenerate iff the induced map $G \times H \to \mathrm{Hom}(G, \mathbf{Q}/Z) \oplus \mathrm{Hom}(H, \mathbf{Q}/\mathbf{Z})$ is an isomorphism. Since by orthogonality it respects the decomposition, it is an isomorphism iff $G \to \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$ and $H \to \mathrm{Hom}(H, \mathbf{Q}/\mathbf{Z})$ are both isomorphisms. □

Problem 0.1.12. Classify the metric pairs (G,b) where b non-degenerate up to isomorphy.

We can also state it as follows: Let Wb be the monoid of non-degenerate metric pairs (G,b) where addition is defined as the orthogonal sum (use Lemma 0.1.11) up to isomorphy. Give generators and relations for Wb.

Lemma 0.1.13. *Let (G,b) be a metric pair. Suppose that $G = G_1 \times G_2$ for subgroups $G_1, G_2 \subset G$. If G_1 and G_2 have exponent m respectively n where $\gcd(m,n) = 1$, then $G = G_1 \oplus G_2$. If (G,b) is non-degenerate, then so are G_1 and G_2.*

Proof. Write $xm + yn = 1$. Then for $g_1 \in G_1$ and $g_2 \in G_2$ we have:

$$\begin{aligned} b(g_1, g_2) &= b((xm+yn)g_1, g_2) \\ &= b(xmg_1, g_2) + b(g_1, yng_2) \\ &= b(0, g_2) + b(g_1, 0) \\ &= 0 \end{aligned}$$

Hence G_1 and G_2 are orthogonal to each other, now apply Lemma 0.1.9. Apply Lemma 0.1.11 for the statement about non-degeneracy. □

Problem 0.1.14 (Restatement of Problem 0.1.12)**.** By the previous lemma (Lemma 0.1.13) it is enough to solve the problem just for p-groups. So we restate the problem as follows: Fix a prime p. Classify the metric pairs (G,b) where G is a p-group and b is non-degenerate, up to isomorphy.

The previous lemma also says that $Wb \cong \oplus_p Wb_p$ where Wb_p is the monoid on the pairs (G,b) where G is a p-group.

1.1. Getting to vector spaces.

In this section we assume that all groups are (finite) Abelian p-groups where p is fixed.

Definition 0.1.15. A finite Abelian p-group is called homogeneous if it is a direct sum of cyclic groups of the same order p^r.

Definition 0.1.16. For a group G we define:

$$\rho_k(G) := G[p^k]/(G[p^{k-1}] + pG[p^{k+1}])$$

Lemma 0.1.17. *We have the following statements where G and H are finite Abelian p-groups:*

i. *$\rho_k(G)$ is a (finite dimensional) vector space over $\mathbf{F}_p$;*
ii. *$\rho_k(G \times H) = \rho_k(G) \times \rho_k(H)$.*
iii.
$$\rho_k(\mathbf{Z}/p^m\mathbf{Z}) \cong \begin{cases} \mathbf{Z}/p\mathbf{Z} & m = k \\ 0 & \text{else} \end{cases}$$
iv. *If G is a direct sum of r_k cyclic groups each of order p^k, then $\rho_k(G)$ has dimension r_k;*

v. *A symmetric bilinear form b on G determines a bilinear symmetric form b' on $\rho_k(G)$ by the following formula for $x, y \in G[p^k]$:*
$$b'([x],[y]) = p^{k-1}b(x,y)$$

PROOF.

i. Let $x \in G[p^k]$. Then $p^{k-1}(px) = 0$, hence $px \in G[p^{k-1}]$ and it follows that $\rho_k(G)$ is a finite module over $\mathbf{F}_p$.
ii. Follows directly from the definition.
iii. Let $G = \mathbf{Z}/p^m\mathbf{Z}$. If $k > m$ we see that $G[p^k] = G[p^{k-1}]$ and hence $\rho_k(G) = 0$. If $k < m$ se see that $G[p^k] = pG[p^{k+1}]$ and $\rho_k(G) = 0$ as well. If $k = m$ we calculate:
$$\begin{aligned}\rho_k(G) &= G/(pG + pG)\\ &= G/pG\\ &\cong \mathbf{Z}/p\mathbf{Z}\end{aligned}$$
iv. Follows from ii and iii.
v. Symmetry follows from the symmetry of b and it is bilinear if well-defined. Let $x \in G[p^k]$, $z \in G[p^{k-1}]$ and $w \in G[p^{k+1}]$. It is enough (by symmetry) to show that $0 = p^{k-1}b(x,z)$ and $0 = p^{k-1}b(x,pw)$. But $p^{k-1}b(x,z) = b(x,p^{k-1}z) = g(x,0) = 0$. Also $p^{k-1}b(x,pw) = b(p^kx,w) = b(0,w) = 0$.

□

Notation 0.1.18. If (G,b) is a metric pair, then we have an induced metric b' on $\rho_k(G)$ of the previous lemma (Lemm 0.1.17). This makes $(\rho_k(G), b')$ into a metric pair, and we will use the notation with a $'$ throughout this chapter or even don't write the b' at all (we can do this if the b is fixed).

We now want to see what non-degeneracy means in terms of certain matrices. Let (G,b) be a metric pair where G is a p-group with exponent p^k. We know that $\mathrm{Im}(b) \subset \frac{1}{p^k}\mathbf{Z}/\mathbf{Z}$, multiplication by p^k gives us an image in $\mathbf{Z}/p^k\mathbf{Z}$. If g has order p^l, then $b(g,G) \subset p^{k-l}\mathbf{Z}/p^k\mathbf{Z}$. Let $G = \langle e_1\rangle \times \ldots \times \langle e_n\rangle$ where e_i has order p^{k_i}. Let $A = (b(e_i,e_j)p^k)_{i,j=1}^n \in \mathrm{Mat}_n(\mathbf{Z}/p^k\mathbf{Z})$. Now let $x = (x_1,\ldots,x_n) \in \prod_{i=1}^n p^{k-k_i}\mathbf{Z}/p^k\mathbf{Z}$, this represents the element $(\frac{x_1}{p^{k-k_1}}e_1,\ldots,\frac{x_n}{p^{k-k_n}}e_n)$ of G. Let $y = (y_1,\ldots,y_n) = Ax \in \prod_{i=1}^n p^{k-k_i}\mathbf{Z}/p^k\mathbf{Z}$, then y represents the map in $\mathrm{Hom}(G,\mathbf{Q}/\mathbf{Z})$ which maps e_i to $\frac{1}{p^k}y_i$. It now follows from the definition that (G,b) is non-degenerate if the corresponding map $A : \prod_{i=1}^n p^{k-k_i}\mathbf{Z}/p^k\mathbf{Z} \to \prod_{i=1}^n p^{k-k_i}\mathbf{Z}/p^k\mathbf{Z}$ is an isomorphism (which in this case is equivalent to being injective or surjective).

Lemma 0.1.19. *Let (G,b) be a metric pair where G is homogeneous of exponent p^r. Let $(e_1,\ldots,e_n)$ be a basis of G. Then b is non-degenerate iff $\det(p^rb(e_i,e_j))_{i,j=1}^n \not\equiv 0 \pmod p$ where we see $p^rb(e_i,e_j)$ as an element of $\mathbf{Z}/p^r\mathbf{Z}$ or of $\mathbf{Z}/p\mathbf{Z}$.*

PROOF. We use the above technique and we see that the map is non-degenerate iff the corresponding matrix $A \in \mathrm{Mat}_n(\mathbf{Z}/p^r\mathbf{Z})$ givens an isomorphism from $(\mathbf{Z}/p^r\mathbf{Z})^n$ to $(\mathbf{Z}/p^r\mathbf{Z})^n$, which just means that $A \in \mathrm{Gl}_n(\mathbf{Z}/p^r\mathbf{Z})$, hence it is equivalent that the determinant of A is invertible in $\mathbf{Z}/p^r\mathbf{Z}$, hence coprime with p. □

Corollary 0.1.20. *Let (G,b) be a non-degenerate metric pair where G is homogeneous of exponent p^r. Then $(p^mG, \frac{1}{p^m}b)$ is non-degenerate for $0 \le m < r$.*

Proof. We give a proof for $m = 1$, then continue by induction. Let $(e_1, \ldots, e_n)$ be a basis of G. Then $(pe_1, \ldots, pe_n)$ is a basis for pG. First notice the following:

$$\begin{aligned} \frac{1}{p}b(p^{r-1}(pe_i), pe_j) &= b(p^r e_i, e_j) \\ &= b(0, e_j) \\ &= 0 \end{aligned}$$

Of course $\frac{1}{p}b(pe_i, pe_j) = \frac{1}{p}b(pe_j, pe_j)$. Hence we at least have a bilinear symmetric form. Notice that pG has exponent $r - 1$ and we have

$$\det(p^{r-1}\frac{1}{p}b(pe_i, pe_j))_{i,j=1}^n = \det(p^r b(pe_i, pe_j))_{i,j=1}^n \neq 0 \pmod p$$

according to Lemma 0.1.19. Apply Lemma 0.1.19 again to see that the form is non-degenerate. □

Lemma 0.1.21. *Let (G, b) be a non-degenerate metric pair, then $(\rho_k(G), b')$ is non-degenerate.*

Proof. Write $G = \prod_{i=1}^n \mathbf{Z}/p^{k_i}\mathbf{Z}$ where $k_1, \ldots, k_r = k$ and $k_{r+1}, \ldots, k_n \neq k$. Let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (where the 1 is on the i-th place). We have a natural isomorphism $\varphi : G \to \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$. For $1 \leq i \leq n$ let $b_i = \varphi^{-1}(e_j \mapsto \delta_{ij}\frac{1}{p^{k_j}})$. It is obvious that the b_i for $1 \leq i \leq r$ generate a group isomorphic to $(\mathbf{Z}/p^k\mathbf{Z})^r$. By the proof of Lemma 0.1.17 we see that both $\{[e_i] : 1 \leq i \leq r\}$ and $\{[b_i] : 1 \leq i \leq r\}$ form a basis of $\rho_k(G)$. We calculate the determinant of $(pb'([e_i], [e_j])_{i,j=1}^n$. This determinant is up to a unit the same as the determinant $(pb'([e_i], [b_j]))_{i,j=1}^n$. We have:

$$\begin{aligned} pb'([e_i], [b_j]) &= p^k b(e_i, b_j) \\ &= \delta_{ij} \end{aligned}$$

This shows that the determinant of $(pb'([e_i], [b_j])_{i,j=1}^n$ is invertible, and as a consequence so is the determinant of $(pb'([e_i], [e_j]))_{i,j=1}^n$, now apply Lemma 0.1.19. □

Corollary 0.1.22. *Let (G, b) be a metric pair where G is a p-group. Then (G, b) is non-degenerate iff all $(\rho_r(G), b')$ are.*

Proof. $\Longrightarrow$: This is Lemma 0.1.21.

$\Longleftarrow$: First suppose that G is homogeneous of exponent p^k. We let $e_1, \ldots, e_n$ be a basis of G. Notice that:

$$pb'([e_i], [e_j]) = p^k(be_i, e_j)$$

Now apply Lemma 0.1.19.

Now we do the general case. We give a proof by induction on the exponent of G. Let G have exponent p^r and write $G = G_1 \times G_2$ where G_1 is homogeneous of exponent p^r and G_2 has exponent smaller than p^r. Since $\rho_r(G_1) = \rho_r(G)$, and by the previous part of the proof, it follows that G_1 is non-degenerate. By Lemma 0.1.10 it follows that $G = G_1 \oplus G_1^\perp$. This $G_1^\perp$ has lower exponent, and $\rho_i(G) = \rho_i(G_1)$ for $i < r$ (Lemma 0.1.17) and they are all non-degenerate by assumption ($\rho_i(G_1)$ for $i \geq r$ is always 0, hence non-degenerate). We apply the induction hypothesis to conclude that $G_1^\perp$ is non-degenerate, now finish by Lemma 0.1.11. □

Lemma 0.1.23. *The following statements are true.*

i. *Let (H,b) be a non-degenerate metric pair where H is homogeneous and has exponent p^k. There is a bijection of splittings of H in non-degenerate parts of H and the splitting of $(\rho_k(H),b')$ in non-degenerate parts.*
ii. *Let (G,b) be non-degenerate of exponent p^r, then $G \cong \bigoplus_{i=1}^r H_i$ (orthogonal decomposition!) where H_i is homogeneous of exponent p^i and non-degenerate. We also have that $\rho_k(H_k) = \rho_k(G)$ and they are non-degenerate.*

Proof.

i. Suppose that $H = H_1 \oplus H_2$ where H_1 and H_2 are non-degenerate. By Lemma 0.1.17 we see that $\rho_k(H) = \rho_k(H_1) \times \rho_k(H_2)$. By Lemma 0.1.21 we see that $\rho_k(H)$ and $\rho_k(H_1)$ are still non-degenerate. Observe that $\rho_k(H_2) \subset \rho_k(H_1)^\perp$ and that $\#\rho_k(H_2) = \#\rho_k(H_1)^\perp$ (Lemma 0.1.10), so $\rho_k(H_2) = \rho_k(H_1)^\perp$, and apply Lemma 0.1.10.

   Now suppose that $\rho_k(H) = K_1 \oplus K_2$ where K_1 and K_2 are non-degenerate. Pick a basis $\{e_i : 1 \leq i \leq m\}$ such that the classes of these e_i give a basis of K_1. Let H_1 be the group generated by the e_i. First notice that $\rho_k(H_1) = K_1$. By Lemma 0.1.22 we see that H_1 is non-degenerate. Now apply Lemma 0.1.10.

   We will show that both operations are inverse. Since our groups are finite, it is enough to check that the composition in one direction is the identity. Start with a splitting of $\rho_k(H) = K_1 \oplus K_2$ into non-degenerate parts. We get a decomposition $G = H_1 \oplus H_2$, where $\rho_k(H_1) = K_1$. But the other operation just gets a decomposition back with one component equal to $\rho_k(H_1) = K_1$, by Lemma 0.1.10 we get the same decomposition back.
ii. Let G have exponent p^r. We know by Lemma 0.1.21 that $\rho_r(G)$ is non-degenerate. Write $G = H_r \times G'$ where H_r is homogeneous of exponent p^r and G' has a smaller exponent. Notice that $\rho_r(G) = \rho_r(H_r)$ (Lemma 0.1.17). By Lemma 0.1.22 we see that H_r is non-degenerate. Use Lemma 0.1.10 to see that $G \cong H_r \oplus H_r^\perp$ where $H_r^\perp$ is non-degenerate and of exponent smaller than p^r. We continue by induction and obtain a splitting with H_i homogeneous groups of exponent p^i. Since ρ_k is additive and $\rho_k(H_i) = 0$ if $i \neq k$, we see that $\rho_k(G) = \rho_k(H_k)$. The non-degeneracy statement follows from Lemma 0.1.21.

$\square$

2. Classification in the odd case

We assume that p is odd. Since $\rho_k(G)$ will have exponent p, we will first consider this case: this is just the classical case of finite dimensional vector spaces over $\mathbf{F}_p$.

Let (G,b) be a non-degenerate metric pair where G has exponent p (hence $G \neq 0$). First suppose that $b(x,x) = 0$ for all x. But then for all $x, y \in G$ $2b(x,y) = b(x+y,x+y) - b(x,x) - b(y,y) = 0$ and since we have assumed that p is odd, it follows that $b(x,y) = 0$, contradiction the non-degeneracy. So there is an x with $b(x,x) \neq 0$.

Notation 0.2.1. Instead of writing $\bigoplus_{i=1}^{n} A$ where A is a metric pair we will use the monoid notation to write it as nA.

Definition 0.2.2. Let (G, b) be a non-degenerate metric pair where G has exponent p ($\mathbf{F}_p$ vector space). Let $(e_1, \ldots, e_n)$ be a basis of G over $\mathbf{F}_p$. Let $A = (pb(e_i, e_j))_{i,j=1}^{n} \in \mathrm{Gl}_n(\mathbf{Z}/p\mathbf{Z})$. Define the determinant of (G, b) to be $\det(A) \in \mathbf{Z}/p\mathbf{Z}^*/(\mathbf{Z}/p\mathbf{Z}^*)^2$. This is well defined. Indeed, this determinant is a unit if b is non-degenerate (Lemma 0.1.19). Also if we transform another basis into the basis $(e_1, \ldots, e_n)$ using an invertible matrix B, we get the matrix BAB^t, which has the same determinant up to a a square of a unit. We will denote the determinant by $\det(G, b)$.

Lemma 0.2.3. *There are* 2 *isomorphy classes of bilinear symmetric non-degenerate forms on* $\mathbf{Z}/p\mathbf{Z}$ *if* p *is odd. Let* $\overline{a}$ *be a non-square in* $\mathbf{Z}/p\mathbf{Z}$ *(*$a \in \mathbf{Z}$*). Then these classes are* $A_p = (\mathbf{Z}/p\mathbf{Z}, b_1)$ *and* $B_p = (\mathbf{Z}/p\mathbf{Z}, b_2)$*, where for* $x, y \in \mathbf{Z}$*:*

$$b_1(\overline{x}, \overline{y}) = \frac{xy}{p}$$

and

$$b_2(\overline{x}, \overline{y}) = \frac{xya}{p}.$$

Proof. Let b be a bilinear symmetric non-degenerate form on $\mathbf{Z}/p\mathbf{Z}$. We know that 1 is a generator of $\mathbf{Z}/p\mathbf{Z}$ and the form is completely determined by $b(1, 1) = \frac{a}{p} \in \mathbf{Q}/\mathbf{Z}$ where $a \in \mathbf{Z}$ is determind modulo p. For non-degeneracy it is enough that $\gcd(a, p) = 1$. Denote the form obtained in such a way by $[a]$. Let $c \in \mathbf{Z} \setminus \{0\}$. An isomorphism $\varphi : \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ with $\varphi(1) = c$ gives an isomorphy between $[a]$ and $[c^2 a]$, since $b(c, c) = \frac{c^2 a}{p}$ and all isomorphisms are of this form. This shows that a class is determined by a unit up to squares of units, and since we have two such classes, the squares and non squares, we have the two isomorphy classes as in the statement. $\square$

Lemma 0.2.4. *Let* p *be an odd prime. In* $\mathbf{Z}/p\mathbf{Z}$ *the element* 1 *can be written as the sum of two non-squares.*

Proof. Consider the set $A := \{1 - a : a \in (\mathbf{Z}/p\mathbf{Z})^* \text{ not square }\}$. Then $\#A = \frac{p-1}{2}$ and it doesn't contain 1 and 0 and hence is not contained in the set of squares which has size $\frac{p-1}{2} + 1$. Hence $A \cap \{a \in a \in (\mathbf{Z}/p\mathbf{Z})^* \text{ not square }\} \neq \emptyset$, that is, we can write 1 as the sum of two non-squares. $\square$

Lemma 0.2.5. *Let* G *be a group of exponent* p *where* p *is odd of size* p^n*. Then there are two isomorphy classes of non-degenerate symmetric bilinear forms on* G*, namely* $A_{n,1} := nA_p$ *and* $B_{n,1} := (n-1)A_p \oplus B_p$*. The pair* (G, b) *is isomorphic to* $A_{n,1}$ *if* $\det(G, b)$ *is a square, and to* $B_{n,1}$ *otherwise.*

Proof. Let (G, b) be a metric pair of exponent p of size p^n. We first claim that if $n \geq 2$, there is an $x \in G$ with $b(x, x) = 1$. If not fix an element $y \in G$ with $b(y, y) = a$ where a is a non square (if it was a square, we could directly rescale). Then $\langle y \rangle$ is non-degenerate, and write $G = \langle y \rangle \oplus \langle y \rangle^{\perp}$ where $\langle y \rangle^{\perp}$ is non-degenerate (Lemma 0.1.10). Hence we know that there is an element $z \in \langle y \rangle^{\perp}$ with $b(z, z) = b$ where b is a non square. Now notice that $b(n_1 y + n_2 z, n_1 y + n_2 z) = n_1^2 a + n_2^2 b$. Since $n_1^2 a$ and $n_2^2 b$ run over all quadratic non-residues if we let n_1 and n_2 run, we see by the previous lemma (Lemma 0.2.4) that there is an $x = n_1 y + n_2 z$ with $b(x, x) = 1$, a contradiction.

Notice that the case $n = 1$ is done in Lemma 0.2.3. If $n \geq 2$ we can keep splitting of parts isomorphic to A_p, and in the last step we are left with an A_p or B_p.

We just have to thow that $A_{n,1}$ and $B_{n,1}$ are not isomorphic. This follows since the first one has a square as a determinant, the second one a non-square. $\square$

Remark 0.2.6. We have diagonalised the non-degenerate bilinear form. This is also essentially Proposition 5 on page 34 of [**SE**].

We will now do the homogeneous case and this is done using Lemma 0.1.23 i.

Lemma 0.2.7. *Let G be a homogeneous group of exponent p^r of size p^{rn}. Then there are 2 isomorphy classes of non-degenerate metric pairs (G, b). Let A_{p^r} and B_{p^r} be the unique classes on $\mathbf{Z}/p^r\mathbf{Z}$ satisfying $\rho_r(A_{p^r}) \cong A_p$ and $\rho_r(B_{p^r}) \cong B_p$. More precisely, if $\overline{a}$ is a non-square in $\mathbf{Z}/p^r\mathbf{Z}$, then $(\mathbf{Z}/p^r\mathbf{Z}, b_1)$ and $(\mathbf{Z}/p^r\mathbf{Z}, b_2)$ are representativs of A_{p^r} respectively B_{p^r} where*

$$\begin{aligned} b_1(1,1) &= \frac{1}{p^r} \\ b_2(1,1) &= \frac{a}{p^r}. \end{aligned}$$

Then the two classes are $A_{n,r} := nA_{p^r}$ and $B_{n,r} := (n-1)A_{p^r} \oplus B_{p^r}$. If (G, b) is a non-degenerate metric pair, then it is isomorphic to $A_{n,r}$ if $\det(\rho_r(G))$ is a square, and to $B_{n,r}$ otherwise.

Proof. First consider the case where (G, b) has size p^r. Let $G = \mathbf{Z}/p^r\mathbf{Z}$. Then $\rho_r(G) \cong A_p$ or $\rho_r(G) \cong B_p$. Notice that $\frac{a}{p} = b'([1],[1]) = p^{r-1}b(1,1)$. Hence $b(1,1) = \frac{a+bp}{p^r}$ where $b \in \mathbf{Z}$ and $\gcd(a,p) = 1$ for some $a \in \mathbf{Z}$. As before $b(1,1) = \frac{c}{p^r}$ determines the form and c is determined up to squares of units in $\mathbf{Z}/p^r\mathbf{Z}$. Notice that $c \in (\mathbf{Z}/p^r\mathbf{Z}^*)^2$ iff $c \pmod p \in (\mathbf{Z}/p\mathbf{Z}^*)^2$ (use Hensel's lemma). This shows that there are two isomorphy classes, which are determined by $\rho_r(G) \cong A_p$ or $\rho_r(G) \cong B_p$, we call these classes A_{p^r} respectively B_{p^r}.

We will now do the general case where (G, b) has size p^{rn}. Use Lemma 0.2.5 to decompose $\rho_r(G)$ into nA_p or $(n-1)A_p \oplus B_p$. Lift this splitting using Lemma 0.1.23 i to a splitting $G \cong nA_{p^r}$ or $G \cong (n-1)A_{p^r} \oplus B_{p^r}$. Both types are not isomorphic, since they are not isomorphic after applying ρ_r. $\square$

Corollary 0.2.8. *The sole relation between A_{p^r} and B_{p^r} are multiples of $2A_{p^r} = 2B_{p^r}$.*

Proof. We first prove the relation. Notice that $\rho(2A_{p^r}) \cong \rho(2B_{p^r})$ (determinant is a square), hence $2A_{p^r} = 2B_{p^r}$ by lemma 0.2.7. Suppose we have a relation $aA_{p^r} + B_{p^r} = cA_{p^r} + dB_{p^r}$ where $a + b = c + d$. Reduce it to an equation of the form $a'A_{p^r} = a'A_{p^r}$ or $a''A_{p^r} + B_{p^r} = a''A_{p^r} + B_{p^r}$ or $a''A_{p^r} + B_{p^r} = a'''A_{p^r}$. Notice that the last equation does not hold (take ρ_r and then determinants), so we don't find any other equations. $\square$

Theorem 0.2.9. *Let (G,b) be a non-degenerate metric pair where G is a p-group and $d_i = \dim_{\mathbf{F}_p}(\rho_i(G))$. Then*

$$G \cong \bigoplus_{i:d_i\neq 0} C_i$$

where C_i is $A_{d_i,i}$ if $\det(\rho_i(G,b))$ is a square and $B_{d_i,i}$ if it is a non-square. All different choices lead to different isomorphy classes.

Proof. We use Lemma 0.1.23 ii to write $G = \bigoplus H_i$ where H_i is homogeneous of exponent p^i. By Lemma 0.2.7 we see that $H_i \cong A_{d_i,i}$ or $B_{d_i,i}$ which are determined by $\det(\rho_i(H_i)) = \det(\rho_i(G))$ (if it is a square, then it is $A_{d_i,i}$, and $B_{d_i,i}$ otherwise; use Lemma 0.1.23 ii and Lemma 0.2.7).

Suppose that $\bigoplus_{i:d_i\neq 0} C_i \cong \bigoplus_{i:d_i\neq 0} C_i'$ where C_i and C_i' are either $A_{d_i,i}$ or $B_{d_i,i}$ (for the groups to be isomorphic, the d_i need to be the same already). Apply ρ_i to see that $\rho_i(C_i) \cong \rho_i(C_i')$, hence by Lemma 0.2.7 $C_i = C_i'$. $\square$

Corollary 0.2.10. *We have that Wb is a monoid generated by A_{p^r} and B_{p^r} with relations $2A_{p^r} = 2B_{p^r}$ for $r \in \mathbf{Z}_{\geq 1}$.*

Proof. Use Lemma 0.2.8 and the proof of Lemma 0.2.9. $\square$

Algorithm 0.2.11. Theorem 0.2.9 is algorithmic so to speak. It shows that the class of a non-degenerate form is completely determined by the pairs $(d_i, \left(\frac{\det(\rho_i(G,b))}{p}\right))$ for all i up to the exponent of the group. Using this fact, remark 0.1.3 and Corollary 0.1.22 we can make this into a nice algorithm.

Description: Determines the isomorphy class of a bilinear form on a finite Abelian p-group where $p \neq 2$.

Input: A group $G = \prod_{i=1}^n \mathbf{Z}/p^{r_i}$ where $p \neq 2$, $r_i \leq r_j$ if $i \leq j$. And a matrix $b = (b_{ij})_{i,j=1}^n \in \mathrm{Mat}_n(\mathbf{Q}/\mathbf{Z})$. Let $e_i = (0,\ldots,0,1,0,\ldots,0)$ where the 1 is on the i-th place. Then b represents the map $b : \{e_i : 1 \leq i \leq n\} \times \{e_i : 1 \leq i \leq n\} \to \mathbf{Q}/\mathbf{Z}$ where $b(e_i,e_j) = b_{ij}$.

Output: The fact that b can be extended to a bilinear map or not. If so it tells if the obtained map is symmetric and non-degenerate. If this all holds, it will give the isomorphy class of (G,b).

Procedure:

i. Check that $p^{r_{\max i,j}} b_{ij} = 0 \in \mathbf{Q}/\mathbf{Z}$. If not, output: NOT EXTENDABLE, and terminate, otherwise output EXTENDABLE.
ii. Check that $b_{ij} = b_{ji}$ for all $1 \leq i < j \leq n$. If it fails somewhere, output: NOT SYMMETRIC, otherwise output SYMMETRIC.
iii. For $s = 1,\ldots,r_n$ do the following:
   (a) If there is no r_i with $r_i = s$, set $d_s := 0$ and $E_s := 0$ and continue with the next s. Otherwise define a_s and b_s such that $s = r_i$ iff $a_s \leq i \leq b_s$. Now define $d_s := a_s - b_s + 1$. Continue with the next step.
   (b) Calculate the matrix $A_s := (p^s b(e_i,e_j))_{i,j=a_s}^{b_s} \in \mathrm{Mat}_{d_s}(\mathbf{Z}/p\mathbf{Z})$. Let $D_s := \det(A_s) \in \mathbf{Z}/p\mathbf{Z}$. Calculate $E_s := \left(\frac{D_s}{p}\right)$ (Legendre symbol; use quadratic reciprocity for this). If $E_s = 0$ then output DEGENERATE and terminate. Otherwise remember (d_S, E_s) and forget the rest of the data.

iv. Output NON-DEGENERATE and the numbers (i, d_i, E_i) for $1 \leq i \leq r_s$ and terminate.

3. Classification in the case $p = 2$

In this section we will assume that (G, b) is a non-degenerate metric pair where G is a 2-group. There are a few differences with the case where p is odd. First of all, it can happen that $b(x, x) = 0$ for all x. And secondly, $\mathbf{Z}/p\mathbf{Z}^*/(\mathbf{Z}/p\mathbf{Z}^*)^2$ has size 1, 2 or even 4 instead of 2. We will try to overcome these problems.

Definition 0.3.1. On $\mathbf{F}_2^2$ we have the non-degenerate form represented by $\frac{1}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Such a pair is called a hyperbolic plane, and is denoted by H_2. Notice that in a hyperbolic plane with form b any element x satisfies $b(x, x) = 0$ (since $x \mapsto b(x, x)$ is a group homomorphism).

On $\mathbf{F}_2$ we have the non-degenerate form b where $b(1, 1) = \frac{1}{2}$, we will call it H_1.

Lemma 0.3.2. *Let (G, b) be a non-degenerate pair where G has exponent 2 of size 2^n. Then $G \cong rH_2 \oplus (n - 2r)H_1$ for some r with $0 \leq r \leq \frac{n}{2}$.*

Proof. Suppose that there is an element x with $b(x, x) = \frac{1}{2}$ (this is equivalent to saying that $b(x, x) \neq 0$). Then $\langle x \rangle$ is non-degenerate and by Lemma 0.1.10 we see that $G = \langle x \rangle \oplus \langle x \rangle^\perp$ where $\langle x \rangle^\perp$ is non-degenerate and we split of a factor H_1. We continue this process until all elements satisfy $b(x, x) = 0$. Suppose now that $b(x, x) = 0$ for all $x \in H$ where H is some obtained vector space. Since the form is non-degenerate, there are $x, y \in H$ with $b(x, y) = \frac{1}{2}$. This splits of a H_2 and we continue with the orthogonal complement. This gives us the desired decomposition. $\square$

Unfortunately this r is not uniquely determined, but fortunately, we don't have that many relations.

Lemma 0.3.3. *The relations between H_1 and H_2 are generated by $H_1 + H_2 = 3H_1$.*

Proof. Observe the following:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

We have applied a basis transformation and we see that the matrix for $H_1 + H_2$ transforms into the matrix for $3H_1$, hence $3H_1 \cong H_1 + H_2$.

Now suppose that we have a relation $a_1H_1 + a_2H_2 = a_3H_1 + a_4H_2$ where $a_1 + 2a_2 = a_3 + 2a_4 > 0$. Suppose that $a_1 \neq a_3$ (otherwise we have the trivial relation), we may suppose that $a_1 > 0$. Using the relation $3H_1 = H_1 + H_2$ to reduce the equation to $(a_3 + 2a_4)H_1 = a_3H_1 + a_4H_2$. If $a_3 > 0$, we can do the same trick, and obtain the trivial relation. So $a_3 = 0$ and the relation is a not a multiple of $H_1 + H_2 = 3H_1$. We obtain the relation $(2a_4)H_1 = a_4H_2$. But a_4H_2 is a space where every element has a zero inner product with itself, and in $(2a_4)H_1$ this is not true, so we we get a contradiction and we had all relations already. $\square$

Definition 0.3.4. Let $m \in \mathbf{Z}_{\geq 0}$. We define $H_{1,m} := mH_1$ and $H_{2,m} = mH_2$.

Corollary 0.3.5. *Let (G,b) be a non-degenerate pair where G has exponent 2 of size 2^n. If n is odd, $G \cong H_{1,n}$. If n is even, then $(G,b) \cong H_{1,n}$ or $(G,b) \cong H_{2,\frac{n}{2}}$. Let $(e_1,\ldots,e_n)$ be a basis for G. Then it is isomorphic to $H_{2,\frac{n}{2}}$ if $b(e_i,e_i)=0$ for $1 \leq i \leq n$, and to $H_{1,n}$ otherwise.*

Proof. Use Lemma 0.3.2 and Lemma 0.3.3 to get (G,b) into the desired form. Apparently, there is 1 possibility if n is odd. If n is even and (G,b) is isomorphic to $H_{2,\frac{n}{2}}$, then for $x \in G$ we have that $b(x,x)=0$. If it is isomorphic to $H_{1,n}$, this is not the case. Since we have a group homomorphism $x \mapsto b(x,x)$, we only need to check it on a basis. □

Lemma 0.3.6. *Let $G = \mathbf{Z}/2^n\mathbf{Z}$ where $n \geq 1$. Define $C_n = (G,b_1)$ $(n \geq 1)$, $D_n = (G,b_2)$ $(n \geq 2)$, $E_n = (G,b_3)$ $(n \geq 3)$ and $F_n = (G,b_4)$ $(n \geq 3)$ where:*

$$\begin{aligned} b_1(1,1) &= \frac{1}{2^n} \\ b_2(1,1) &= \frac{-1}{2^n} \\ b_3(1,1) &= \frac{5}{2^n} \\ b_4(1,1) &= \frac{-5}{2^n} \end{aligned}$$

Let (G,b) be a non-degenerate metric pair. Then (G,b) is isomorphic to exactly one of the allowed C_n, D_n, E_n, F_n.

Proof. Let (G,b) be a non-degenerate metric pair. It is completely determined by $b(1,1) = \frac{a}{p^n}$ where $a \in \mathbf{Z}$. Non-degeneracy is equivalent to saying that $\gcd(a,p)=1$. As in Lemma 0.2.3 we see that the class of (G,b) is determined by a modulo squares of units. Hence we need to finde representatives for $\mathbf{Z}/2^n\mathbf{Z}/(\mathbf{Z}/2^n\mathbf{Z}^*)^2$. For this look at Lemma 9.15 in [**?**]. It says that $\mathbf{Z}/2^n\mathbf{Z}^*$ is cyclic if $k \leq 2$ and $\mathbf{Z}/2^n\mathbf{Z}^* \cong \langle 5 \rangle \times \langle -1 \rangle$ if $n \geq 3$ and this gives us the required representatives and finishes the proof. □

The C_n, D_n, E_n, F_n will be the lifts of H_1. We still need to find lifts for H_2.

Lemma 0.3.7. *Let (G,b) be a non-degenerate metric pair where $G = (\mathbf{Z}/2^n\mathbf{Z})^2$ with $\rho_n(G) \cong H_2$ and $n \geq 2$. Then $(G,b) \cong I_n$ or J_n where I_n has matrix A_n and J_n matrix B_n as follows:*

$$\begin{aligned} A_n &:= \frac{1}{2^n}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ B_n &:= \frac{1}{2^n}\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \end{aligned}$$

Furthermore, $I_n \not\cong J_n$.

Proof. First of all notice that I_n and J_n indeed give non-degenerate forms (look at the determinant of $2^n A_n$ and $2^n B_n$ modulo 2, Lemma 0.1.19).

We will first show that (G,b) is isomorphic to I_n or J_n. We know from Lemma 0.1.20 that $(2G, \frac{1}{2}b)$ is non-degenerate. By induction we may assume that $(2G, \frac{1}{2}) \cong I_{n-1}$ or J_{n-1} (notice that they coincide if $n=2$).

First suppose that $(2G, \frac{1}{2}b) \cong I_{n-1}$. Hence there is basis x,y such that $2b(y,y) = 2b(x,x) = \frac{1}{2}b(2y,2y) = \frac{1}{2}b(2x,2x) = 0$ and $2b(x,y) = \frac{1}{2}b(2x,2y) = \frac{1}{2^{n-1}}$. This shows that $b(x,x), b(y,y) \in \{0, \frac{1}{2}\}$ and $b(x,y) \in \{\frac{1}{2^n}, \frac{1}{2^n} + \frac{1}{2}\}$. First suppose that $b(x,x) \neq b(y,y)$. Suppose that $b(x,x) = 0$ and $b(y,y) = \frac{1}{2}$. Now do a base change $x' = x$ and $y' = y + 2^{n-2}x$. Then $b(y',y') = b(y,y) + 2^{n-1}b(x,y) = 0$. Notice that $b(x',y') = b(x,y)$. If $b(x,y) = \frac{1}{2^n}$, then just keep the pair x', y'. Otherwise pick a such that $a \cong (1 + 2^{n-1})^{-1} \pmod{2^n}$. Then take $x'' := ax'$ and $y'' := y'$. Now notice that $b(x'', x'') = b(y'', y'') = 0$ and finally

$$\begin{aligned} b(x'', y'') &= ab(x,y) \\ &= \frac{a(1+2^{n-1})}{2^n} \\ &= \frac{1}{2^n} \end{aligned}$$

This is just the matrix for I_n. If $b(x,x) = b(y,y) = \frac{1}{2}$ The other case was that $b(x,x) = b(y,y) = \frac{1}{2}$ and $b(x,y) \in \{\frac{1}{2^n}, \frac{1}{2^n} + \frac{1}{2}\}$. We claim that both cases are isomorphic. Let $a = 2^{n-1} + 1 \in \mathbf{Z}/2^n\mathbf{Z}$. Then $a^2 = 1$. Now consider the following matrix relation with coefficients in $\mathbf{Z}/2^n\mathbf{Z}$:

$$\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 2^{n-1} & 1 \\ 1 & 2^{n-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 2^{n-1} & a \\ a & a^2 2^{n-1} \end{pmatrix} = \begin{pmatrix} 2^{n-1} & 1+2^{n-1} \\ 1+2^{n-1} & 2^{n-1} \end{pmatrix}$$

This shows that both cases are actually the same. Define $A_n, B_n \in \mathrm{Mat}_2(\mathbf{Z}/2^n\mathbf{Z})$

$$\begin{aligned} U_n &= \frac{1}{2^n} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ V_n &= \frac{1}{2^n} \begin{pmatrix} 2^{n-1} & 1 \\ 1 & 2^{n-1} \end{pmatrix} \end{aligned}$$

We will look for $C \in \mathrm{Gl}_2(\mathbf{Z}/2^n\mathbf{Z})$ such that $CU_nC^t = V_n$. It turns out (by an exhaustive search) that for $n = 2$ we obtain two different forms, which give rise to I_2 and J_2 (here it splits). For $n \geq 3$ such matrices exist. For $n = 3$ one can take

$$C = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$$

we leave the verification to the reader). For $n \geq 4$ one can take

$$C = \begin{pmatrix} 1 & 2^{n-2} \\ 2^{n-2} & 1 \end{pmatrix}.$$

Indeed, since $2(n-2) \geq 2$ if $n \geq 4$ we have:

$$\begin{pmatrix} 1 & 2^{n-2} \\ 2^{n-2} & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2^{n-2} \\ 2^{n-2} & 1 \end{pmatrix} = \begin{pmatrix} 2^{n-1} & 1+2^{2(n-2)} \\ 1+2^{2(n-2)} & 2^{n-1} \end{pmatrix} = \begin{pmatrix} 2^{n-1} & 1 \\ 1 & 2^{n-1} \end{pmatrix}$$

Now suppose that $(2G, \frac{1}{2}b) \cong J_{j-1}$, where $n \geq 3$ ($n = 2$ is already done). After lifting we have 6 (essentially different) possibilities, where we drop the $\frac{1}{2^n}$ factor:

$$\begin{aligned}
U_1 &= \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \\
U_2 &= \begin{pmatrix} 2 & 1+2^{n-1} \\ 1+2^{n-1} & 2+2^{n-1} \end{pmatrix} \\
U_3 &= \begin{pmatrix} 2 & 1 \\ 1 & 2+2^{n-1} \end{pmatrix} \\
U_4 &= \begin{pmatrix} 2+2^{n-1} & 1 \\ 1 & 2+2^{n-1} \end{pmatrix} \\
U_5 &= \begin{pmatrix} 2+2^{n-1} & 1+2^{n-1} \\ 1+2^{n-1} & 2+2^{n-1} \end{pmatrix} \\
U_6 &= \begin{pmatrix} 2 & 1+2^{n-1} \\ 1+2^{n-1} & 2 \end{pmatrix}
\end{aligned}$$

We will give matrices $V_i \in \mathrm{Gl}_n(\mathbf{Z}/2^n\mathbf{Z})$ which will show that all forms are equivalent. We define:

$$\begin{aligned}
V_2 :&= \begin{pmatrix} 0 & 1 \\ 1 & 2^{n-2} \end{pmatrix} \\
V_6 :&= \begin{pmatrix} 1 & 0 \\ 0 & 2^{n-1}+1 \end{pmatrix}
\end{aligned}$$

A quick calculation shows that $V_2U_1V_2^t = U_2$ and $V_6U_1V_6^t = U_6$. Furthermore we define:

$$\begin{aligned}
V_3 &= \begin{pmatrix} 0 & 1 \\ 1 & 2^{n-2} \end{pmatrix} \\
V_4 = V_5 &= \begin{pmatrix} 2^{n-1}+1 & 0 \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

Then $V_3U_6V_3^t = U_3$, $V_4U_4V_4^t = U_2$ and $V_5U_5V_5^t = U_3$. The calculations rely on the fact that $n \geq 3$. Hence we obtain:

$$\begin{aligned}
U_1 &= V_2^{-1}U_2V_2^{-t} \\
&= (V_6^{-1}V_3^{-1})U_3(V_6^{-1}V_3^{-1})^t \\
&= (V_2^{-1}V_4)U_4(V_2^{-1}V_4)^t \\
&= (V_6^{-1}V_3^{-1}V_5)U_5(V_6^{-1}V_3^{-1}V_5)^t \\
&= V_6^{-1}U_6V_6^{-t}
\end{aligned}$$

So in this case all forms are equivalent and we just have one lift, call it J_n.

We have shown that $I_2 \not\cong J_2$. Hence if $I_n \cong J_n$ for $n \geq 3$, we do the inverse of the lifting and obtain $I_2 \cong J_2$, a contradiction. $\square$

Theorem 0.3.8. *The monoid Wb_2 is generated by C_n, I_n ($n \geq 1$), D_n, J_n ($n \geq 2$), E_n, F_n ($n \geq 3$).*

Proof. This follows from Lemma 0.3.2, Lemma 0.1.23, Lemma 0.3.6 and Lemma 0.3.7. $\square$

We did not determine the relations between these generators, but according to Wall in [**WA**] it will be very complicated.

Bibliography

[SE] J-P Serre, A Course in Arithmetic, Verlag New York Inc., 1973

[WA] C.T.C. Wall, Quadratic Forms on Finite Groups, and related Topics, Topology Vol. 2. pp. 281-298. Pergamon Press, 1964