TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 351, Number 5, Pages 2101–2139
S 0002-9947(99)02469-1
Article electronically published on January 26, 1999

SYMPLECTIC GROUP LATTICES

RUDOLF SCHARLAU AND PHAM HUU TIEP

ABSTRACT. Let p be an odd prime. It is known that the symplectic group $Sp_{2n}(p)$ has two (algebraically conjugate) irreducible representations of degree $(p^n+1)/2$ realized over $\mathbb{Q}(\sqrt{\epsilon p})$, where $\epsilon = (-1)^{(p-1)/2}$. We study the integral lattices related to these representations for the case $p^n \equiv 1 \bmod 4$. (The case $p^n \equiv 3 \bmod 4$ has been considered in a previous paper.) We show that the class of invariant lattices contains either unimodular or p-modular lattices. These lattices are explicitly constructed and classified. Gram matrices of the lattices are given, using a discrete analogue of Maslov index.

1. Introduction

Let p be an odd prime, and set $S_n = Sp_{2n}(p)$ for the symplectic group of degree $2n$ over $\mathbb{F}_p$. Euclidean integral lattices in the space of the Weil representation of S_n have been investigated by several authors (see for instance [BaV], [Dum], [Gow], [Gro], [Tiep 1], [Tiep 2]). The Weil representation $\mathcal{W}$ of S_n is a complex representation of degree p^n that can be obtained from the action of S_n on the extraspecial group p_+^{1+2n} (as the outer automorphism group). See, for example, [Isa], [Sei], or [Ward 1] for a more general approach. $\mathcal{W}$ is a sum of two irreducible representations of degrees $(p^n-1)/2$ and $(p^n+1)/2$. (These two characters seem to have been first investigated in [BRW].) One of these representations, which we shall denote by $\mathcal{W}_1$, is faithful and has even degree, and the kernel of the other representation, $\mathcal{W}_2$, is the center $Z = C_2$ of S_n. Following [Gow], we shall refer to $\mathcal{W}_1$ and $\mathcal{W}_2$ as *Weil representations*. Weil representations have been characterized in several ways in [TZa 1], [TZa 2].

Set $\epsilon = (-1)^{(p-1)/2}$ and suppose that $(\dim \mathcal{W}_i, \epsilon) \neq (\frac{p^n-1}{2}, 1)$. It is shown in [Gro] that, under this assumption, the character ψ_i of the representation $\mathcal{W}_i$ generates the field $\mathbb{Q}(\sqrt{\epsilon p})$ over the rational field $\mathbb{Q}$, and has Schur index 1 over $\mathbb{Q}$. Hence, there exist an extension G_n of S_n and an absolutely irreducible $\mathbb{Q}G_n$-module V affording the S_n-character $\psi_i + \overline{\psi}_i$, where the bar denotes the algebraic conjugation of the field $\mathbb{Q}(\sqrt{\epsilon p})$. The group G_n can be chosen as a homomorphic

Received by the editors December 10, 1996.
1991 *Mathematics Subject Classification.* Primary 20C10, 20C15, 20C20, 11E12, 11H31, 94B05.
Key words and phrases. Integral lattice, unimodular lattice, p-modular lattice, finite symplectic group, Weil representation, Maslov index, linear code, self-dual code.
Part of this work was done during the second author's stay at the Department of Mathematics, Israel Institute of Technology. He is grateful to Professor D. Chillag and his colleagues at the Technion for stimulating conversations and their generous hospitality. His work was also supported in part by the DFG.

image of the *conformal symplectic group*

$$G_n = CSp_{2n}(p) = \{\varphi \in GL(W) | \quad \exists \kappa \in \mathbb{F}_p^\bullet, \forall u, v \in W, \langle \varphi(u), \varphi(v) \rangle = \kappa \langle u, v \rangle\},$$

where W denotes a natural $2n$-dimensional S_n-module over $\mathbb{F}_p$, with the symplectic form $\langle \cdot, \cdot \rangle$. In what follows we shall be concerned with the following two homomorphic images of G_n: the factor-group G_n^+ of G_n by its center C_{p-1} (consisting of the scalar matrices λE_{2n}, $\lambda \in \mathbb{F}_p^\bullet$), and G_n^-, the factor-group of G_n by the central group $C_{(p-1)/2}$ (consisting of scalar matrices λE_{2n}, $\lambda \in \mathbb{F}_p^{\bullet 2}$). Throughout the paper, C_m denotes the cyclic group of order m, and E_m denotes the identity matrix of order m (over any field).

The lattices for the Weil representations of degree $\psi(1) = (p^n - 1)/2$ have been investigated in [Gow] and [Gro]. Recall that in this case $p \equiv 3 \bmod 4$, according to our general assumption; see [Tiep 2] for the excluded case. If n is even, then every $\mathbb{Z}S_n$-lattice in V is even unimodular. If n is odd, V contains p-modular invariant lattices. Recall that an integral lattice Λ is said to be *p-modular* (or *modular of level* p) if the lattices ${}^p\Lambda^\#$ (the dual lattice $\Lambda^\#$ rescaled by the scalar p) and Λ are isometric. p-modular lattices have been introduced and investigated in [CoS 1] and [Que]. In either of these cases, the corresponding representations are *globally irreducible* in the sense of Gross [Gro]. Some of the corresponding lattices have been realized as sublattices of the Mordell-Weil lattices of certain elliptic curves (cf. [Dum] and [Gro]).

The Weil representations of degree $\psi(1) = (p^n + 1)/2$ are the subject of our present work, begun in [SchT] and continued in this paper. Here the corresponding representation cannot be globally irreducible anymore; namely, $\psi \bmod 2 = 1_S + \eta$ for some $\eta \in \mathrm{IBr}_2(S)$. In [SchT], the case $p^n \equiv 3 \bmod 4$ has been treated. The existence of unimodular $\mathbb{Z}G$-lattices in V has been established, where $G = G_n^- \simeq S_n \cdot C_2$. All $\mathbb{Z}G$-lattices contained in V have been classified.

In this paper, we are concerned with the case $p^n \equiv 1 \bmod 4$. Then $\mathcal{W}_2$ viewed over $\mathbb{Q}$ is in fact a faithful representation of $PSp_{2n}(p)$ of degree $p^n + 1$. Moreover, if $p \equiv 3 \bmod 4$, this representation can be extended (in a unique way) to a rational representation of G_n^+. If $p \equiv 1 \bmod 4$, it can be extended to a rational representation for *each* of the two groups G_n^+ and G_n^- (cf. Proposition 2.3). The reason is that when $p \equiv 1 \bmod 4$ the two groups $C_2 \times G_n^+$ and G_n^- are *isoclinic* to each other. For more detail on isoclinic groups see [Atlas] and [Tiep 2], Lemma 2.11. When $p \equiv 3 \bmod 4$, it follows from this lemma that the rational representation of S_n of degree $p^n + 1$ is extendible to a rational faithful representation of G_n^+ if n is even, and of G_n^- if n is odd, but not for its isoclinic variant.

From now on we keep the following notation: $S_n = Sp_{2n}(p)$, $G_n = CSp_{2n}(p)$, $Z \cong C_{p-1}$ the center of G_n^+, $G_n^+ = G_n/Z$, $G_n^- = G_n/Z^2$, θ a fixed generating element of $\mathbb{F}_p^\bullet$. Clearly, G_n is generated by S_n and an element ϑ_n with matrix $\mathrm{diag}(E_n, \theta E_n)$ in a fixed symplectic basis $(e_1, \dots, e_n, f_1, \dots, f_n)$ of the natural S_n-module $W = W_n = \mathbb{F}_p^{2n}$ (that is, a basis in which the symplectic form $\langle \cdot, \cdot \rangle$ is given as follows: $\langle e_i, e_j \rangle = 0$, $\langle f_i, f_j \rangle = 0$, $\langle e_i, f_j \rangle = \delta_{i,j}$). $V = V_n$ denotes an irreducible $\mathbb{Q}G_n$-module with character χ such that $\chi|_{S_n} = \psi + \overline{\psi}$. Furthermore, either $\mathrm{Ker}\,\chi = Z$ (and then V_n is a faithful G_n^+-module), or $p \equiv 1 \bmod 4$ and $\mathrm{Ker}\,\chi = Z^2$ (and then V_n is a faithful G_n^--module). Under these assumptions χ exists and is unique by Proposition 2.3. It is clear that there exists a unique (up to scalar) G_n-invariant positive definite symmetric bilinear form $(\cdot, \cdot)$ on V_n.

Our first main result is the following theorem which includes Theorem 1.1 of [SchT]:

Theorem 1.1. *Let p be an odd prime. If $p \equiv 3 \bmod 4$, then suppose in addition that n is odd. Then V_n contains G_n^--invariant odd unimodular Euclidean lattices (of rank p^n+1). If $n > 1$, these lattices have no roots.*

Actually, we provide an explicit construction of a G_n^--stable odd unimodular lattice $\Delta = \Delta(p,n)$ contained in V_n (cf. Theorem 3.9 and Corollary 5.4) for n odd, and a G_n^--stable odd unimodular lattice $\Delta^-(p,n)$ for the case where n is even and $p \equiv 1 \bmod 4$ (cf. Corollary 5.9). In the case $p \equiv 3 \bmod 4$ this is just the construction exposed in [SchT]. The cases $p^n = 27$ and $p^n = 25$ have been considered by R. Bacher and B. B. Venkov [BaV], and G. Nebe, respectively. The corresponding lattices have minimum 3. In general, Theorem 7.1 yields $\min \Delta(p,n) \geq (p+1)/2$ for all $n \geq 3$.

Our next results are concerned with p-modular lattices.

Theorem 1.2. *Let p be any odd prime. If $p \equiv 3 \bmod 4$, then suppose in addition that n is even. Then V_n contains G_n^+-invariant p-modular Euclidean lattices (of rank p^n+1).*

Again, we provide an explicit construction of a G_n^+-stable p-modular lattice $\Delta = \Delta^-(p,n)$ if n is odd and $p \equiv 1 \bmod 4$ (cf. Corollary 5.10), respectively $\Delta = \Delta(p,n)$ if n is even (cf. Theorem 4.4 and Corollary 5.6). This result generalizes Theorem (V.2) of [NPl] dealing with the case $n = 1$ and $p \equiv 1 \bmod 4$. The case $n = 2$ and $p = 5$ has been considered by Nebe; the corresponding 5-modular lattice ($\Delta(5,2)$ in our notation) has minimum 5. As before, Theorem 7.1 yields $\min \Delta(p,n) \geq (p+1)/2$ for all $n \geq 2$.

Gram matrices of the lattices $\Delta(p,n)$, $\Delta^-(p,n)$ are given in §5 using a discrete analogue of *Maslov index*. In a few words, our explicit constructions can be described as follows. First we start with the case n is odd and the group G_n^-. Using *Lagrangians*, an idea going back to [BaV] (cf. §3) and Maslov index (cf. §5), we explicitly construct the unimodular lattices $\Delta(p,n)$ (for any odd prime p). Then *descending* from $n+1$ to n (cf. §4), we obtain the p-modular lattices $\Delta(p,n)$ which are stable under G_n^+, for any even n and any odd prime p. Finally, let $p \equiv 1 \bmod 4$. Then the isoclinism between $C_2 \times G_n^+$ and G_n^- and Proposition 2.4 allow us to construct the lattices $\Delta^-(p,n)$, for any n.

We wish to point out that V cannot contain simultaneously invariant unimodular and p-modular lattices. Namely, the unimodular lattices are acted on faithfully by G_n^-, and the p-modular ones by G_n^+. Moreover, the invariant unimodular (p-modular) lattices are essentially unique (if they exist). More precisely, the classification of G_n-invariant lattices in V_n is provided by the following theorem. Given a lattice Γ, let $\Gamma^\#$ denote the dual lattice and Γ^0 denote the sublattice consisting of all vectors of even norm in Γ; furthermore, $\Gamma^1 = \Gamma \cap 2(\Gamma^0)^\#$. Two integral lattices $(\Gamma, (\cdot,\cdot))$ and $(\Gamma', (\cdot,\cdot)')$ are called *similar* if there exist a surjective homomorphism $\phi : \Gamma \to \Gamma'$ and a scalar $\lambda \in \mathbb{Q}$ such that $(\phi(u), \phi(v))' = \lambda(u,v)$ for any $u, v \in \Gamma$.

Theorem 1.3. *Let p be any odd prime and n any integer. Suppose that G_n acts irreducibly on an integral lattice Γ of rank p^n+1, with kernel K. If $p^n = 3$ or $p^n = p \equiv 1 \bmod 6$, then suppose in addition that S_n acts reducibly on $\Gamma \otimes \mathbb{C}$. Then one of the following holds.*

(i) *G_n/K is equal to G_n^- for odd n, and G_n^+ for even n. Furthermore, Γ is similar to one of the lattices Δ, Δ^0, Δ^1, where $\Delta = \Delta(p, n)$.*

(ii) *$p \equiv 1 \bmod 4$, and G_n/K is equal to G_n^+ for odd n, and G_n^- for even n. Furthermore, Γ is similar to one of the lattices Δ, Δ^0, Δ^1, where $\Delta = \Delta^-(p, n)$.*

The $GL_2(p)$-invariant $(p+1)$-dimensional lattices which are not covered by Theorem 1.3 (here $p = 3$ or $p \equiv 1 \bmod 6$) have been investigated in [NPl], Theorem (V.4).

The full automorphism groups of *all* G_n-invariant lattices Λ in V_n have been determined in [Tiep 1]. In particular, if $n > 1$, then either $\mathrm{Aut}(\Lambda) \in \{C_2 \times G_n^+, G_n^-\}$, or $p = 3$ and $\mathrm{Aut}(\Lambda) = (C_6 \cdot PSp_{2n}(3)) \cdot C_2$.

2. Implicit proofs

We recall the notations S_n, ψ of degree $(p^n + 1)/2$, G_n, Z, G_n^+, G_n^-. We start with the following simple observation:

Lemma 2.1. *Let p be any odd prime and n any integer. Suppose χ is an irreducible complex character of G_n of degree $p^n + 1$ with the following properties:*

(i) *χ restricted to S_n is equal to $\psi + \overline{\psi}$;*

(ii) *χ is rational-valued.*

Then one of the following holds.

(a) *χ is a faithful character, say χ^+, of G_n^+; furthermore, n is even if $p \equiv 3 \bmod 4$.*

(b) *χ is a faithful character, say χ^-, of G_n^-; furthermore, n is odd if $p \equiv 3 \bmod 4$.*

Proof. Let $K = \mathrm{Ker}\,\chi$. Schur's Lemma and (ii) imply that $Z/(Z \cap K)$ is a cyclic group of order at most 2. In particular, either $K = Z$, or $K = Z^2$. Observe that G_n permutes the two characters ψ and $\overline{\psi}$ of S_n nontrivially. Denote $\bar{G} = G_n/K$, $\bar{S} = S_n/(S_n \cap K)$.

First consider the case $K = Z$. Since $K \subseteq \mathrm{Ker}\,\psi$, the degree $\psi(1)$ is odd, i.e. $p^n \equiv 1 \bmod 4$. Here we have $\bar{G} = G_n^+$, $\bar{S} = PSp_{2n}(p)$, and $\bar{G} = \bar{S} \cdot C_2$. Clearly, the desired character χ is now uniquely determined: $\chi = \mathrm{Ind}_{\bar{S}}^{\bar{G}}(\psi)$.

Next let $K = Z^2$. If $p \equiv 1 \bmod 4$, then $\bar{G} = (\bar{S} \times Z/K) \cdot C_2$. If $p \equiv 3 \bmod 4$, then in view of (i) n must be odd, and $\bar{G} = \bar{S} \cdot C_2$. Now the desired character χ exists and is unique: $\chi = \mathrm{Ind}_{\bar{S}}^{\bar{G}}(\psi)$ if $p \equiv 3 \bmod 4$, and $\chi = \mathrm{Ind}_{\bar{S} \times Z/K}^{\bar{G}}(\widetilde{\psi})$ if $p \equiv 1 \bmod 4$ (where $\widetilde{\psi}$ is equal to ψ on $\bar{S}$ and to $-\psi(1)$ on the unique nontrivial element of Z/K). Clearly, $\mathbb{Q}(\chi) = \mathbb{Q}$. □

As we have mentioned above, $C_2 \times G_n^+$ and G_n^- are isoclinic to each other if $p \equiv 1 \bmod 4$. In this case, $\mathrm{ind}(\psi) = 1$ (cf. [Gro], Corollary 13.7); hence by Lemma 2.11 of [Tiep 2] $\mathrm{ind}(\chi^+) = \mathrm{ind}(\chi^-) = 1$. If $p \equiv 3 \bmod 4$ and n is odd, then $\mathrm{ind}(\psi) = 0$, and $\mathrm{ind}(\chi^-) = 1$ (see [SchT] or Proposition 2.3 below). Hence by Lemma 2.11 of [Tiep 2], the corresponding character of degree $p^n + 1$ of the isoclinic variant of G_n^- (which now is not isomorphic to $C_2 \times G_n^+$) has Schur-Frobenius indicator -1 and so cannot be written over $\mathbb{R}$. Similarly, if $p \equiv 3 \bmod 4$, then $\mathrm{ind}(\psi) = 0$, $\mathrm{ind}(\chi^+) = 1$, but the corresponding character of degree $p^n + 1$ of the isoclinic variant of $C_2 \times G_n^+$ (which is no longer G_n^-) cannot be written over $\mathbb{R}$.

The next proposition is an analogue of [SchT], Lemma 5.1.

Proposition 2.2. *Let p be an odd prime and n any integer. Let r be any prime and let χ be as in Lemma 2.1. Then the following assertions hold.*

(i) *The reduction $\chi \bmod r$ is irreducible if $r \neq 2, p$.*

(ii) $\chi \bmod 2 = 2 \cdot 1_{G_n} + \beta$ *for a certain $\beta \in \mathrm{IBr}_2(G_n)$. Furthermore, β is of symplectic type, if $p \equiv 1 \bmod 4$.*

(iii) $\chi \bmod p = \eta_1 + \eta_2$, *where $\eta_1, \eta_2 \in \mathrm{IBr}_p(G_n)$ are distinct characters which can be written over $\mathbb{F}_p$. Furthermore, for $k = 1, 2$ η_k is not self-dual if $\chi = \chi^-$, and η_k is of type $+$ if $\chi = \chi^+$.*

Proof. The case $p^n \equiv 3 \bmod 4$ has already been handled in [SchT] (cf. the proof of Theorem 1.1 and Lemma 5.1 therein). Hence in what follows we suppose that $p^n \equiv 1 \bmod 4$.

1) It is well-known (see e.g. [Gow], [Gro]) that $\psi \bmod r \in \mathrm{IBr}_r(S_n)$ for any odd prime r. Furthermore, $\psi \bmod 2 = 1_{S_n} + \alpha$ for some $\alpha \in \mathrm{IBr}_2(S_n)$. If x is a regular unipotent element of S_n, then $\psi(x) = (1 \pm p^{n-1}\sqrt{\epsilon p})/2$. Furthermore, ϑ_n interchanges the S_n-conjugacy classes of x and some power of x^s and $\psi(x^s) = (1 \mp p^{n-1}\sqrt{\epsilon p})/2$. Therefore, $\chi \bmod r \in \mathrm{IBr}_r(G_n)$ for any prime r, $r \neq 2, p$. On the other hand, $\chi \bmod 2 = 2 \cdot 1_{G_n} + \beta$ for some $\beta \in \mathrm{IBr}_2(G_n)$. If $p \equiv 1 \bmod 4$, then the fact that α is of symplectic type has been established in [GoW]. From this it follows by [Tiep 2], Lemma 2.4 that β is of symplectic type.

2) Consider the reduction $\chi \bmod p$. Recall that $\chi|_{S_n} = \psi + \overline{\psi}$. It is shown in [Gro] that $\psi \bmod p = \overline{\psi} \bmod p = \eta$ is obtained by restricting the irreducible algebraic representation of $Sp_{2n}(\overline{\mathbb{F}_p})$ with highest weight $\frac{p-1}{2}\omega_n$ to S_n. Furthermore, due to Lemma 2.6 [Tiep 3], η is invariant under the action of the distinguished element ϑ_n. Therefore, G_n has just two irreducible Brauer characters η_1, η_2 with $\eta_k|_{S_n} = \eta$ and $\eta_1 + \eta_2 = 0$ on $G_n \setminus S_n$. In this case, $\chi \bmod p = \eta_1 + \eta_2$, since $\chi = 0$ on $G_n \setminus S_n$.

3) We can embed S_n into $T = Sp_{2n}(p^2)$ in the following way. In a natural $2n$-dimensional $\mathbb{F}_{p^2}$-module $\widetilde{W}$ of T consider a symplectic basis

$$(e_1, \dots, e_n, f_1, \dots, f_n).$$

In this basis we can set $W = \langle e_1, \dots, e_n, f_1, \dots, f_n \rangle_{\mathbb{F}_p}$, $J = \mathrm{diag}(\varsigma^{-1}E_n, \varsigma E_n)$. Here $\varsigma \in \mathbb{F}_{p^2}$ is chosen with order $2(p-1)$ such that $\theta = \varsigma^2$. Now we set $S_n = T \cap \mathrm{End}(W) \simeq Sp_{2n}(p)$, $H = \langle S_n, J \rangle$. Then $J^2 \in S_n$ and J normalizes S_n; therefore $H \simeq S_n \cdot C_2$. Furthermore, $H/Z(S_n) \simeq G_n^+$.

Assume $p \equiv 1 \bmod 4$. Factoring the embedding $S \hookrightarrow Sp_{2n}(\overline{\mathbb{F}_p})$ through $T = Sp_{2n}(p^2)$, one sees that η is extended to two absolutely irreducible Brauer characters μ_1, μ_2 of H. We calculate the value of μ_1, μ_2 at the element J. If one denotes $\sigma = \exp(\frac{\pi i}{p-1})$, then $\mu_1(J) = \sum_{u \in I_n^+} \sigma^{|u|}$, since $n(p-1)/2$ is even in our case. Here

$$I_n^+ = \left\{ u = (u_1, \dots, u_n) \mid u_j \in \mathbb{Z}, |u_j| \leq (p-1)/2, \sum_{j=1}^n u_j \equiv 0 \bmod 2 \right\},$$

$$I_n^- = \left\{ u = (u_1, \dots, u_n) \mid u_j \in \mathbb{Z}, |u_j| \leq (p-1)/2, \sum_{j=1}^n u_j \equiv 1 \bmod 2 \right\},$$

$$S_n^+ = \sum_{u \in I_n^+} \sigma^{|u|},\ S_n^- = \sum_{u \in I_n^-} \sigma^{|u|},$$

and $|u| = \sum_j u_j$ for $u \in I_n^{\pm}$. Denote also $\tau = \cot(\frac{\pi}{2(p-1)})$. Then we have

$$S_1^+ = \frac{\tau - \tau^{-1}}{2},\ S_1^- = \frac{\tau + \tau^{-1}}{2},$$

$$S_{n+1}^+ = S_n^+ S_1^+ + S_n^- S_1^-,\ S_{n+1}^- = S_n^+ S_1^- + S_n^- S_1^+.$$

From this it follows that

$$S_n^+ = \frac{\tau^n + (-\tau)^{-n}}{2},\ S_n^- = \frac{\tau^n - (-\tau)^{-n}}{2}.$$

In particular, $\mu_1(J) = (\tau^n + (-\tau)^{-n})/2$. Since $p \geq 5$, $\tau > 1$, and so $\mu_1(J)$ is a positive real number. Moreover, the Frobenius endomorphism $\sigma \mapsto \sigma^p$ sends σ to $-\sigma$, $i = \sigma^{(p-1)/2}$ to i, $\mu_1(J)$ to $\mu_1(J) = -\mu_2(J)$. We have shown that $\mu_k^{(p)} = \mu_k = \overline{\mu_k}$ for $k = 1, 2$.

If $p \equiv 3 \bmod 4$, then n is even. Under the above notation, the computation in the proof of [SchT], Lemma 5.1 shows that $\mu_1(J) = (\tau^n + \tau^{-n})/2$. In particular, $\mu_1(J)$ is again a positive real number. Moreover, the Frobenius endomorphism $\sigma \mapsto \sigma^p$ sends σ to $-\sigma$, $i = \sigma^{(p-1)/2}$ to $-i$, $\mu_1(J)$ to $\mu_1(J) = -\mu_2(J)$. Therefore, $\mu_k^{(p)} = \mu_k = \overline{\mu_k}$ for $k = 1, 2$.

4) Here we consider the case $\chi = \chi^+$. Since $\operatorname{Ker} \mu_k = Z(S_n)$ and $H/Z(S_n) \simeq G_n^+$, we have $\eta_k = \mu_k$, $k = 1, 2$. Thus η_k can be written over $\mathbb{F}_p$. Furthermore, since η_k is real-valued and $\eta_k|_{S_n} = \eta$ is of quadratic type, η_k itself is of quadratic type.

5) Next let $\chi = \chi^-$. Then $p \equiv 1 \bmod 4$. Consider a representation $\Phi : H \to GL_{(p^n+1)/2}(\overline{\mathbb{F}_p})$ with Brauer character μ_1. Put $\omega = \varsigma^{(p-1)/2}$, and set $\widetilde{G} = \{\pm\Phi(g), \pm\omega\Phi(h) \mid g \in S_n,\ h \in H\backslash S_n\}$. Since $\omega^2 = -1$, $\widetilde{G}$ is a group. We claim that $\widetilde{G} \simeq \bar{G} = G_n/K = G_n^-$, where $K = \operatorname{Ker}\chi \simeq Z^2$. For the proof, we first observe that $\widetilde{G}$ is generated by the subgroup $G' = \{\pm\Phi(g) \mid g \in S_n\}$ and the element $\omega\Phi(J)$. Observe that the representation Φ is not faithful: its kernel is equal to the center $Z(S_n)$ of S_n. But the factor-group $H/Z(S_n) \simeq PSp_{2n}(p) \cdot C_2$ has trivial center; therefore $\Phi(H)$ also has trivial center. In particular, $G' \simeq S_n/Z(S_n) \times C_2$. The subgroup C_2 here is generated by $\mathbf{j}$, the multiplication by -1 (on the representation space of Φ); hence we can identify $\mathbf{j}$ with the central element θE_{2n} in $\bar{G}$. Now one has:

$$\vartheta_n^2 = \operatorname{diag}(E_n, \theta^2 E_n) = \theta E_{2n} \cdot \operatorname{diag}(\theta^{-1} E_n, \theta E_n) = \mathbf{j} J^2,$$
$$(\omega\Phi(J))^2 = -\Phi(J^2) = \mathbf{j}\Phi(J^2).$$

Modulo $Z(S_n) = \operatorname{Ker}(\Phi|_{S_n})$ one can identify the two elements ϑ_n^2 and $(\omega\Phi(J))^2$. Furthermore, the actions of $\omega\Phi(J)$ and of ϑ_n on S_n via conjugation are obviously the same. This means that $\widetilde{G} \simeq \bar{G}$.

The isomorphism $\bar{G} \simeq \widetilde{G}$ gives us a representation $\Psi : G_n \to GL_{(p^n+1)/2}(\overline{\mathbb{F}_p})$ with kernel K. One may suppose that this representation affords the Brauer character η_1. Then $\eta_1(\vartheta_n) = \sqrt{-1}\mu_1(J)$. The computations in item 3) show that $\eta_1(\vartheta_n)$ is purely imaginary, and that the Frobenius endomorphism $^{(p)}$ leaves $\eta_1(\vartheta_n)$ fixed. Consequently, for $k = 1, 2$ the Brauer character η_k can be realized over $\mathbb{F}_p$ but it is not real. □

Proposition 2.3. *Let p be any odd prime and n any integer. Let χ be as in Lemma 2.1. Then χ is afforded by a $\mathbb{Q}G_n$-module (of dimension $p^n + 1$).*

Proof. 1) First we give an argument settling the case where n is odd and $\chi = \chi^-$. Let $q = p^n$. Then we can identify W with $\mathbb{F}_q^2$, and endow W with the symplectic form $\langle u, v\rangle = \mathrm{tr}(ad - bc)$, where $u = (a, b)$, $v = (c, d)$, $a, b, c, d \in \mathbb{F}_q$, and tr stands for the trace form $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$. Make the group

$$R = \{\varphi \in H = GL_2(q) \mid \det \varphi \in \mathbb{F}_p^\bullet\} \simeq SL_2(q) \cdot C_{p-1}$$

act on W in a natural way. Clearly, this action embeds R in $G_n = CSp(W)$. Let T denote the central subgroup $\{\mathrm{diag}(\lambda, \lambda) \mid \lambda \in \mathbb{F}_q^{\bullet 2}\} \simeq C_{(q-1)/2}$ of H. Then the assumption that n is odd implies that $T \cap R = K$, where $K = \mathrm{Ker}\,\chi = C_{(p-1)/2}$, and $RT = H$. Hence, $\chi|_R$ can be viewed as a faithful character of $R/K = R/(T \cap R) \simeq H/T$ and so as a character, say ρ, of H (with kernel T). Beside that, the restriction of χ to the subgroup $R' = SL_2(q)$ is the sum of two irreducible Weil characters of degree $(q+1)/2$ of R'. Inspecting the character table of H (cf. [DiM]) we see that $\rho = \mathrm{Ind}_B^H(\mu)$, where

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{F}_q^\bullet, c \in \mathbb{F}_q \right\}$$

is a Borel subgroup of H, and the linear character μ sends $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ to $\delta(a)$, δ the quadratic character of $\mathbb{F}_q$. In particular, ρ is rational and absolutely irreducible. The same is true for $\chi|_R$. Now a standard lemma (see for instance [KoT], Lemma 8.3.1) says that χ is also rational.

2) Now we give another argument handling the case $p^n \equiv 1 \bmod 4$. The equality $\mathbb{Q}(\chi) = \mathbb{Q}$ implies by the Brauer-Speiser theorem that the Schur index $m_{\mathbb{Q}}(\chi)$ is either 1 or 2. If $m_{\mathbb{Q}}(\chi) = 1$, we are done. Assuming $m_{\mathbb{Q}}(\chi) = 2$, we get an irreducible $\mathbb{Q}G_n$-module V with character 2χ. Clearly, the commuting algebra $\mathbb{K} = \mathrm{End}_{G_n}(V)$ is a quaternion algebra over $\mathbb{Q}$. If a prime r is ramified in $\mathbb{K}$, then there exists a Brauer character μ such that $\chi \bmod r = \mu + \mu^{(r)}$. By Proposition 2.2, this cannot occur for any prime r. Thus $\mathbb{K}$ is unramified at any prime r, and by Hasse's principle we get a contradiction. □

Having established Proposition 2.3, we are given a $\mathbb{Q}G$-module $V = V_n$ with character χ such that $\chi|_{S_n} = \psi + \overline{\psi}$, where $(G, \chi) = (G_n^+, \chi^+)$ or (G_n^-, χ^-). We shall maintain this notation in what follows.

Proof of Theorem 1.1. Proposition 2.2 shows that the pair $(G, \chi) = (G_n^-, \chi^-)$ satisfies the conditions (i), (ii) of Proposition 2.4 from [SchT]. Below (cf. (7) and Corollary 4.3) we shall see that condition (iii) is also fulfilled: $\det V = \mathbb{Q}^{\bullet 2}$. Applying that proposition, we obtain a G_n^--invariant unimodular lattice Γ. Standard arguments show that Γ is odd, and $\min \Gamma \geq 3$ if $n > 1$. □

The link between lattices invariant under isoclinic groups is indicated in the following statement. We make use of the following observation: for any prime $p \equiv 1 \bmod 4$, there exist $a, b \in \mathbb{N}$ such that $a^2 - pb^2 = -1$ (cf. [Coh], pp. 105, 106). Henceforth we fix such a pair $\mathbf{a}, \mathbf{b}$.

Proposition 2.4. *Let $p \equiv 1 \bmod 4$ be a prime. Let $G^+ \simeq H \cdot C_2$ and $G^- = (H \cdot C_2)^-$ be isoclinic groups, where H is a finite group with center of order 2. Suppose V is an absolutely irreducible $\mathbb{Q}G^+$-module with character χ^+, and $\mathbb{Q}(\psi) = \mathbb{Q}(\sqrt{p})$ where $\chi^+|_H = \psi + \overline{\psi}$. Then the following assertions hold.*

(i) *V can be viewed as an absolutely irreducible $\mathbb{Q}G^-$-module. In particular, for each sign $\varepsilon \in \{+,-\}$, V has a unique (up to scalar) G^ε-invariant scalar product $(\cdot,\cdot)^\varepsilon$.*

(ii) *V has an endomorphism σ with the following properties: σ centralizes the group H, $\sigma^2 = p \cdot \mathrm{id}_V$, σ is a self-adjoint similarity of norm p w.r.t. both scalar products $(\cdot,\cdot)^\pm$, and*

$$g\sigma g^{-1} = -\sigma \text{ for } g \in G^\pm \smallsetminus H\,. \tag{1}$$

(iii) *V contains σ-stable lattices which are invariant under both groups G^+ and G^-.*

(iv) *Let Λ be a lattice as in (iii), and denote by Λ^ε, $\varepsilon \in \{+,-\}$, its dual lattice with respect to $(\cdot,\cdot)^\varepsilon$. After suitably rescaling one of $(\cdot,\cdot)^\varepsilon$, we have the equality*

$$\Lambda^- = \sigma^{-1}(\Lambda^+)\,.$$

On this scale, Λ is unimodular w.r.t. $(\cdot,\cdot)^+$ if and only if it is p-modular w.r.t. $(\cdot,\cdot)^-$. Similarly, Λ is p-modular w.r.t. $(\cdot,\cdot)^+$ if and only if it is unimodular w.r.t. $\frac{1}{p}(\cdot,\cdot)^-$.

Proof. The equality $\chi|_H = \psi + \overline{\psi}$ implies that the commuting algebra

$$\mathbb{K} = \mathrm{End}_H(V) = \{\varphi \in \mathrm{End}_{\mathbb{Q}}(V) \mid \forall h \in H, \varphi \cdot h = h \cdot \varphi\}$$

is isomorphic to the field $\mathbb{Q}(\psi) = \mathbb{Q}(\sqrt{p})$. Denoting by σ the (unique up to sign) element $\sigma \in \mathbb{K}$ with $\sigma^2 = p \cdot \mathrm{id}_V$, we have to show that it satisfies all other properties stated. We begin with (1). Fix an element $g \in G^+ \smallsetminus H$. For $h \in H$ and $\lambda \in \mathbb{K}$ it is readily checked that $h \cdot g\lambda g^{-1} = g\lambda g^{-1} \cdot h$; in other words, $g\lambda g^{-1} \in \mathbb{K}$. Thus, conjugation by g induces an automorphism of $\mathbb{K}$. If λ is fixed by this automorphism, then λ centralizes H and g, and thus G^+, that is, $\lambda \in \mathbb{Q}$. Thus, $\lambda \mapsto g\lambda g^{-1}$ is the unique nontrivial field automorphism of $\mathbb{K}$. Property (1) is a special case of this (σ corresponds to $\sqrt{p}$).

If Γ is any G^+-invariant lattice, then $\Gamma + \sigma(\Gamma)$ is clearly σ-invariant, and by (1) still G^+-invariant, which proves (iii) in the "+"-case. The scalar product $(\sigma(x), \sigma(y))$, $x, y \in V$, is also G^+-invariant and therefore of the form $(\sigma(x), \sigma(y)) = c(x, y)$ for some $c \in \mathbb{R}$. From $\sigma^2 = p \cdot \mathrm{id}_V$ it follows that $c = p$. The self-adjointness

$$(\sigma(x), y)^+ = (x, \sigma(y))^+$$

now is a formal consequence, and part (i) is proved for $(\cdot,\cdot)^+$.

Recall that we have fixed positive integers $\mathbf{a}$, $\mathbf{b}$ with $\mathbf{a}^2 - p\mathbf{b}^2 = -1$. Denote by $\rho \mapsto \bar\rho$ the non-trivial automorphism of $\mathbb{K}$, that is, $g\rho = \bar\rho g$ for any $g \in G^+ \smallsetminus H$ (see above), and by μ the particular element

$$\mu = \mathbf{a} + \mathbf{b}\sigma \in \mathbb{K}\,.$$

Since $\mu \circ \overline{\mu} = \overline{\mu} \circ \mu = -\mathrm{id}_V$, $\overline{\mu} = \mathbf{a} - \mathbf{b}\sigma$, this element induces in fact an automorphism of any G^+-stable lattice. If $g \in G^+ \smallsetminus H$ and $g' := g\mu$, then $g'^2 = g\mu g\mu = g^2\overline{\mu}\mu = -g^2$. Thus $\langle H, g'\rangle \cong G^-$. Observe that the particular representation of G^- thus constructed is obviously absolutely irreducible, and an H-invariant σ-stable lattice is G^+-invariant if and only if it is G^--invariant.

For a given choice of $(\cdot,\cdot)$, consider the bilinear form

$$(x, y)^- := (x, \sigma\mu(y))^+$$

which is clearly H-invariant. Since $\sigma\mu$ is self-adjoint w.r.t. $(\cdot,\cdot)^+$, this bilinear form is symmetric. From the fact that $\sigma\mu$ is a totally positive element in $\mathbb{K}$ it easily follows that $(\cdot,\cdot)^-$ is also positive definite. The following computation shows that $(\cdot,\cdot)^-$ is invariant under $g' = g\mu$ and thus under all of G^-:

$$\begin{array}{rcl}(g'x, g'y)^- & = & (g\mu(x), (\sigma\mu)g\mu(y))^+ \\ & = & (g\mu(x), g\overline{\sigma\mu}\mu(y))^+ \\ & = & (\mu(x), \overline{\sigma\mu}\mu(y))^+ \\ & = & (\mu(x), \sigma(y))^+ \\ & = & (x, \mu\sigma(y)) = (x,y)^-\end{array}$$

(since $\overline{\mu}\mu = -\operatorname{id}_V$).

For the dual lattices, we clearly have

$$\Lambda^- = (\sigma\mu)^{-1}\Lambda^+ = \sigma^{-1}\mu^{-1}\Lambda^+ = \sigma^{-1}\Lambda^+ .$$

If Λ is unimodular w.r.t. $(\cdot,\cdot)^+$, then $\Lambda^+ = \Lambda$; therefore $\Lambda^- = \sigma^{-1}(\Lambda)$, i.e. σ is the desired similarity between Λ and Λ^-. Conversely, if Λ is p-modular w.r.t. $(\cdot,\cdot)^-$, then

$$\begin{gathered} p^{\operatorname{rank}\Lambda/2} = (\Lambda^- : \Lambda) = (\sigma^{-1}(\Lambda^+) : \Lambda) \\ = (\Lambda^+ : \sigma(\Lambda)) = (\Lambda^+ : \Lambda)(\Lambda : \sigma(\Lambda)) = p^{\operatorname{rank}\Lambda/2}(\Lambda^+ : \Lambda), \end{gathered}$$

yielding $\Lambda^+ = \Lambda$. The last assertion follows from the previous one by considering $(x,y)^{--} := (x, \sigma(-\overline{\mu})(y))^-$. □

Clearly, Proposition 2.4 applies to $\{G^+, G^-\} = \{C_2 \times G_n^+, G_n^-\}$ and the module $V = V_n$, if $p \equiv 1 \bmod 4$. Also, the endomorphism σ is uniquely determined up to sign. Therefore, in what follows we can speak about σ-stable lattices in V.

We shall need the following supplement to Proposition 2.4:

Lemma 2.5. *Keep all the notation of Proposition 2.4. Suppose that, as $\mathbb{F}_pH$-module, $U := \Lambda/p\Lambda$ is the direct sum of two copies M, M' of an absolutely irreducible $\mathbb{F}_pH$-module. Then the $\mathbb{F}_pG^+$-module U is indecomposable if and only if the $\mathbb{F}_pG^-$-module U is indecomposable.*

Proof. By our assumption, in a suitably chosen basis of $U = M \oplus M'$ the commuting algebra $K := \operatorname{End}_H(U)$ consists of matrices of the form $\begin{pmatrix} aE_n & bE_n \\ cE_n & dE_n \end{pmatrix}$, where $a, b, c, d \in \mathbb{F}_p$ and $n = \dim M$. Clearly, the endomorphism σ (cf. Proposition 2.4 (ii)) belongs to K, and without loss of generality one may suppose that $\sigma = \begin{pmatrix} 0 & E_n \\ 0 & 0 \end{pmatrix}$, because $\sigma^2 = 0$ on U. Recall that $G^+ = \langle H, g\rangle$ and $G^- = \langle H, g'\rangle$ with $g' = g(\mathbf{a} + \mathbf{b}\sigma)$. Since $g\sigma = -\sigma g$, g has the matrix $\begin{pmatrix} A & B \\ 0 & -A \end{pmatrix}$, and g' has the matrix $\begin{pmatrix} \mathbf{a}A & \mathbf{b}A + \mathbf{a}B \\ 0 & -\mathbf{a}A \end{pmatrix}$. Denoting $L^+ = \operatorname{End}_{G^+}(U)$, we see that $L^+ = C_K(g)$. In particular, if $f = \begin{pmatrix} xE_n & yE_n \\ zE_n & tE_n \end{pmatrix}$ belongs to L^+, then either $f = xE_{2n}$, or $x \neq t$ and $B = \frac{2y}{x-t}A$. Now observe that: the $\mathbb{F}_pG^+$-module U is decomposable if and only if L^+ contains two nonzero idempotents f, g such that $fg = gf = 0$ if and only if $B \in \langle A\rangle_{\mathbb{F}_p}$. The same applies to the $\mathbb{F}_pG^-$-module U. But

$$B \in \langle A\rangle_{\mathbb{F}_p} \Longleftrightarrow \mathbf{b}A + \mathbf{a}B \in \langle \mathbf{a}A\rangle_{\mathbb{F}_p};$$

hence our statement follows. □

Corollary 2.6. *Let $p \equiv 1 \bmod 4$ and n any integer. Then V_n contains σ-stable G_n^--invariant odd unimodular lattices.*

Proof. By Proposition 2.4, V_n contains σ-stable G_n^--invariant lattices. Choose such a lattice Γ with minimal possible determinant, and suppose that $\det \Gamma > 1$. Clearly, the symmetry of σ implies that the dual lattice $\Gamma^{\#}$ is σ-stable. In particular, taking the sum $\Gamma + m\Gamma^{\#}$, $m \in \mathbb{Z}$, produces again a σ-stable lattice. Hence Lemma 2.1 [SchT] holds inside the class of σ-stable lattices. Now the arguments in the proof of [SchT], Proposition 2.4, show that $A = \Gamma^{\#}/\Gamma = (C_2)^2$. Consider the form $q : A \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, $q(v+\Gamma) = (v,v) + \mathbb{Z}$. Clearly, σ acts on A as an endomorphism of order 1 or 2, and σ preserves q. If $\sigma = 1$ on A, then we are done by Lemma 2.2 [SchT]. If $\sigma \neq 1$ on A, then σ has a unique nonzero fixed vector $\bar{v}$ in A. This vector is obviously fixed by G_n^-, and one can check that $q(\bar{v}) = 0$. Thus $\langle \Gamma, v\rangle$ is a σ-stable G_n^--invariant unimodular lattice, contrary to the choice of Γ. □

A σ-stable G_n^--invariant odd unimodular lattice will be explicitly constructed in Theorem 3.9 (for odd n) and Corollary 5.9 (for even n and $p \equiv 1 \bmod 4$).

Proof of Theorem 1.2 for the case $p \equiv 1 \bmod 4$. By Corollary 2.6, V_n contains a σ-stable G_n^--invariant unimodular lattice ∇. Applying Proposition 2.4, we obtain a G_n^+-invariant scalar product on ∇ that converts it into a p-modular lattice which is acted on by G_n^+. □

Remark 2.7. Let $n = 1$ and $p \equiv 1 \bmod 4$. Then Proposition 2.3 and its proof tell us that the group $G_1^- = GL_2(p)/C_{(p-1)/2}$ has a (unique) faithful, absolutely irreducible, rational representation of degree $p+1$, which is monomial. On the other hand, $G_1^+ = PGL_2(p)$ has a (unique) faithful, absolutely irreducible, rational representation of degree $p+1$, which is non-monomial. These observations were mentioned in [NPl], Lemma (V.3) and its proof. Theorem (V.2) of [NPl] exposes a G_1^+-invariant lattice of rank $p+1$ and determinant $p^{(p+1)/2}$, called $M_{p+1,2}$. Observe that $M_{p+1,2}$ is obtained from the G_1^--invariant lattice with Gram matrix E_{p+1} by means of the procedure indicated in Proposition 2.4. Hence by this proposition $M_{p+1,2}$ is p-modular.

An explicit construction of G_n^--invariant odd unimodular lattices is exposed in Theorem 3.9 for any odd n. Combined with the procedure indicated in Proposition 2.4, this yields an explicit construction of G_n^+-invariant p-modular lattices $\Delta^-(p,n)$ for any odd n (cf. Corollary 5.10), which generalizes Theorem (V.2) of [NPl].

The rest of the section is devoted to proving Theorem 1.2 for the case $p \equiv 3 \bmod 4$. Denote $\theta = \sqrt{-p}$, $\pi = (1+\theta)/2$, $\mathbb{K} = \mathbb{Q}(\theta)$, $\mathfrak{o} = \langle 1, \pi\rangle_{\mathbb{Z}}$ the maximal order in $\mathbb{K}$. By Proposition 5.2 [SchT], whose proof does not use the oddness of n, $V = V_n$ has an endomorphism σ such that

$$\sigma^2(v) = -pv,\ (\sigma(u),v) = -(u,\sigma(v)),\ (\sigma(u),\sigma(v)) = p(u,v),\\ s\sigma s^{-1} = \sigma,\ g\sigma g^{-1} = -\sigma \tag{2}$$

for any $u, v \in V$, $s \in \bar{S}_n = PSp_{2n}(p)$, $g \in G_n^+ \setminus \bar{S}_n$. Following the proof of that proposition, it is not difficult to show that V contains a G_n^+-invariant lattice Λ, which is stable under the endomorphism $(1+\sigma)/2$. For $u, v \in V$ we set

$$u \circ v = \frac{(u,v)}{2} + \theta\frac{(u,\sigma(v))}{2p} \in \mathbb{K}. \tag{3}$$

Using (2) it is straightforward to check that $v \circ u = \overline{u \circ v}$, $u \circ \sigma(v) = -\theta(u \circ v)$, $su \circ sv = u \circ v$, $gu \circ gv = v \circ u$, and

$$(u, v) = \mathrm{Tr}(u \circ v), \tag{4}$$

where $s \in \bar{S}_n$, $g \in G_n^+ \setminus \bar{S}_n$, and Tr denotes the trace of $\mathbb{K}$ over $\mathbb{Q}$. Thus, if we set $\theta \cdot v = \sigma(v)$, then V is a $\mathbb{K}$-space of dimension $(p^n+1)/2$, with $\bar{S}_n$-invariant positive definite Hermitian scalar product $u \circ v$. Multiplying $(\cdot, \cdot)$ by a suitable scalar, for instance by $2p$, we can ensure that $\Lambda \circ \Lambda \subseteq \mathfrak{o}$. Thus Λ is a G_n^+-invariant integral $\mathfrak{o}$-lattice, that is contained in its *Hermitian dual*,

$$\Gamma^{\perp} = \{u \in V \mid u \circ \Gamma \subseteq \mathfrak{o}\}.$$

The property (4) by the way characterizes the Hermitian form uniquely, that is, implies (3). Clearly, both $\Lambda^{\perp}$ and $\Lambda^{\#}$, the Euclidean dual, are stable under $\mathfrak{o}$ and G_n^+. Using (3), one readily checks that

$$\Lambda^{\perp} = \theta\Lambda^{\#}.$$

(This is actually well known from (4), since (θ) is the different of $\mathfrak{o}$ over $\mathbb{Z}$.) We shall use this formula frequently in what follows. We shall also need the following two simple statements.

Lemma 2.8. *Let $p \equiv 3 \bmod 4$ as above, and let G be a finite group. Suppose that Γ is a G-invariant integral Hermitian $\mathfrak{o}$-lattice such that $\Gamma \supseteq 2\Gamma^{\perp}$. Then the $\mathbb{F}_2G$-module $\Gamma^{\perp}/\Gamma$ supports a non-degenerate G-invariant alternating form, namely $b(u,v) = \mathrm{Tr}(2u \circ v) \bmod 2$ for any $u, v \in \Gamma^{\perp}$. In particular, the index $(\Gamma^{\perp} : \Gamma)$ differs from 2 for any integral hermitian $\mathfrak{o}$-lattice Γ.*

Proof. Since $\Gamma \supseteq 2\Gamma^{\perp}$, $2u \in \Gamma$ and so $2u \circ v \in \mathfrak{o}$ and $\mathrm{Tr}(2u \circ v) \in \mathbb{Z}$ for all $u, v \in \Gamma^{\perp}$. If $v \in \Gamma$, then $2u \circ v \in 2\mathfrak{o}$ and $\mathrm{Tr}(2u \circ v) \in 2\mathbb{Z}$. Thus b is well defined. Clearly, it is $\mathbb{F}_2$-bilinear and G-invariant. If $u \in \Gamma^{\perp}$, then $2u \circ u \in \mathbb{R} \cap \mathfrak{o} = \mathbb{Z}$, yielding $b(u,u) = 0$, i.e. b is alternating. Finally, assume that $v \in \Gamma^{\perp}$ such that $\mathrm{Tr}(u \circ v) \in \mathbb{Z}$ for any $u \in \Gamma^{\perp}$. Then $v \in (\Gamma^{\perp})^{\#} = \theta^{-1}\Gamma^{\perp\perp} = \theta^{-1}\Gamma$ and $\theta^{-1}\Gamma \cap (1/2)\Gamma = \Gamma$. In other words, b is non-degenerate. □

Lemma 2.9. *Let Γ be an $\bar{S}_n$-invariant $\mathfrak{o}$-lattice in V. Suppose that the index $(\Gamma^{\perp} : \Gamma)$ is divisible by p. Then in fact $\Gamma \subseteq p\Gamma^{\perp}$.*

Proof. Consider the $\mathbb{F}_p\bar{S}_n$-module $U = \Gamma/\theta\Gamma$. Here we are identifying $\mathfrak{o}/\theta\mathfrak{o}$ with $\mathbb{F}_p$ (and π with $1/2$). First we show that $\Gamma \subseteq \theta\Gamma^{\perp}$. We know that U is a simple $\mathbb{F}_pS_n$-module with character $\psi \bmod p$. Furthermore, $U' = (\Gamma \cap \theta\Gamma^{\perp})/\theta\Gamma$ is an S_n-submodule of U. Suppose that $U' = 0$. Then $\Gamma \cap \theta\Gamma^{\perp} = \theta\Gamma$. As $(\Gamma^{\perp} : \Gamma)$ is divisible by p, one can find a vector $v \in \theta\Gamma^{\perp} \setminus \theta\Gamma$ such that $pv \in \theta\Gamma$. Then

$$\theta v \in p\Gamma^{\perp} \cap \Gamma \subseteq \theta\Gamma^{\perp} \cap \Gamma = \theta\Gamma,$$

i.e. $v \in \Gamma$. Hence, $v \in \Gamma \cap \theta\Gamma^{\perp} = \theta\Gamma$, contradicting the choice of v. Therefore, $U' \neq 0$, which implies that $U' = U$, $\Gamma \subseteq \theta\Gamma^{\perp}$.

Now we can define on U an S_n-invariant form:

$$f(\bar{x}, \bar{y}) = \frac{1}{\theta} x \circ y \bmod \theta\mathfrak{o},$$

where $\bar{x} = x + \theta\Gamma$, $\bar{y} = y + \theta\Gamma$. Clearly, f is well defined and bilinear. But f is alternating: $f(\bar{x}, \bar{x}) = 0$ because $x \circ x \in \mathbb{R} \cap \theta\mathfrak{o} = \theta^2\mathbb{Z}$ for any $x \in \Gamma$. Suppose the kernel of f is zero. Then U carries a non-degenerate alternating bilinear form (namely f) and so ψ mod p is of symplectic type, contrary to Proposition 2.2 (iii). We have shown that the kernel of f is nonzero. Since U is irreducible, f is zero, i.e. $\Gamma \subseteq p\Gamma^{\perp}$. $\square$

Now we choose a G_n^+-invariant $\mathfrak{o}$-lattice Λ lying in V such that $\det \Lambda = (\Lambda^{\#} : \Lambda)$ is minimal. We also suppose that Λ is not integral for any rescaled Hermitian form $\frac{1}{\lambda} u \circ v$ with $\lambda \in \mathbb{R}$ and $\lambda > 1$. (If such a λ exists, we simply divide the Hermitian scalar product to λ and get an invariant Hermitian lattice with strictly smaller determinant.)

First we observe that $\det \Lambda$ cannot be divisible by any odd prime $r \neq p$. Suppose the contrary. Then consider the form $(\bar{x}, \bar{y})_r = (x, y) \bmod r$ on $\Lambda / r\Lambda$, where $\bar{x} = x + r\Lambda$, $\bar{y} = y + r\Lambda$. As r divides $\det \Lambda$, this G_n^+-invariant symmetric bilinear form is degenerate, and so its kernel $(\Lambda \cap r\Lambda^{\#})/r\Lambda$ is nonzero. By Proposition 2.2 (i) this means simply that $\Lambda \subseteq r\Lambda^{\#}$. Then for any $u, v \in \Lambda$ one has $(u, v), (u, \pi v) \in r\mathbb{Z}$. Denote $u \circ v = a + \pi b$ for some $a, b \in \mathbb{Z}$. Then $(u, v) = 2a + b$ and $(u, \pi v) = a - b(p-1)/2$ belong to $r\mathbb{Z}$. This implies $a, b \in r\mathbb{Z}$. In particular, $u \circ v \in r\mathfrak{o}$ for any $u, v \in \Lambda$. Thus, one can divide the form $u \circ v$ by r, a contradiction.

We have seen that $\det \Lambda$ can be divisible only by the primes 2 and p. Furthermore, if p divides $(\Lambda^{\perp} : \Lambda)$, then by Lemma 2.9 one can divide the form $u \circ v$ by p, a contradiction. Therefore, there exists a non-negative integer k such that $(\Lambda^{\perp} : \Lambda) = 2^k$. In this case,

$$\det \Lambda = (\Lambda^{\#} : \Lambda^{\perp})(\Lambda^{\perp} : \Lambda) = 2^k p^N,$$

where $N = (p^n + 1)/2$.

It is obvious that $\Lambda \supseteq 2^k \Lambda^{\perp}$. Suppose that $\Lambda \not\supseteq 2\Lambda^{\perp}$. Let l denote the minimal integer such that $\Lambda \supseteq 2^l \Lambda^{\perp}$. Then $l \geq 2$. Set $\Gamma = \Lambda + 2^{l-1}\Lambda^{\perp}$. One readily checks that Γ is a G_n^+-invariant $\mathfrak{o}$-lattice with $\det \Gamma$ strictly smaller than $\det \Lambda$, contradicting the choice of Λ. Hence, $\Lambda \supseteq 2\Lambda^{\perp}$. This implies that $\Lambda \supseteq 2p\Lambda^{\#}$, i.e. the discriminant group $\Lambda^{\#}/\Lambda$ has exponent $2p$ (and order $2^k p^N$).

The inclusion $\Lambda \supseteq 2p\Lambda^{\#}$ also implies $k \leq 2N$. Setting $\Gamma = \sqrt{2}\Lambda^{\perp}$ (which is equivalent to considering $\Lambda^{\perp}$ and multiplying the form $u \circ v$ by 2), we have

$$\Gamma \circ \Gamma = \sqrt{2}\Lambda^{\perp} \circ \sqrt{2}\Lambda^{\perp} = 2\Lambda^{\perp} \circ \Lambda^{\perp} \subseteq \Lambda \circ \Lambda^{\perp} \subseteq \mathfrak{o},$$

i.e. Γ is an G_n^+-invariant integral $\mathfrak{o}$-lattice. Furthermore,

$$2\Gamma^{\perp} = \sqrt{2}\Lambda \subseteq \sqrt{2}\Lambda^{\perp} = \Gamma,$$

and

$$(\Gamma^{\perp} : \Gamma) = (\frac{1}{\sqrt{2}}\Lambda : \sqrt{2}\Lambda^{\perp}) = (\Lambda : 2\Lambda^{\perp}) = \frac{(\Lambda^{\perp} : 2\Lambda^{\perp})}{(\Lambda^{\perp} : \Lambda)} = 2^{2N-k}.$$

This computation shows that, after replacing Λ by Γ if necessary, one may suppose that $0 \leq k \leq N$. Claim that the last condition implies $k = 0, 1, 2$. For $F = (\Lambda \cap 2\Lambda^{\#})/2\Lambda$ is a G_n^+-submodule of $\Lambda/2\Lambda$, and $|F| = 2^k$. By Proposition 2.2 (ii), $k = 0$, 1, or 2.

We have arrived at the situation where $(\Lambda^{\perp} : \Lambda) = 2^k$, $k = 0, 1, 2$. By Lemma 2.8, $k \neq 1$. If $k = 0$, then $\Lambda = \Lambda^{\perp} = \theta\Lambda^{\#}$, and Λ is a p-modular Euclidean lattice of rank $2N$, and we are done. Suppose $k = 2$. Then the discriminant group $\Lambda^{\#}/\Lambda$ is isomorphic to $(C_2)^2 \oplus (C_p)^N$, and $(\Lambda^{\perp} : \Lambda) = (C_2)^2$. By Lemma 2.2 of [SchT], there exists a vector $v \in \Lambda^{\perp} \backslash \Lambda$ with $2v \in \Lambda$ such that $\Delta = \langle \Lambda, v \rangle_{\mathbb{Z}}$ is a G_n^+-invariant Euclidean lattice and $\Delta^{\#}/\Delta \simeq (C_p)^N$. Remark that $\theta\Delta \subseteq \Delta$. Indeed,

$\theta v = \pi \cdot 2v - v \in \Delta$. Furthermore, $\theta\Delta \subseteq p\Delta^{\#}$. (For

$$(\theta\Delta, \Delta) \subseteq (\theta\Lambda, \Lambda) + (\theta\Lambda, v) + (\Lambda, \theta v) + (\theta v, v).$$

Here, $\theta\Lambda \subseteq \theta\Lambda^{\perp} = p\Lambda^{\#}$, so $(\theta\Lambda, \Lambda) \subseteq p\mathbb{Z}$. As $v \in \Lambda^{\perp}$, we have $\Lambda \circ v \subseteq \mathfrak{o}$, and so

$$(\theta\Lambda, v) = (\Lambda, \theta v) \subseteq \theta\mathfrak{o} \cap \mathbb{Z} = p\mathbb{Z}.$$

Finally, $(\theta v, v) = \theta v \circ v - \theta v \circ v = 0$.) Now we have

$$(\theta\Delta : p\Delta) = p^N = (\Delta^{\#} : \Delta) = (p\Delta^{\#} : p\Delta);$$

therefore in fact $\theta\Delta = p\Delta^{\#}$, $\Delta = \theta\Delta^{\#}$. The map $f : x \mapsto \theta x$, where $x \in \Delta^{\#}$, maps $\Delta^{\#}$ onto Δ and preserves $(\cdot,\cdot)$ up to the scalar p: $(f(x), f(y)) = p(x, y)$. This means the lattice Δ is p-modular, as desired.

The proof of Theorem 1.2 is finished. □

Remark 2.10. Observe that all the lattices $\Delta = \Delta(p, n)$, $\Delta^-(p, n)$, are *symplectic* (for the definition of symplectic lattices cf. [BuS]). For suppose first that Δ is invariant under G_n^-. Then $\det \Delta = 1$. Taking $\tau = \begin{pmatrix} 0 & E_n \\ \theta E_n & 0 \end{pmatrix}$ (in the chosen symplectic basis of W), $\mathbb{F}_p^{\bullet} = \langle\theta\rangle$, one sees that $\tau \in G_n^-$ and $\tau^2 = \theta E_{2n}$ acts on Δ as -1. According to [BuS], this means that Δ is symplectic. Suppose now that Δ is invariant under G_n^+. If $p \equiv 3 \bmod 4$, then we put $\tau = \frac{1}{\sqrt{p}}\sigma$. Considered under the new scalar product $(u, v)' = (u, v)/\sqrt{p}$, the dual lattice of Δ equals $\tau(\Delta)$. Also, τ preserves $(\cdot,\cdot)'$ and $\tau^2 = -1$. Hence Δ is symplectic. Finally, let $p \equiv 1 \bmod 4$. Taking $g = \begin{pmatrix} 0 & E_n \\ \theta E_n & 0 \end{pmatrix}$, one sees that $g \in G_n^+ \setminus S_n$. Put $\tau = \frac{1}{\sqrt{p}} g\sigma$ and consider Δ w.r.t. the new scalar product $(\cdot,\cdot)'$ introduced above. Clearly, τ preserves $(\cdot,\cdot)'$ and sends Δ to its dual (w.r.t. the new scalar product). Besides, $g \in G_n^+ \setminus S_n$ implies that $\tau^2 = -\frac{1}{p} g^2\sigma^2 = -1$. Consequently, Δ is symplectic.

Remark 2.11. One could formalize Lemmas 2.8, 2.9 and the above arguments in order to get an analogue of Proposition 2.4 in [SchT] for the existence of p-modular lattices. Here is one more well known example. Let $G = {}^2G_2(3) = SL_2(8) \cdot C_3$ and χ an irreducible complex character of G of degree 7 with $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{-3})$. Then for any prime $r \neq 2, 3$, $\chi \bmod r$ is an irreducible Brauer character, which is not of quadratic type. Furthermore, $\chi \bmod 3$ is irreducible and of quadratic type. Finally, $\chi \bmod 2$ is a sum of a character of degree 1 and an irreducible Brauer character of degree 6 which is of symplectic type. From this it follows that G has an irreducible $\mathbb{Q}$-module V with character $\chi + \overline{\chi}$. The above arguments show that G stabilizes a 3-modular lattice Λ in V with $\mathrm{Aut}(\Lambda) = C_2 \times G_2(3)$. The lattice Λ occurs in [Atlas] and was investigated in detail in [KoT], Chapter 8. It is the unique extremal 3-modular lattice in dimension 14, after [SchHem].

3. Explicit construction. I: n odd

We maintain the notation W for the natural $\mathbb{F}_p S_n$-module $\mathbb{F}_p^{2n}$ endowed with a non-degenerate symplectic form $\langle\cdot,\cdot\rangle$. Throughout this section we suppose that *n is odd*. We use the ideas of [SchT], §3 to explicitly construct G_n^--invariant lattices in $V = V_n$, for any odd prime p.

Consider an arbitrary G_n^--invariant (integral) lattice Λ in V. Fix a symplectic basis $(e_1, \ldots, e_n, f_1, \ldots, f_n)$ of W. Recall that G_n is generated by S_n and the element ϑ_n with matrix $\mathrm{diag}(E_n, \theta E_n)$ in this basis. We shall view V as a G_n-module with kernel $Z^2 \simeq C_{(p-1)/2}$. A *Lagrangian* is a maximal totally isotropic subspace in W. Following [BaV], we consider them *oriented*, i.e. equipped with an appropriate equivalence class of bases. Two bases $(l_1, \dots, l_n)$ and $(l'_1, \dots, l'_n)$ of a Lagrangian L are equivalent, i.e. define the same orientation, if the element $g \in GL_n(L)$ defined by $g(l_i) = l'_i$, $1 \le i \le n$, has $\det g \in \mathbb{F}_p^{\bullet 2}$. We denote by $\mathcal{L}(W)$ the set of all oriented Lagrangians contained in W.

To each Lagrangian L of W we now associate the following two subgroups:

(5) $$G(L) = \{\varphi \in G_n \mid \varphi(L) = L\}\,,\; S(L) = \left\{\varphi \in G(L) \mid \det(\varphi|_L) \in \mathbb{F}_p^{\bullet 2}\right\}.$$

Since the determinant of λE_{2n} ($\lambda \in \mathbb{F}_p^{\bullet 2}$) acting on any Lagrangian L is a square in $\mathbb{F}_p$, the definition (5) of $S(L)$ factors through the kernel Z^2 of χ. Let ξ_L denote the linear character of $G(L)$ (and $S(L)$) which sends $g \in G(L)$ to $\left(\frac{\det(\varphi|_{W/L})}{p}\right)$. Here and hereafter, $\left(\frac{\cdot}{p}\right)$ stands for the Legendre symbol.

Proposition 3.1. *Let n be odd. For any Lagrangian L in W, the sets*

$$\Lambda(L) = \{v \in \Lambda \mid \forall \varphi \in S(L), \varphi(v) = v\},$$
$$\Lambda^-(L) = \{v \in \Lambda \mid \forall \varphi \in S(L), \varphi(v) = \xi_L(g)v\}$$

are 1*-dimensional* $\mathbb{Z}$*-modules.*

Proof. 1) Without loss of generality, one can take $L = \langle e_1, \dots, e_n\rangle_{\mathbb{F}_p}$ with the basis $(e_1, \dots, e_n)$. Denote

$$P = St_S(L) = E \cdot H,\; Q = S(L),\; R = P \cap Q = E \cdot H^\bullet,$$

where $E = (C_p)^{n(n+1)/2}$, $H = GL_n(p)$, $H^\bullet = \{g \in GL_n(p) \mid \det g \in \mathbb{F}_p^{\bullet 2}\}$. A model for the Weil representation of S with character ψ is described in [Gro]. From this description it follows that $\psi|_P = \delta + \zeta$, where ζ is a P-character of degree $(p^n-1)/2$ and

$$\delta(\varphi) = \left(\frac{\det(\varphi|_L)}{p}\right)$$

for $\varphi \in P$. In particular, $\psi|_R = 1_R + \zeta|_R$.

If $n = 1$, one directly checks that the trivial character of $S(L)$ and the character ξ_L each enter into $\chi|_{S(L)}$ with multiplicity 1.

2) In this paragraph we suppose $n > 1$. We claim that $\zeta|_R \in \mathrm{Irr}(R)$. Indeed, one can identify E with the space of symmetric matrices of degree n over $\mathbb{F}_p$. Furthermore, $P/E = H$ acts on E by the rule:

$$A \circ X = A \cdot X \cdot {}^tA$$

for $A \in H$ viewed as an element of $GL_n(p)$ and $X \in E$. Obviously $E \not\subseteq \mathrm{Ker}\,\zeta$. So it is sufficient to show that every R/E-orbit on the set $\mathrm{Irr}(E) \setminus \{1_E\}$ has length $\ge (p^n-1)/2$, or equivalently, every $H^\bullet$-orbit on the set $E^* \setminus \{0\}$ has length $\ge (p^n-1)/2$. Here E is viewed as a $\mathbb{F}_p$-space, and E^* stands for the dual space. Actually, one can identify the $GL_n(p)$-module E^* with E itself, but endowed with the action $A \bullet X = {}^tA^{-1} \cdot X \cdot A^{-1}$, where $A \in GL_n(p)$, $X \in E$. (Indeed, each element $f \in E^*$ can be realized as the map $f = f_M : X \mapsto \mathrm{Tr}(X \cdot M)$ for a uniquely determined $M \in E$. Now we can write down the action of $A \in GL_n(p)$ on E^*:

$$\begin{aligned}(A \bullet f)(X) &= f_M(A^{-1} \circ X) = \mathrm{Tr}(A^{-1} \cdot X \cdot {}^tA^{-1} \cdot M)\\ &= \mathrm{Tr}(X \cdot {}^tA^{-1} \cdot M \cdot A^{-1}) = f_{A\bullet M}(X).)\end{aligned}$$

Consider a $GL_n(p)$-orbit $\mathcal{O}$ on $E\backslash\{0\}$ and $X \in \mathcal{O}$. Then the stabilizer $H(X)$ of X in $GL_n(p)$ is nothing else but the isometry group of the symmetric bilinear form on $\mathbb{F}_p^n$ with the matrix X. It is not difficult to show that the cardinality of $\mathcal{O}$ is $(p^n-1)/2$ if $\operatorname{rank} X = 1$, and strictly greater than $(p^n-1)/2$ if $\operatorname{rank} X > 1$ (and greater than p^n-1 if $\operatorname{rank} X = n > 1$). On the other hand, if $\operatorname{rank} X \leq n-1$, then $H(X)$ contains an element A not contained in $H^\bullet$, whence $\mathcal{O}$ is also an $H^\bullet$-orbit. Therefore, an $H^\bullet$-orbit in $E \setminus \{0\}$ can have length less than $(p^n-1)/2$ only in case $n = 1$. (When $n = 1$, any $H^\bullet$-orbit in $E \setminus \{0\}$ has length $(p^n-1)/4$.) Now $n > 1$ by our assumption, so our claim has been proved.

Decompose $V \otimes_{\mathbb{Q}} \mathbb{C}$ into a sum $U \oplus U_1 \oplus U_2$ of three R-submodules, with character $2 \cdot 1_R$, ζ and $\overline{\zeta}$, respectively. Remark that R contains a regular unipotent element x and $\zeta(x) = (-1 \pm p^{n-1}\sqrt{\epsilon p})/2$. Furthermore, $Q = \langle R, \vartheta_n\rangle$, and ϑ_n normalizes R. Therefore ϑ_n fixes U, and either leaves both U_1, U_2 invariant or interchanges them. But ϑ_n interchanges the S-conjugacy classes of x and $x^{\cdots}$ (some power of x), and $\zeta(x^{\cdots}) = \overline{\zeta(x)} \neq \zeta(x)$. This means ϑ_n interchanges U_1 and U_2. The construction of χ (see the proof of Lemma 2.1) ensures that $\chi(\vartheta_n) = 0$. As a consequence, ϑ_n acting on U has trace 0. Observe that ϑ_n^2 leaves U pointwise fixed. (Indeed, ϑ_n^2 is the product of $\alpha = \operatorname{diag}(\theta^{-1}E_n, \theta E_n)$ and $\beta = \theta E_{2n}$. Clearly, α belongs to P and acts on U as multiplication by $\delta(\alpha) = \left(\frac{\theta^{-n}}{p}\right) = -1$, because n is odd. Furthermore, β acts as multiplication by -1 on the whole of V.) We have shown that both of the subspaces

$$\widetilde{F} = \{v \in V \otimes_{\mathbb{Q}} \mathbb{C} \mid \forall\, \varphi \in Q,\ \varphi(v) = v\} = U \cap \operatorname{Ker}(\vartheta_n - 1),$$

$$\widetilde{F}^- = \{v \in V \otimes_{\mathbb{Q}} \mathbb{C} \mid \forall\, \varphi \in Q,\ \varphi(v) = \xi_L(g)v\} = U \cap \operatorname{Ker}(\vartheta_n + 1)$$

have dimension 1.

3) For any odd n, Lemma 3 of [CoT] now implies that both of the subspaces

$$F = \{v \in V \mid \forall\, \varphi \in Q,\ \varphi(v) = v\},$$
$$F^- = \{v \in V \mid \forall\, \varphi \in Q,\ \varphi(v) = \xi_L(g)v\}$$

also have dimension 1 (over $\mathbb{Q}$). Since $V = \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$, we arrive at the conclusion that $\Lambda(L)$ and $\Lambda^-(L)$ are 1-dimensional $\mathbb{Z}$-modules. □

Keeping Proposition 3.1 in mind, we denote by $v(L)$ (resp. $u(L)$) a generating element of the $\mathbb{Z}$-module $\Lambda(L)$ (resp. $\Lambda^-(L)$) for Lagrangian L. Then $v(L)$ (resp. $u(L)$) is determined uniquely up to sign. It is clear that $\Lambda(L)$ and $\Lambda^-(L)$ are stabilized by $G(L)$. Namely,

$$\varphi(v(L)) = \left(\frac{\det(\varphi|_L)}{p}\right) \cdot v(L),\ \varphi(u(L)) = \left(\frac{\det(\varphi|_{W/L})}{p}\right) \cdot u(L) \tag{6}$$

for $\varphi \in G(L)$. Since we consider Lagrangians oriented, we can set $v(-L) = -v(L)$, $u(-L) = -u(L)$ for the opposite Lagrangian $-L$ corresponding to a given oriented Lagrangian L. We fix an oriented Lagrangian L_0 with a basis $(e_1, \ldots, e_n)$, and fix a generating vector $v(L_0)$ of $\Lambda(L_0)$ (resp. $u(L_0)$ of $\Lambda^-(L_0)$). For an arbitrary oriented Lagrangian M with a basis $(f_1, \ldots, f_n)$, we find an element $\nu_M \in G$ such that $\nu_M(e_i) = f_i$ for all i, and set $v(M) = \nu_M(v(L_0))$, $u(M) = \nu_M(u(L_0))$. This definition is independent of the choice of ν_M. Moreover, for any $h \in G$ with

$h(L_0) = M$, we have

$$h(v(L_0)) = \left(\frac{\det((\nu_M^{-1}h)|_{L_0})}{p}\right) \cdot v(M),\ h(u(L_0)) = \left(\frac{\det((\nu_M^{-1}h)|_{W/L_0})}{p}\right) \cdot u(M).$$

Lemma 3.2. *Let L and M be arbitrary Lagrangians. Then $|(v(L), v(M))|$ (resp. $|(u(L), u(M))|$, $|(u(L), v(M))|$) depends only on the dimension of $L \cap M$ (and on the choice of the norm $(v(L), v(L))$). In other words, there exist non-negative constants a_k, b_k, c_k, $k = 0, 1, \ldots, n$, such that $|(v(L), v(M))| = a_k$, $|(u(L), u(M))| = b_k$, $|(u(L), v(M))| = c_k$ whenever* $\dim(L \cap M) = k$.

Proof. Consider Lagrangians L', M' with $\dim(L \cap M) = \dim(L' \cap M')$. It is clear that there exists an element $\varphi \in S$ mapping L into L' and M into M'. One readily verifies that $\varphi S(L) \varphi^{-1} = S(L')$. Taking $g \in S(L)$ and applying (6) we have

$$g\varphi^{-1}(v(L')) = \varphi^{-1} \cdot \varphi g \varphi^{-1}(v(L')) = \varphi^{-1}(v(L'))$$

for each $g \in S(L)$. By Proposition 3.1 this implies that $\varphi^{-1}(v(L')) = \pm v(L)$, i.e. $\varphi(v(L)) = \pm v(L')$. Similarly, $\varphi(v(M)) = \pm v(M')$. In particular, $(v(L'), v(M')) = \pm(v(L), v(M))$. Next we have $\xi_L(g) = \xi_{L'}(\varphi g \varphi^{-1})$, and

$$g\varphi^{-1}(u(L')) = \varphi^{-1} \cdot \varphi g \varphi^{-1}(u(L')) = \varphi^{-1}(\xi_{L'}(\varphi g \varphi^{-1}) u(L')) = \xi_L(g)\varphi^{-1}(u(L')).$$

By Proposition 3.1 this implies that $\varphi^{-1}(u(L')) = \pm u(L)$, i.e. $\varphi(u(L)) = \pm u(L')$. Similarly, $\varphi(u(M)) = \pm u(M')$. Hence,

$$(u(L'), u(M')) = \pm(u(L), u(M)),\ (u(L'), v(M')) = \pm(u(L), v(M)). \qquad \square$$

Lemma 3.3. *If k is even, then $a_k = 0$. If k is odd, then $c_k = 0$.*

Proof. Again consider the symplectic basis $(e_1, \ldots, e_n, f_1, \ldots, f_n)$. If the intersection of given Lagrangians L, L' has dimension k, k a non-negative integer, then without loss of generality one can suppose that

$$L = \langle e_1, \ldots, e_n \rangle_{\mathbb{F}_p},\ L' = \langle e_1, \ldots, e_k, f_{k+1}, \ldots, f_n \rangle_{\mathbb{F}_p}.$$

Clearly that ϑ_n is contained in both of $G(L)$, $G(L')$. Furthermore, $\det(\vartheta_n|_L) = 1$, $\det(\vartheta_n|_{W/L}) = \theta^n$, and $\det(\vartheta_n|_{L'}) = \theta^{n-k}$.

First suppose that k is even. Due to (6) one then has $\vartheta_n(v(L)) = v(L)$, $\vartheta_n(v(L')) = -v(L')$. Therefore,

$$(v(L), v(L')) = (\vartheta_n(v(L)), \vartheta_n(v(L'))) = -(v(L), v(L')),$$

i.e. $(v(L), v(L')) = 0$.

Next suppose that k is odd. Then due to (6) one has $\vartheta_n(u(L)) = -u(L)$, $\vartheta_n(v(L')) = v(L')$. Now we get

$$(u(L), v(L')) = (\vartheta_n(u(L)), \vartheta_n(v(L'))) = -(u(L), v(L')),$$

i.e. $(u(L), v(L')) = 0$. $\square$

Our next goal is to determine a_k for k odd, and c_k for k even. Recall that a *symplectic spread* of W is a collection $\pi = \{W_i \mid 1 \leq i \leq p^n + 1\}$ consisting of $p^n + 1$ maximal totally isotropic subspaces such that $\bigcup_{i=1}^{p^n+1} W_i = W$. The so-called *standard*, or *desarguesian*, symplectic spread of W can be constructed in the following way. Identify W with $\mathbb{F}_q^2$, $q = p^n$, and endow W with the symplectic form $\langle u,v\rangle = \mathrm{tr}(\alpha\delta-\beta\gamma)$, where $u=(\alpha,\beta)$, $v=(\gamma,\delta)$, $\alpha,\beta,\gamma,\delta\in\mathbb{F}_q$, and tr stands for the trace form $\mathrm{tr}:\mathbb{F}_q\to\mathbb{F}_p$. Then

$$\pi_D=\left\{W^\lambda \mid \lambda\in\mathbb{F}_q\cup\{\infty\}\right\},$$

where $W^\infty=\{(0,\alpha)\mid\alpha\in\mathbb{F}_q\}$, $W^\lambda=\{(\alpha,\lambda\alpha)\mid\alpha\in\mathbb{F}_q\}$ for $\lambda\in\mathbb{F}_q$ is the desired spread. One may suppose that

$$W^0=\langle e_1,\dots,e_n\rangle_{\mathbb{F}_p},\ W^\infty=\langle f_1,\dots,f_n\rangle_{\mathbb{F}_p}.$$

For a given symplectic spread $\pi=\{W_i\}$, its *automorphism group* $\mathrm{Aut}\,(\pi)$ is defined as the group $\{\varphi\in CSp_{2n}(p)\mid \forall i\,\exists j \text{ s.t. } \varphi(W_i)=W_j\}$. For example (see [KoT], Lemma 1.2.6),

$$\mathrm{Aut}\,(\pi_D)=SL_2(q)\cdot C_n\cdot C_{p-1},$$

the extension of $SL_2(q)$ first by the Galois group of the extension $\mathbb{F}_q/\mathbb{F}_p$ and then by the element ϑ_n. Set

$$\Lambda(\pi)=\langle v(L)\mid L\in\pi\rangle_{\mathbb{Z}}.$$

Then, by Lemma 3.3, $\Lambda(\pi)$ is a sublattice of Λ of determinant $(a_n)^{p^n+1}$, where $a_n=(v(L),v(L))$ as in Lemma 3.2. In particular,

$$\det V=\mathbb{Q}^{\bullet 2}, \tag{7}$$

the fact we used in the proof of Theorem 1.1. Also, it shows that V contains no p-modular lattices (if $p^n\equiv 1 \bmod 4$).

Now we consider the standard symplectic spread π_D, and project $v(M)$ and $u(M)$, M a fixed Lagrangian, to the orthogonal basis $(v(W^\lambda))$:

$$v(M)=\sum_{\lambda\in\mathbb{F}_q\cup\{\infty\}} z_\lambda v(W^\lambda),\ u(M)=\sum_{\lambda\in\mathbb{F}_q\cup\{\infty\}} y_\lambda v(W^\lambda).$$

It is obvious that $z_\lambda=a_n^{-1}(v(M),v(W^\lambda))$, $y_\lambda=a_n^{-1}(u(M),v(W^\lambda))$, and so

$$\sum_{\lambda\in\mathbb{F}_q\cup\{\infty\}}(v(M),v(W^\lambda))^2=a_n^2,\quad \sum_{\lambda\in\mathbb{F}_q\cup\{\infty\}}(u(M),v(W^\lambda))^2=a_nb_n. \tag{8}$$

Proposition 3.4. *In the notation of Lemma 3.2 one has*

(i) $a_k=p^{-(n-k)/2}\cdot a_n$ *for odd* k, $1\le k\le n$;

(ii) $(c_k)^2=p^{k-n}\cdot a_nb_n$ *for even* k, $0\le k<n$.

Proof. We shall proceed by induction on $n=1,3,\dots$.

1) Applying (8) to $M=W^\infty$ we get $a_nb_n=p^n(c_0)^2$. Next we take $M=\langle e_1,f_2,\dots,f_n\rangle_{\mathbb{F}_p}$ and write $e_1=(e,0)$ for $e\in\mathbb{F}_q^\bullet$. Then $M\cap W^\infty=\langle f_2,\dots,f_n\rangle$ has dimension $n-1$. Furthermore, for an arbitrary $\lambda\in\mathbb{F}_q$ one has

$$\begin{aligned} M\cap W^\lambda &=\{(xe,\lambda xe)\mid x\in\mathbb{F}_p,\langle(0,\lambda e),e_1\rangle=0\}\\ &=\left\{(xe,\lambda xe)\mid x\in\mathbb{F}_p,\mathrm{tr}(\lambda e^2)=0\right\}.\end{aligned}$$

Therefore, $\dim(M\cap W^\lambda)$ is equal to 1 for just p^{n-1} values of $\lambda\in\mathbb{F}_q$, and 0 for the other λ's. Applying (8), one has $p^{n-1}a_1^2=a_n^2$, i.e. $a_1=p^{-(n-1)/2}a_n$. Thus we have proved Proposition 3.4 for a_1 and c_0 with $n\ge 1$. In particular, the induction base $n=1$ has been established.

2) For the induction step we suppose $n\ge 3$. We already proved the desired relations for a_1 and c_0. Put

$$W'=\langle e_1,\dots,e_{n-2},f_1,\dots,f_{n-2}\rangle_{\mathbb{F}_p},\ W''=\langle e_{n-1},e_n,f_{n-1},f_n\rangle_{\mathbb{F}_p},$$

$U = \langle e_{n-1}, e_n \rangle_{\mathbb{F}_p}$, and introduce the following subgroups in S: $B = St_S(W')$, $S' = \{\varphi \in B \mid \varphi|_{W''} = 1_{W''}\}$, $S'' = \{\varphi \in B \mid \varphi|_{W'} = 1_{W'}\}$, $C = S'' \cap St_S(U)$, $K = S' \times C$. Then $S' \simeq Sp(W') = Sp_{2n-4}(p)$, $S'' \simeq Sp(W'') = Sp_4(p)$, $C \simeq (C_p)^3 \cdot GL_2(p)$, $B = S' \times S''$. We also set $G' = \langle S', \vartheta_n \rangle$, $H = \langle K, \vartheta_n \rangle = G' \cdot C$. It is well known that $\psi|_B = \psi' \otimes \psi'' + \tau' \otimes \tau''$, where ψ' (resp. τ') is an irreducible Weil character of S' of degree $(p^{n-2}+1)/2$ (resp. $(p^{n-2}-1)/2$). Furthermore, ψ'' (resp. τ'') is an irreducible Weil character of S'' of degree $(p^2+1)/2$ (resp. $(p^2-1)/2$). Arguing as in the proof of Proposition 3.1, we are convinced that $\alpha := \tau''|_C \in \mathrm{Irr}(C)$, and $\psi''|_C = \delta + \beta$, where $\beta \in \mathrm{Irr}(C)$ and $\delta(\varphi) = \left(\frac{\det(\varphi|_U)}{p}\right)$ for $\varphi \in C$. (In particular, $\delta(1) = 1$.) Thus

$$\psi|_K = \psi' \otimes \delta + \psi' \otimes \beta + \tau' \otimes \alpha$$

is a sum of three (pairwise distinct) irreducible constituents. From this it follows that

$$\chi|_K = (\psi' + \overline{\psi'}) \otimes \delta + (\psi' \otimes \beta + \overline{\psi'} \otimes \overline{\beta}) + (\tau' \otimes \alpha + \overline{\tau'} \otimes \overline{\alpha}).$$

Observe that ϑ_n acts on S' as an outer automorphism, and ϑ_n interchanges the characters ψ' and $\overline{\psi'}$. Furthermore, $C \lhd H$. Consequently, *$\chi|_H$ has a unique irreducible constituent in which C acts by scalars.* This constituent affords K-character $(\psi' + \overline{\psi'}) \otimes \delta$. Also,

$$(\chi|_C, \delta)_C = p^{n-2} + 1. \tag{9}$$

3) Next we consider the following $\mathbb{Z}$-submodule:

$$\Lambda' = \langle v(L) \mid L = L' \oplus U, L' \text{ Lagrangian in } W' \rangle_{\mathbb{Z}}$$

in Λ. (The symplectic form on W' is inherited from the one on W.) Clearly, H leaves Λ' fixed. Moreover, let $L = L' \oplus U$, L' a Lagrangian in W' and $\varphi \in C$. Then $\varphi(L) = L$. Hence, due to (6) the subgroup C acts on Λ' as scalars (and the corresponding character is $\dim_{\mathbb{Z}} \Lambda' \cdot \delta$). By the result of 2), $\dim_{\mathbb{Z}} \Lambda' = p^{n-2}+1$. Recall that we chose G' to be generated by $S' = Sp(W')$ and ϑ_n. Considering the natural action of G' on W', we conclude that $G' \simeq CSp(W')$. We want to find the kernel of G' acting on Λ'. To this end, consider a generating element $z = \theta E_{2n-4}$ of the center C_{p-1} of $CSp(W')$. Then z acting on W has the following matrix: $\mathrm{diag}(\theta E_{2n-4}, E_2, \theta^2 E_2)$ in the basis $(e_1, \ldots, e_{n-2}, f_1, \ldots, f_{n-2}, e_{n-1}, e_n, f_{n-1}, f_n)$. If $L = L' \oplus U$ (L' any Lagrangian in W'), then due to (6) $z(v(L)) = -v(L)$, as n is odd. Thus z acts on Λ' as multiplication by -1. We have shown that the lattice Λ' is in fact acted on by $CSp_{2n-4}(p)/C_{(p-1)/2} = G^-_{n-2}$, and this action affords S'-character $\psi' + \overline{\psi'}$. If we denote $G'(L') = St_{G'}(L')$, and define $S'(L')$ similarly to (5), then of course $G'(L') = G(L) \cap G'$, $S'(L') = S(L) \cap G'$ for $L = L' \oplus U$. In other words, W', Λ', L', $v'(L')$ and $u'(L')$ (generating vectors of $\Lambda'(L')$ and $\Lambda'^-(L')$, cf. Proposition 3.1) play the same roles for G' as W, Λ, L, $v(L)$ and $u(L)$ do for G.

Observe that there are nonzero rational scalars s and t such that $v'(L') = \pm s v(L)$, $u'(L') = \pm t u(L)$. Indeed, $v(L) \in \Lambda'$ by the definition of Λ', and $v(L)$ is obviously fixed by $S'(L')$; hence $v(L) \in \Lambda'(L')$, and $v'(L') = \pm s v(L)$ for some $s \in \mathbb{Q}^\bullet$. Next, $\langle u(L) \rangle_{\mathbb{Z}}$ is a C-module with character δ (cf. (6)). On the other hand, Λ' affords C-character $(p^{n-2}+1)\delta$. Hence by (9) we have $u(L) \in \Lambda' \otimes_{\mathbb{Z}} \mathbb{C}$. From this it follows that $u(L) \in \Lambda'^-(L') \otimes_{\mathbb{Z}} \mathbb{C}$, i.e. $u'(L') = \pm t u(L)$ for a certain $t \in \mathbb{C}^\bullet$. Observe that

$$st = \pm (u'(L'), v'(M'))/(u(L), v(M))$$

is a rational number, where L', M' are Lagrangians inside W' with $\dim(L' \cap M') = n-3$. Hence t is rational. We may suppose that $s, t > 0$.

Now we can apply the induction hypothesis to G' and Λ'. In doing so we consider two arbitrary Lagrangians L', M' of W' with $\dim(L' \cap M') = k$. Then for $L = L' \oplus U$, $M = M' \oplus U$ one has $\dim(L \cap M) = k + 2$, which implies that $a'_k = |(v'(L'), v'(M'))| = s^2|(v(L), v(M))| = s^2 a_{k+2}$, $b'_k = |(u'(L'), u'(M'))| = t^2|(u(L), u(M))| = t^2 b_{k+2}$, $c'_k = |(u'(L'), v'(M'))| = st|(u(L), u(M))| = stc_{k+2}$. By the induction hypothesis, for k odd we have

$$s^2 a_{k+2} = a'_k = p^{(n-2-k)/2} a'_{n-2} = s^2 p^{(n-(k+2))/2} a_n,$$

i.e. $a_{k+2} = p^{(n-(k+2))/2} a_n$. Thus we have proved the desired relation for a_l with $l = 3, 5, \ldots, n$. Similarly, if k is even, then

$$s^2 t^2 (c_{k+2})^2 = (c'_k)^2 = p^{k-n+2} a'_{n-2} b'_{n-2} = s^2 t^2 p^{k-n+2} a_n b_n,$$

i.e. $(c_{k+2})^2 = p^{k+2-n} a_n b_n$. Thus we have proved the desired relation for c_l with $l = 2, 4, \ldots, n-1$. The induction step is over. □

Corollary 3.5. *Rescale the $v(L)$'s such that $(v(L), v(L)) = p^{(n-1)/2}$. Then*

$$(v(L), v(M)) = \begin{cases} \pm p^{(k-1)/2}, & \dim(L \cap M) = k \equiv 1 \bmod 2, \\ 0, & \dim(L \cap M) \equiv 0 \bmod 2. \end{cases} \quad \square$$

The signs $\pm$ involved in this corollary will be determined in §5, cf. Corollary 5.4.

Now we consider the endomorphism σ of V (constructed in Proposition 2.4 for $p \equiv 1 \bmod 4$ and in [SchT], §5 for $p \equiv 3 \bmod 4$. Recall that Λ is a G-invariant lattice in V. Let Γ be the sublattice of Λ generated by $v(L)$ with L running over all Lagrangians in W. Clearly, one can rescale the scalar product on V such that $\nabla = \Gamma + \sigma(\Gamma)$ is an integral G-invariant σ-stable lattice lying in V. Also, $\Gamma(L) = \Lambda(L)$ for any Lagrangian L. We can now apply Propositions 3.1, 3.4 and Lemmas 3.2, 3.3 to the lattice ∇. Let $\widetilde{v}(L)$, $\widetilde{u}(L)$ be generating vectors of $\nabla(L)$, $\nabla^-(L)$.

Lemma 3.6. *For the lattice $\nabla = \Gamma + \sigma(\Gamma)$ we have $\widetilde{v}(L) = \pm v(L)$ and $\widetilde{u}(L) = \pm\sigma(v(L))$. In particular, the parameters a_k, b_k, c_k of ∇ satisfy the following relations:*

(i) *$b_k = pa_k$ for any k;*
(ii) *$c_k = p^{(k+1-n)/2} \cdot a_n$ for any even k.*

Proof. Since $\Gamma \subseteq \nabla$, $v(L) = m\widetilde{v}(L)$ for some integer m. As Γ is generated by the $v(L)$'s, $\Gamma \subseteq m\nabla$, and so $\nabla = \Gamma + \sigma(\Gamma) \subseteq m(\nabla + \sigma(\nabla)) = m\nabla$, yielding $m = \pm 1$, i.e. $\widetilde{v}(L) = \pm v(L)$.

Recall that $g\sigma = \left(\frac{\det(g|_W)}{p}\right)\sigma g$ for any $g \in G$. If $g \in G(L)$, then $\det(g|_W) = \det(g|_L) \cdot \det(g|_{W/L})$, and so $\left(\frac{\det(g|_W)}{p}\right) = \left(\frac{\det(g|_L)}{p}\right) \cdot \xi_L(g)$. Therefore, by (6) one has

$$\begin{aligned} g\sigma(v(L)) &= \left(\frac{\det(g|_W)}{p}\right)\sigma g(v(L)) \\ &= \left(\frac{\det(g|_W)}{p}\right) \cdot \left(\frac{\det(g|_L)}{p}\right)\sigma(v(L)) = \xi_L(g)\sigma(v(L)). \end{aligned}$$

This means: $\sigma(v(L)) \in \nabla^-(L)$; hence $\sigma(v(L)) = k \cdot \widetilde{u}(L)$ for some $k \in \mathbb{Z}$. Similarly,

$$\begin{aligned} g\sigma(\widetilde{u}(L)) &= \left(\frac{\det(g|_W)}{p}\right)\sigma g(\widetilde{u}(L)) \\ &= \left(\frac{\det(g|_W)}{p}\right) \cdot \xi_L(g)\sigma(\widetilde{u}(L)) = \left(\frac{\det(g|_L)}{p}\right)\sigma(\widetilde{u}(L)), \end{aligned}$$

which implies that $\sigma(\widetilde{u}(L)) \in \nabla(L)$. From this it follows that $\sigma(\widetilde{u}(L)) = l \cdot v(L)$ for some $l \in \mathbb{Z}$. In this case we have

$$\epsilon p \cdot v(L) = \sigma^2(v(L)) = \sigma(k \cdot \widetilde{u}(L)) = k\sigma(\widetilde{u}(L)) = kl \cdot v(L),$$

i.e. $kl = \pm p$. Assume $k \neq \pm 1$. Then $k = \pm p$, $l = \pm 1$, and $v(L) = \pm\sigma(\widetilde{u}(L))$ belongs to $\sigma(\nabla)$. Since ∇ is generated by the vectors $v(L)$ and the sublattice $\sigma(\Gamma)$ which is contained in $\sigma(\nabla)$, we conclude that $\nabla \subseteq \sigma(\nabla)$. Applying σ once more again, we get $\nabla \subseteq \sigma^2(\nabla) = p\nabla$, a contradiction. Hence $k = \pm 1$, i.e. $\widetilde{u}(L) = \pm\sigma(v(L))$.

Next we take L, M such that $\dim(L \cap M) = k$. Then

$$b_k = |(\widetilde{u}(L), \widetilde{u}(M))| = |(\sigma(v(L)), \sigma(v(M)))| = p|(v(L), v(M))| = pa_k.$$

Furthermore, by Proposition 3.4 for even k one has

$$(c_k)^2 = p^{k-n} a_n b_n = p^{k+1-n}(a_n)^2,$$

i.e. $c_k = p^{(k+1-n)/2} \cdot a_n$. □

Remark 3.7. The assumption $\Gamma = \langle v(L) \mid L \text{ any Lagrangian}\rangle$ is essential for the conclusions of Lemma 3.6. For example, the parameters a_k, b_k of the lattice $\sigma(\nabla)$ satisfy $a_k = pb_k$.

A key ingredient in our further arguments is the following observation:

Proposition 3.8. *Let $(e_1, \dots, e_n, f_1, \dots, f_n)$ be any arbitrary symplectic basis of W, and let M, L^λ, $\lambda \in \mathbb{F}_p$, be Lagrangians with bases $(f_1, \dots, f_n)$, $(e_1 + \lambda f_1, f_2, \dots, f_n)$, respectively. Then in the notation of Lemma 3.6 one has*

$$\widetilde{u}(M) = \sum_{\lambda \in \mathbb{F}_p} d_\lambda v(L^\lambda),\ pv(M) = \sum_{\lambda \in \mathbb{F}_p} d'_\lambda \widetilde{u}(L^\lambda)$$

with $d_\lambda, d'_\lambda = \pm 1$.

Proof. Observe that $\dim(M \cap L^\lambda) = n - 1$. Hence in accordance with Lemma 3.6 we have $(\widetilde{u}(M), v(L^\lambda)) = d_\lambda a_n$ with $d_\lambda = \pm 1$. Besides, $(\widetilde{u}(M), \widetilde{u}(M)) = pa_n$ and $(v(L^\lambda), v(L^{\lambda'})) = a_n \delta_{\lambda,\lambda'}$. Hence, for $v = \widetilde{u}(M) - \sum_{\lambda \in \mathbb{F}_p} d_\lambda v(L^\lambda)$ we have $(v, v) = 2pa_n - 2pa_n = 0$, yielding $\widetilde{u}(M) = \sum_{\lambda \in \mathbb{F}_p} d_\lambda v(L^\lambda)$. Applying σ to this identity, we obtain $pv(M) = \sum_{\lambda \in \mathbb{F}_p} d'_\lambda \widetilde{u}(L^\lambda)$. □

Now we are in a position to explicitly exhibit a G-invariant odd unimodular lattice in V.

Theorem 3.9. *Let p be any odd prime and n any odd integer. For every Lagrangian L in W, choose a vector $v(L)$ in $V \otimes_{\mathbb{Q}} \mathbb{R}$ fixed by $S(L)$ and such that $(v(L), v(L)) = p^{(n-1)/2}$. Then the lattice $\Delta = \Delta(p, n)$ generated by all $v(L)$'s*

$$\Delta = \langle v(L) \mid L \in \mathcal{L}(W)\rangle_{\mathbb{Z}}$$

is a σ-stable G_n^--invariant odd unimodular lattice.

Proof. We start with some G-invariant integral lattice Λ and choose $v'(L)$ to be a generating vector of the $\mathbb{Z}$-module $\Lambda(L)$, L any Lagrangian. Then according to Lemma 3.3 and Proposition 3.4, $(v'(L), v'(M)) = 0$ if $k = \dim(L \cap M)$ is even, and $(v'(L), v'(M)) = \pm p^{(k-1)/2} a_1$ if k is odd. Here a_1 is some natural integer. Now we set $v(L) = a_1^{-1/2} v'(L)$ for all Lagrangians L. Clearly, $v(L) \in V \otimes_{\mathbb{Q}} \mathbb{R}$, $(v(L), v(L)) = p^{(n-1)/2}$ and $v(L)$ is $S(L)$-stable. (We could assume $v(L) \in V$ by means of rescaling the scalar product on V by the scalar a_1^{-1}.) Furthermore,

$(v(L), v(M)) \in \mathbb{Z}$ for any L, M. We see that Δ as defined in the theorem is a G-invariant *integral* lattice. Moreover, if π_D denotes the standard symplectic spread, then Δ contains the sublattice

$$\Delta(\pi_D) = \langle v(L) \mid L \in \pi_D \rangle_{\mathbb{Z}}$$

of determinant $p^{(n-1)(p^n+1)/2}$. In particular, $\det \Delta$ is a power of p: $\det \Delta = p^m$ for some non-negative integer m.

If $m = 0$, we are done. Suppose that $m \geq 1$. Then consider the form $(\bar{x}, \bar{y})_p = (x, y) \bmod p$ on $\Delta/p\Delta$, where $\bar{x} = x + p\Delta$, $\bar{y} = y + p\Delta$. As p divides $\det \Delta$, $(\cdot,\cdot)_p$ is degenerate on $\Delta/p\Delta$. This means that $p\Delta$ is a proper sublattice of $\Delta \cap p\Delta^{\#}$. If $\Delta \cap p\Delta^{\#} = \Delta$, then $\Delta \subseteq p\Delta^{\#}$; in particular, $(v(L), v(M)) \in p\mathbb{Z}$ for all L, M, contrary to the equality $(v(L), v(M)) = \pm 1$ for $\dim(L \cap M) = 1$. Therefore, $\Delta \supset \Delta \cap p\Delta^{\#} \supset p\Delta$. One may then suppose that $\Delta/(\Delta \cap p\Delta^{\#})$ affords the G-character η_1 mentioned in Proposition 2.2 (iii). Since $\Delta/(\Delta \cap p\Delta^{\#})$ supports the G-invariant non-degenerate symmetric bilinear form $(\cdot,\cdot)_p$, η_1 is of quadratic type, contrary to Proposition 2.2 (iii).

2) By Lemma 3.6 and Proposition 3.8, $\sigma(v(L))$ belongs to Δ for any L. Hence Δ is σ-stable. □

Corollary 3.10. *For the lattice $\Delta = \Delta(p, n)$ and generating vectors $v(L)$, $u(L)$ of $\Delta(L)$, $\Delta^-(L)$, we have $u(L) = \pm\sigma(v(L))$. In particular, the parameters a_k, b_k, c_k of Δ satisfy the following relations:*

(i) *$b_k = pa_k$ for any k;*

(ii) *$c_k = p^{(k+1-n)/2} \cdot a_n$ for any even k.* □

4. Explicit construction. II: n is even

Let p be an odd prime and n any even integer. In this section we exploit the results of §3 to describe an explicit construction of G_n^+-invariant p-modular lattices in $V = V_n$. Setting $S' = S_{n+1} = Sp_{2n+2}(p)$, we consider a natural $\mathbb{F}_pS'$-module $W' = W_{n+1} = \mathbb{F}_p^{2n+2}$ endowed with a non-degenerate symplectic form $\langle\cdot,\cdot\rangle$. Fix some symplectic basis $(e_1, \ldots, e_{n+1}, f_1, \ldots, f_{n+1})$ of W'. Consider the endomorphism ϑ_{n+1} of W' with the matrix $\mathrm{diag}(E_{n+1}, \theta E_{n+1})$, and set $G' = G_{n+1} = \langle S', \vartheta_n' \rangle \simeq CSp_{2n+2}(p)$. Now we can embed W into W', $S = S_n$ into S', $G = G_n$ into G' by means of setting $W = \langle e_1, \ldots, e_n, f_1, \ldots, f_n \rangle_{\mathbb{F}_p}$, $S = St_{S'}(e_{n+1}, f_{n+1})$, $G = \langle S, \vartheta_{n+1} \rangle$. Clearly, $G \simeq CSp_{2n}(p)$, and one can identify ϑ_{n+1} with ϑ_n. Choose an irreducible Weil character ψ' of S' of degree $(p^{n+1}+1)/2$ such that $(\psi'|_S, \psi)_S > 0$. Let χ' be the rational irreducible character of G' of degree $p^{n+1}+1$ and with kernel $C_{(p-1)/2}$, and let $V' = V_{n+1}$ be an irreducible $\mathbb{Q}G'$-module with character χ' (cf. Proposition 2.3). Thus V' is a faithful G_{n+1}^--module.

We collect several facts from [SchT] and §3. For any Lagrangian L' in W' set

$$G'(L') = \{\varphi \in G' \mid \varphi(L') = L'\}, \ S'(L') = \left\{\varphi \in G'(L') \mid \det(\varphi|_{L'}) \in \mathbb{F}_p^{\bullet 2}\right\}.$$

The subspace $\{v \in V' \mid \forall \varphi \in S'(L'), \varphi(v) = v\}$ has dimension 1. Therefore, one can choose an $S'(L')$-stable vector $v(L')$ such that $(v(L'), v(L')) = p^{n/2}$. Then the lattice

$$\Delta' = \Delta(p, n+1) = \langle v(L') \mid L' \in \mathcal{L}(W') \rangle_{\mathbb{Z}}$$

is an odd unimodular G'-invariant lattice in V'. Moreover, Δ' has a $\mathbb{Z}$-linear endomorphism σ with the following properties:

(a) σ commutes with S', and $\sigma\vartheta_{n+1} = -\vartheta_{n+1}\sigma$;

(b) $\sigma^2(v) = \epsilon pv$, $(\sigma(u), v) = \epsilon(u, \sigma(v))$, $(\sigma(u), \sigma(v)) = p(u, v)$ for any $u, v \in V'$, where $\epsilon = (-1)^{(p-1)/2}$.

Let L', M' are any Lagrangians in W', and set $u(L') = \sigma(v(L'))$. If $k = \dim_{\mathbb{F}_p}(L' \cap M')$ is odd, then $a_k = |(v(L'), v(M'))| = p^{(k-1)/2}$, $b_k = |(u(L'), u(M'))| = p^{(k+1)/2}$, $c_k = |(u(L'), v(M'))| = 0$. If k is even, then $a_k = b_k = 0$, and $c_k = p^{k/2}$.

The descent from G^-_{n+1} to G^+_n is provided by the following statement. Denote $U = \langle e_{n+1} \rangle_{\mathbb{F}_p}$, $W'' = \langle e_{n+1}, f_{n+1} \rangle_{\mathbb{F}_p}$.

Proposition 4.1. *The subspace $V = \langle v(L') \mid L' = L \oplus U, L \in \mathcal{L}(W) \rangle_{\mathbb{Q}}$ of V' is a faithful absolutely irreducible $\mathbb{Q}G^+_n$-module of dimension $p^n + 1$. Moreover, V is σ-stable.*

Proof. 1) We introduce the following subgroups in S': $B = St_{S'}(W)$, $S'' = \{\varphi \in B \mid \varphi_W = 1_W\}$, $C = S'' \cap St_{S'}(U)$, $K = S \times C$. Then $S'' \simeq Sp(W'') = Sp_2(p)$, $C \simeq C_p \cdot GL_1(p)$, $B = S \times S''$. By our definition, $G = \langle S, \vartheta_{n+1} \rangle$. We also set $H = \langle K, \vartheta_{n+1} \rangle = G \cdot C$. It is well known that $\psi'|_B = \psi \otimes \psi'' + \tau \otimes \tau''$, where ψ'' (resp. τ'') is an irreducible Weil character of S'' of degree $(p+1)/2$ (resp. $(p-1)/2$). Furthermore, τ is an irreducible Weil character of S of degree $(p^n - 1)/2$ (ψ_1 in the notation of §1). It is easy to check that $\alpha := \tau''|_C \in \mathrm{Irr}(C)$, and $\psi''|_C = \delta + \beta$, where $\beta \in \mathrm{Irr}(C)$ and $\delta(\varphi) = \left(\frac{\det(\varphi|_U)}{p}\right)$ for $\varphi \in C$. (In particular, $\delta(1) = 1$.) Observe that $\beta \neq \delta$. It is so if $p > 3$, since in this case $\beta(1) = (p-1)/2 > 1$. If $p = 3$, then $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{-3}) \neq \mathbb{Q} = \mathbb{Q}(\delta)$. Thus

$$\psi'|_K = \psi \otimes \delta + \psi \otimes \beta + \tau \otimes \alpha$$

is a sum of three (pairwise distinct) irreducible constituents. From this it follows that

$$\chi|_K = (\psi + \overline{\psi}) \otimes \delta + (\psi \otimes \beta + \overline{\psi} \otimes \overline{\beta}) + (\tau \otimes \alpha + \overline{\tau} \otimes \overline{\alpha}).$$

Observe that ϑ_{n+1} acts on S as an outer automorphism, and ϑ_{n+1} interchanges the characters ψ and $\overline{\psi}$. Furthermore, $C \lhd H$. Consequently, $\chi|_H$ *has a unique irreducible constituent, say γ, in which C acts via a multiple of the character δ.* This constituent γ affords K-character $(\psi + \overline{\psi}) \otimes \delta$.

2) Next we observe that H leaves V fixed. Moreover, let $L' = L \oplus U$, let L be a Lagrangian in W and $\varphi \in C$. Then $\varphi(L) = L$. Hence, due to (6) the subgroup C acts on V as scalars (and the corresponding character is $\dim_{\mathbb{Q}} V \cdot \delta$). By the result of 1), $\dim_{\mathbb{Q}} V = p^n + 1$. Recall that we chose $G \simeq CSp(W)$ to be generated by $S = Sp(W)$ and ϑ_{n+1}. We want to find the kernel of G acting on V. For consider a generating element $z = \theta E_{2n}$ of the center C_{p-1} of $CSp(W)$. Then z acting on W' has the following matrix: $\mathrm{diag}(\theta E_{2n}, 1, \theta^2)$ in the basis $(e_1, \dots, e_n, f_1, \dots, f_n, e_{n+1}, f_{n+1})$. If $L' = L \oplus U$ (L any Lagrangian in W), then due to (6) $z(v(L')) = v(L')$, as n is even. Thus z acts trivially on V. We have shown that V is in fact acted on by $CSp_{2n}(p)/C_{p-1} = G^+_n$, and this action affords G^+_n-character χ^+ (cf. Proposition 2.3).

3) Finally, we show that $\sigma(V) = V$. Recall that the endomorphism σ centralizes S'. In particular, σ centralizes K. Hence, the subspace $\sigma(V)$ affords the same K-character as of V. Since $\vartheta_{n+1}(V) = V$ and $\vartheta_{n+1}\sigma = -\sigma\vartheta_{n+1}$, $\sigma(V)$ is ϑ_{n+1}-stable, that is, $\sigma(V)$ is an H-module. By the results of 1), $\sigma(V)$ also affords the H-character γ. As γ is irreducible and it enters $\chi'|_H$ with multiplicity 1, $\sigma(V) = V$. □

Now we are in a position to give some more explicit lattice constructions. We start with $(p^n + 1)/2$-dimensional lattices. Let $R = Sp_{2m}(q)$, where $q = p^{2f}$. Then

R has two irreducible Weil characters ϱ, ϱ^* of degree $(q^m+1)/2$. These characters are conjugate under some outer automorphism of R. Both of them are rational, as shown in [Gro]. We want to expose an explicit construction for $\mathbb{Z}R$-lattices of dimension $(q^m+1)/2$. To this end, put $n = mf$. Consider the natural $\mathbb{F}_qR$-module $W^{(f)} = \mathbb{F}_q^{2m}$ endowed with a non-degenerate $\mathbb{F}_q$-valued symplectic form $\langle\cdot,\cdot\rangle_{(f)}$. Then we can identify W with $W^{(f)}$ viewed as $\mathbb{F}_p$-space and assume that $\langle u,v\rangle = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\langle u,v\rangle_{(f)}$. This identification embeds $R = Sp(W^{(f)})$ canonically in $S_n = Sp(W)$. One may also suppose that $\varrho = \psi|_R$. Clearly, any Lagrangian in $W^{(f)}$ (that is, an m-dimensional $\mathbb{F}_q$-subspace in $W^{(f)}$ which is totally isotropic w.r.t. $\langle\cdot,\cdot\rangle_{(f)}$) is also a Lagrangian in W. We call these special Lagrangians *$\mathbb{F}_q$-Lagrangians in W*.

Theorem 4.2. *Keep the above notation. Set*

$$\Delta(q,m) = \langle v(L') \mid L' = L\oplus U,\ L \textit{ any } \mathbb{F}_q\textit{-Lagrangian in } W\rangle_{\mathbb{Z}}.$$

Then $\Delta(q,m)$ is an R-invariant integral lattice affording the Weil character ϱ.

Proof. In addition to $\Gamma := \Delta(q,m)$ we consider

$$\Gamma' = \langle u(L') \mid L' = L\oplus U,\ L \text{ an } \mathbb{F}_q\text{-Lagrangian in } W\rangle_{\mathbb{Z}}.$$

Clearly, Γ and Γ' are invariant under R. We have mentioned that the restriction $\psi|_R$ is equal to ϱ and so it is irreducible. Hence $\chi|_R = 2\varrho$. From this it follows that $\dim_{\mathbb{Z}}\Gamma$ and $\dim_{\mathbb{Z}}\Gamma'$ are at least $\varrho(1) = (p^n+1)/2$. Observe that $\Gamma\perp\Gamma'$. For, if L, M are $\mathbb{F}_q$-Lagrangians in W, then $\dim_{\mathbb{F}_p}(L\cap M) = 2f\cdot\dim_{\mathbb{F}_p}(L\cap M)$ is always even. This implies that $\dim_{\mathbb{F}_p}(L'\cap M')$ is odd, and so $(v(L'),u(M')) = 0$ by Lemma 3.3. By Proposition 4.1, Γ and Γ' are contained in the $\mathbb{Q}$-space V of dimension p^n+1, and the scalar product on V is positive definite. Hence we must have $\dim_{\mathbb{Z}}\Gamma = \varrho(1)$, and $\Gamma = \Delta(q,m)$ is an R-invariant integral lattice affording the Weil character ϱ. □

Corollary 4.3. *In the notation of Proposition 4.1,* $\det V = p\mathbb{Q}^{\bullet 2}$. *On the other hand, if* $p\equiv 1 \bmod 4$ *and V is considered as a G_n^--module by means of Proposition 2.4, then* $\det V = \mathbb{Q}^{\bullet 2}$.

Proof. The proof of Theorem 4.2 shows that V contains the lattice $\Gamma\oplus\sigma(\Gamma)$ of determinant $\det\Gamma\cdot\det\sigma(\Gamma) = p^{(p^n+1)/2}(\det\Gamma)^2 \in p\mathbb{Q}^{\bullet 2}$. The other claim follows from the oddness of $(p^n+1)/2$. □

Theorem 4.4. *Keep the above notation. Set*

$$\Delta = \Delta(p,n) = \langle v(L') \mid L' = L\oplus U,\ L\in\mathcal{L}(W)\rangle_{\mathbb{Z}}.$$

Then Δ is a G_n^+-invariant p-modular lattice.

Proof. Recall that the scalar product on V is inherited from the one on V', and the dual $\Delta^{\#}$ to Δ is taken under this scalar product. Clearly, Δ is fixed by G_n^+. Applying Proposition 3.8, we see that $u(L') = \sigma(v(L'))$ is contained in Δ for any L, and Δ is σ-stable.

1) First assume that $\det\Delta$ is divisible by some prime $r\neq 2,p$. Consider the form $(\bar{x},\bar{y})_r = (x,y) \bmod r$ on $\Delta/r\Delta$, where $\bar{x} = x + r\Delta$, $\bar{y} = y + r\Delta$. As r divides $\det\Delta$, this G-invariant symmetric bilinear form is degenerate, and so its kernel $(\Delta\cap r\Delta^{\#})/r\Delta$ is nonzero, i.e. $\Delta\supseteq\Delta\cap r\Delta^{\#}\supset r\Delta$. By Proposition 2.2 (i), this means $\Delta = \Delta\cap r\Delta^{\#}$. Hence $(u,v)\in r\mathbb{Z}$ for any $u,v\in\Delta$. In the meantime,

$(v(L'), v(M')) = \pm 1$ for $L' = L \oplus U$, $M' = M \oplus U$ with $\dim(L \cap M) = 0$, a contradiction.

2) At this point we show that $\det \Delta$ is odd. Suppose the contrary: 2 divides $\det \Delta$. Consider the form $(\bar{x}, \bar{y})_2 = (x, y) \bmod 2$ on $\Delta/2\Delta$, where $\bar{x} = x + 2\Delta$, $\bar{y} = y + 2\Delta$. As $2 | \det \Delta$, $\Delta' =: \Delta \cap 2\Delta^{\#}$ contains properly 2Δ. Since Δ is an odd lattice, its even part $\Delta^0 = \{v \in \Delta \mid (v, v) \in 2\mathbb{Z}\}$ is a sublattice of index 2 in Δ. Moreover, $\Delta^0 \supset \Delta'$. (For Δ' is clearly contained in Δ^0. On the other hand,

$$(v(L') + u(L'), v(L') + u(L')) \in 2\mathbb{Z},\ (v(L') + u(L'), v(L')) = p^{n/2} \notin 2\mathbb{Z},$$

i.e. $v(L') + u(L') \in \Delta^0 \setminus \Delta'$.) Applying Proposition 2.2 (ii), we see that $A \supset B \supset C \supset 0$ is a composition series for the $\mathbb{F}_2 G$-module $A = \Delta/2\Delta$, where $B = \Delta^0/2\Delta$, $C = \Delta'/2\Delta$.

We exhibit one more nonzero proper submodule inside B. Set $\Gamma = \langle v + \sigma(v) \mid v \in \Delta \rangle_{\mathbb{Z}} + 2\Delta$. Since $g\sigma = \pm \sigma g$ for all $g \in G$, Γ is G-stable. Furthermore,

$$(u + \sigma(u), v + \sigma(v)) = (p + 1)(u, v) + (1 + \epsilon)(u, \sigma(v)) \in 2\mathbb{Z}$$

due to the properties of the endomorphism σ. Thus $D = \Gamma/2\Delta$ is a G-submodule of B and D is totally isotropic w.r.t. $(\cdot, \cdot)_2$. Since $(v(L') + u(L'), v(L')) = p^{n/2}$, we see that $v(L') + u(L') \in \Gamma \setminus \Delta'$. From this it follows that $0 \neq D \neq C$. Since $B \supset C \supset 0$ is a composition series for B, we must have $B = C + D$. But $C = \mathrm{Ker}(\cdot, \cdot)_2$; hence we come to the conclusion that B is totally isotropic w.r.t. $(\cdot, \cdot)_2$. On the other hand, choosing

$$L_1 = \langle e_1, \ldots, e_n, e_{n+1} \rangle_{\mathbb{F}_p},\ L_2 = \langle f_1, \ldots, f_n, e_{n+1} \rangle_{\mathbb{F}_p},$$

$$L_3 = \langle e_1, \ldots, e_{n-2}, e_{n-1} + f_{n-1}, f_n, e_{n+1} \rangle_{\mathbb{F}_p},$$

we get $v(L_1) + v(L_2), v(L_1) + v(L_3) \in \Delta^0$ with

$$(v(L_1) + v(L_2), v(L_1) + v(L_3)) \equiv p^{n/2} + p^{(n-2)/2} + 1 + 0 \equiv 1 \bmod 2,$$

a contradiction.

3) Observe that $p\Delta^{\#} \supseteq \sigma(\Delta)$. (Indeed, Δ is generated by the vectors $v(L')$, and $\sigma(\Delta)$ is generated by the vectors $u(M')$, with $L' = L \oplus U$, $M' = M \oplus U$, L, M arbitrary Lagrangians in W. It is obvious that $k = \dim(L' \cap M') \geq 1$. But $|(v(L'), u(M'))| = c_k$ is 0 if k is odd, and $p^{k/2}$ if k is even. Hence c_k is divisible by p.) In fact we have

$$\Delta \cap p\Delta^{\#} = \sigma(\Delta). \tag{10}$$

For, assume the contrary. Then $\Delta \supseteq \Delta \cap p\Delta^{\#} \supset \sigma(\Delta) \supset p\Delta$. By Proposition 2.2 (iii) $\Delta/\sigma(\Delta)$ is an irreducible $\mathbb{F}_p G$-module. Hence $\Delta \cap p\Delta^{\#} = \Delta$, $\Delta \subseteq p\Delta^{\#}$. The last inclusion contradicts the equality $(v(L'), v(M')) = \pm 1$ for $\dim(L' \cap M') = 1$.

In addition to (10) we show that

$$\Delta \cap p^2\Delta^{\#} \subseteq p\Delta. \tag{11}$$

To this end we denote $\Lambda = \Delta \cap p\Delta^{\#}$. Then $\Lambda \cap p^2\Lambda^{\#}$ is a proper sublattice of Λ, because $u(L'), u(M') \in \Lambda$ and $(u(L'), u(M')) = \pm p$ provided that $\dim(L' \cap M') = 1$. Furthermore, $(\Delta \cap p\Delta^{\#}, p\Delta) \subseteq p^2\mathbb{Z}$. Thus we have

$$p\Delta \subseteq \Lambda \cap p^2\Lambda^{\#} \subset \Lambda = \sigma(\Delta).$$

Now the irreducibility of the $\mathbb{F}_pG$-module $\sigma(\Delta)/p\Delta$ implies that $p\Delta = \Lambda \cap p^2\Lambda^{\#}$. Keeping in mind that

$$\Lambda \cap p^2\Lambda^{\#} = (\Delta \cap p\Delta^{\#}) \cap (p\Delta + p^2\Delta^{\#}) \supseteq \Delta \cap p^2\Delta^{\#},$$

one obtains (11).

4) By the results of 1) and 2), $\det \Delta$ is not divisible by any prime r other than p. Hence $\det \Delta = p^m$ and so $\Delta \supseteq p^m\Delta^{\#}$ for some non-negative integer m. Choose the minimal non-negative integer ℓ such that $\Delta \supseteq p^\ell\Delta^{\#}$. If $\ell = 0$, then by (10) one has $\sigma(\Delta) = p\Delta$, a contradiction. Assume that $\ell \geq 2$. Then applying (11) we have

$$p^\ell\Delta^{\#} \subseteq \Delta \cap p^2\Delta^{\#} \subseteq p\Delta,$$

i.e. $p^{\ell-1}\Delta^{\#} \subseteq \Delta$, contrary to the choice of ℓ. Hence $\ell = 1$. In this case (10) yields $p\Delta^{\#} = \sigma(\Delta)$, $\Delta = \sigma(\Delta^{\#})$. In other words, Δ is p-modular. □

From now on, when considering $\Delta(p, n)$ with n even, we denote $v(L \oplus U)$ by $v(L)$ (L a Lagrangian in W) and then forget the initial descent $n + 1 \rightsquigarrow n$. In particular, $(v(L), v(M)) = \pm p^{k/2}$ if $k = \dim(L \cap M)$ is even, and 0 otherwise. The signs involved in this formula will be determined in the next section.

5. Maslov index and Gram matrix

Let k be any field of characteristic other than 2 and $S(k) = Sp_{2n}(k)$. If $k = \mathbb{C}$ or k is a finite field (and $(n, |k|) \neq (1, 9)$), then it is well known that $S(k)$ is simply connected. However, if k is $\mathbb{R}$ or any local field, then $S(k)$ is not simply connected, and $S(k)$ has a double covering group called the *metasymplectic group*. An important role in physics is played by a faithful complex representation of the metasymplectic group called the *Shale-Weil representation*. A key ingredient of constructing this representation is *Maslov index* (or *Maslov-Kashiwara index*), which is defined on triples of Lagrangians inside the symplectic space k^{2n}. For more detail the reader is referred to [LiV].

Remarkably, we can define a discrete analogue of Maslov index for $Sp_{2n}(p)$, which enables one to completely determine the Gram matrices of the lattices $\Delta(p, n)$, n any integer and p any odd prime (cf. Theorems 3.9, 4.4), and the lattices $\Delta^-(p, n)$ (in the case $p \equiv 1 \bmod 4$). Here, $\Delta^-(p, n)$ is obtained from $\Delta(p, n)$ by means of Proposition 2.4 (with $G^+ = G_n^-$ if n is odd and $G^+ = C_2 \times G_n^+$ if n is even). Throughout this section, Lagrangians are considered oriented.

First we deal with the lattices $\Delta(p, n)$. Fix an oriented Lagrangian L_0 with an ordered basis $(u_1, \ldots, u_n)$ (for short: $L_0 = (u_1, \ldots, u_n)$), and a generating vector $v(L_0)$ of $\Delta(L_0)$. For an arbitrary oriented Lagrangian $M = (v_1, \ldots, v_n)$ we find an element $\nu_M \in Sp_{2n}(p)$ such that $\nu_M(u_i) = v_i$ for all i, and set $v(M) = \nu_M(v(L_0))$. It is easy to see that this definition does not depend on the choice of ν_M. Finally, we put $u(L) = \sigma(v(L))$ (cf. Lemma 3.6).

Definition 5.1. Let p be any odd prime and n any integer. Let L, M be arbitrary *oriented* Lagrangians in $W = \mathbb{F}_p^{2n}$. Then the *index* $[L, M]$ of the ordered pair (L, M) is defined to be $\left(\frac{\det F}{p}\right)$, where the matrix F is defined as follows. Let $\dim(L \cap M) = k$, choose ordered bases

$$(u_1, \ldots, u_k, v_1, \ldots, v_{n-k}),\ (u_1, \ldots, u_k, w_1, \ldots, w_{n-k})$$

of L, M, respectively; set $F := F(L, M) := (\langle v_i, w_j \rangle)_{1 \leq i,j \leq n-k}$.

Proposition 5.2. *The index is well defined. It is symmetric and G_n-invariant on pairs (L, M) with $n - \dim(L \cap M)$ even. Moreover, if L, M, L', M' are oriented Lagrangians and* $\dim(L \cap M) = \dim(L' \cap M')$*, then*

$$\begin{aligned}[L, M](v(L), v(M)) &= [L', M'](v(L'), v(M')),\\ [L, M](u(L), v(M)) &= [L', M'](u(L'), v(M')),\\ [L, M](u(L), u(M)) &= [L', M'](u(L'), u(M')).\end{aligned}$$

Proof. First we show that $\left(\frac{\det F}{p}\right)$ is independent of the bases chosen. For, suppose

$$(u'_1, \dots, u'_k, v'_1, \dots, v'_{n-k}),\ (u'_1, \dots, u'_k, w'_1, \dots, w'_{n-k})$$

are other ordered bases of

$$L = (u_1, \dots, u_k, v_1, \dots, v_{n-k}),\ M = (u_1, \dots, u_k, w_1, \dots, w_{n-k}).$$

Then the transition matrices (from the old bases to the new bases) are $\begin{pmatrix} A & X \\ 0 & B \end{pmatrix}$ and $\begin{pmatrix} A & Y \\ 0 & C \end{pmatrix}$, where $A \in GL_k(p)$, $X, Y \in M_{k,n-k}(\mathbb{F}_p)$, $B, C \in GL_{n-k}(p)$. Since L, M are oriented, $\det A \cdot \det B$ and $\det A \cdot \det C$ belong to $\mathbb{F}_p^{\bullet 2}$. Clearly, F is changed to ${}^tBFC$ and $\left(\frac{\det F}{p}\right) = \left(\frac{\det {}^tBFC}{p}\right)$.

If $g \in G_n$ and $\langle gu, gv\rangle = \lambda \cdot \langle u, v\rangle$ for all $u, v \in V$, then $[g(L), g(M)] = \left(\frac{\lambda}{p}\right)^{n-k}[L, M]$. Furthermore, $[M, L] = \epsilon^{n-k}[L, M]$. In particular, $[L, M]$ is symmetric and G_n-invariant on pairs (L, M) with $n - \dim(L \cap M)$ even.

Finally, assume

$$\begin{aligned}L &= (u_1, \dots, u_k, v_1, \dots, v_{n-k}),\ M = (u_1, \dots, u_k, w_1, \dots, w_{n-k}),\\ L' &= (u'_1, \dots, u'_k, v'_1, \dots, v'_{n-k}),\ M' = (u'_1, \dots, u'_k, w'_1, \dots, w'_{n-k})\end{aligned}$$

are oriented Lagrangians in W. Then there exists $g \in Sp_{2n}(p)$ such that $g(L) = \pm L'$, $g(M) = \pm M'$. Let $\begin{pmatrix} A & X \\ 0 & B \end{pmatrix}$ (resp. $\begin{pmatrix} A & Y \\ 0 & C \end{pmatrix}$) be the transition matrix from the basis $(g(u_1), \dots, g(u_k), g(v_1), \dots, g(v_{n-k}))$ of $g(L)$ to the basis $(u'_1, \dots, u'_k, v'_1, \dots, v'_{n-k})$ of L' (resp. from the basis $(g(u_1), \dots, g(u_k), g(w_1), \dots,$ $g(w_{n-k}))$ to $(u'_1, \dots, u'_k, w'_1, \dots, w'_{n-k})$). Then

$$v(L') = \left(\frac{\det A \cdot \det B}{p}\right) g(v(L)),\ v(M') = \left(\frac{\det A \cdot \det C}{p}\right) g(v(M))$$

and so $(v(L'), v(M')) = \left(\frac{\det B \cdot \det C}{p}\right)(v(L), v(M))$. On the other hand, one can show that $F(L', M') = {}^tB \cdot F(L, M) \cdot C$, yielding $[L', M'] = \left(\frac{\det B \cdot \det C}{p}\right)[L, M]$. Hence $[L, M](v(L), v(M)) = [L', M'](v(L'), v(M'))$. The identities

$$\begin{aligned}[L, M](u(L), v(M)) &= [L', M'](u(L'), v(M')),\\ [L, M](u(L), u(M)) &= [L', M'](u(L'), u(M'))\end{aligned}$$

are proved in the same way. □

Theorem 5.3. *Let p be any odd prime and n any integer, and let $\epsilon = (-1)^{(p-1)/2}$. Under the above notation one has*

$$(v(L), v(M)) = (\epsilon/p)^{(n-k)/2} p^{[n/2]}[L, M]$$

for any oriented Lagrangians L, M with $k = \dim(L \cap M)$ and $n - k$ even.

Proof. By Corollary 3.5, Theorem 4.4 and Proposition 5.2, there are constants $C_k = \pm 1$ such that $[L, M](v(L), v(M)) = p^{[n/2]-(n-k)/2} C_k$ for any oriented Lagrangians L, M with $k = \dim(L \cap M)$ and $n - k$ even. We want to show that

$$C_k = \epsilon^{(n-k)/2}. \tag{12}$$

Clearly, (12) holds for $k = n$.

1) At this point we prove (12) for $k = n - 2$ (and $n \geq 2$). Because of the descent $n \rightsquigarrow n - 1$ used in Theorem 4.4, we can restrict ourselves to the case n is *odd* (and so $n \geq 3$). In order to determine C_{n-2}, we use the standard spread $\{W^\infty, W^\lambda \mid \lambda \in \mathbb{F}_q\}$ of $W = \mathbb{F}_p^{2n}$ (see the discussion before (7)). As usual, we assume that $\langle e_i, f_j \rangle = \delta_{i,j}$, where $W^0 = (e_1, \ldots, e_n)$, $W^\infty = (f_1, \ldots, f_n)$. Due to our identification of W with $\mathbb{F}_q^2$, $q = p^n$, we have $e_i = (\alpha_i, 0)$, $f_i = (0, \beta_i)$ for any i and some α_i, $\beta_i \in \mathbb{F}_q$. Observe that there is a map from $Sp_{2n}(p)$ which sends the oriented Lagrangian $L_0 := W^0$ to W^∞ (resp. to $W^\lambda = ((\alpha_1, \lambda\alpha_1), \ldots, (\alpha_n, \lambda\alpha_n))$, $\lambda \in \mathbb{F}_q$). Now take

$$L = (e_1, f_2, f_3, \ldots, f_n),\ M = (f_1, e_2, f_3, \ldots, f_n).$$

Then $\dim(L \cap M) = n-2$, $[L, M] = \epsilon$. Since $\dim(L \cap W^\infty) = \dim(M \cap W^\infty) = n-1$, we have

$$v(L) = \sum_{\lambda \in \mathbb{F}_q} a_\lambda v(W^\lambda),\ v(M) = \sum_{\lambda \in \mathbb{F}_q} b_\lambda v(W^\lambda)$$

and so

$$\epsilon p^{(n-3)/2} C_{n-2} = (v(L), v(M)) = p^{(n-1)/2} \sum_{\lambda \in \mathbb{F}_q} a_\lambda b_\lambda. \tag{13}$$

One easily sees that $a_\lambda \neq 0$ if and only if $\mathrm{tr}(\lambda(\alpha_1)^2) = 0$. Similarly, $b_\lambda \neq 0$ if and only if $\mathrm{tr}(\lambda(\alpha_2)^2) = 0$. Observe that $(\alpha_1)^2$ and $(\alpha_2)^2$ are linearly independent over $\mathbb{F}_p$; otherwise $\mathbb{F}_q$ would contain $\mathbb{F}_p(\alpha_1/\alpha_2) = \mathbb{F}_{p^2}$, contrary to the assumption that n is odd. Hence $a_\lambda b_\lambda \neq 0$ for exactly p^{n-2} values of $\lambda \in \mathbb{F}_q$. Moreover, if $a_\lambda b_\lambda \neq 0$, then $a_\lambda b_\lambda = p^{1-n}$, since in this case $\dim(L \cap W^\lambda) = \dim(M \cap W^\lambda) = 1$ and $[W^\lambda, L] = [W^\lambda, M] = 1$. Bearing (13) in mind, we obtain $C_{n-2} = \epsilon$, as stated.

2) Here we show that

$$C_{n-2[n/2]} = C_{n+2-2[n/2]} C_{n-2} \tag{14}$$

for any $n \geq 2$.

2a) Because of the descent $n \rightsquigarrow n - 1$ used in Theorem 4.4, we can restrict ourselves to the case n is *even.* In order to prove (14): $C_0 = C_2 C_{n-2}$, we consider the standard spread $\{W^\infty, W^\lambda \mid \lambda \in \mathbb{F}_q\}$ of $W = \mathbb{F}_p^{2n}$. As above, we assume that $\langle e_i, f_j \rangle = \delta_{i,j}$, where $W^0 = (e_1, \ldots, e_n)$, $W^\infty = (f_1, \ldots, f_n)$. Due to our identification of W with $\mathbb{F}_q^2$, $q = p^n$, we have $e_i = (\alpha_i, 0)$, $f_i = (0, \beta_i)$ for any i and some α_i, $\beta_i \in \mathbb{F}_q$. Since n is even, without loss of generality we may suppose that $\alpha_1 = 1$ and $\alpha_2 = e \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Observe that there is a map from $Sp_{2n}(p)$ which sends the oriented Lagrangian $L_0 := W^0$ to W^∞ (resp. to $W^\lambda = ((\alpha_1, \lambda\alpha_1), \ldots, (\alpha_n, \lambda\alpha_n))$, $\lambda \in \mathbb{F}_q$). Our identification of W with $\mathbb{F}_q^2$ embeds $R = SL_2(q)$ naturally in $Sp_{2n}(p)$. Consider the following elements

$$r_a = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix},\ s_b = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix},\ t = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ a \in \mathbb{F}_q^\bullet,\ b \in \mathbb{F}_q$$

of R. Then they act on the vectors $v(W^\lambda)$ as follows:

$$\begin{array}{llll} r_a: & v(W^\infty) \mapsto (\frac{a}{q})v(W^\infty), & v(W^\lambda) \mapsto (\frac{a}{q})v(W^{a^2\lambda}), \\ s_b: & v(W^\infty) \mapsto v(W^\infty), & v(W^\lambda) \mapsto v(W^{\lambda+b}), \\ t: & v(W^\infty) \leftrightarrow \mu v(W^0), & v(W^\lambda) \mapsto (\frac{\lambda}{q})v(W^{-1/\lambda}). \end{array} \tag{15}$$

Here, $(\frac{\lambda}{q}) = \lambda^{(q-1)/2}$ and $\mu = \left(\frac{\det T}{q}\right)$, where $T = (\mathrm{tr}(\alpha_i\beta_j))_{1\leq i,j\leq n}$ and $\mathrm{tr} := \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}$. (For instance, $\mu = -1$ if $n = 2$.) Indeed, the relation (15) is evident for s_b. Furthermore, the factor $(\frac{a}{q})$ appears in (15) for r_a, since the map sending each f_i to af_i has determinant $N_{\mathbb{F}_q/\mathbb{F}_p}(a)$. Similarly, for any $\lambda \in \mathbb{F}_q$, the map sending each $(a^{-1}\alpha_i, a\lambda\alpha_i)$ to $(\alpha_i, a^2\lambda\alpha_i)$ has determinant $N_{\mathbb{F}_q/\mathbb{F}_p}(a)$. By the same reason the factor $(\frac{\lambda}{q})$ appears in the formula for t. Finally, $t(e_i) = (0, \alpha_i)$, and the map sending each $(0, \alpha_i)$ to $f_i = (0, \beta_i)$ has matrix T^{-1}.

2b) Using the action of s_b, we see that there is $\gamma = \pm 1$ such that $(v(W^\infty), v(W^\lambda)) = \gamma$ for all $\lambda \in \mathbb{F}_q$. Next, t acting on this relation yields $(v(W^0), v(W^\lambda)) = \mu\gamma$ if $\lambda \in \mathbb{F}_q$ is a square, and $-\mu\gamma$ otherwise. Finally, using the action of s_b once more, we see that for $\lambda \neq \lambda' \in \mathbb{F}_q$, $(v(W^\lambda), v(W^{\lambda'})) = \mu\gamma$ if $\lambda - \lambda'$ is a square, and $-\mu\gamma$ otherwise. Since $[W^\infty, W^0] = 1$, $\gamma = C_0$.

2c) The proof of Theorem 4.2 shows that $v(W^\infty)$ and $v(W^\lambda)$, $\lambda \in \mathbb{F}_q$, are linearly independent: $v(W^\infty) = \sum_{\lambda\in\mathbb{F}_q} a_\lambda v(W^\lambda)$ for $a_\lambda \in \mathbb{C}$. Averaging this relation by means of s_b, $b \in \mathbb{F}_q$, we get $v(W^\infty) = a\sum_{\lambda\in\mathbb{F}_q} v(W^\lambda)$ for $a \in \mathbb{C}$. Hence

$$\begin{aligned} \gamma &= (v(W^\infty), v(W^0)) \\ &= a\sqrt{q} + a\textstyle\sum_{\lambda\in\mathbb{F}_q^{\bullet 2}}(v(W^0), v(W^\lambda)) + a\sum_{\lambda\in\mathbb{F}_q^\bullet\setminus\mathbb{F}_q^{\bullet 2}}(v(W^0), v(W^\lambda)) \\ &= a\sqrt{q} + \tfrac{q-1}{2}a\mu\gamma - \tfrac{q-1}{2}a\mu\gamma = a\sqrt{q}, \end{aligned}$$

i.e. $a = \gamma p^{-n/2}$. We have shown that

$$v(W^\infty) = C_0 p^{-n/2} \sum_{\lambda\in\mathbb{F}_q} v(W^\lambda). \tag{16}$$

2d) Now we consider the oriented Lagrangian $M = (e_1, e_2, f_3, \ldots, f_n)$. Since $\dim(M \cap W^\infty) = n - 2$ and $[M, W^\infty] = 1$, $(v(M), v(W^\infty)) = p^{n/2-1}C_{n-2}$. We compute this scalar product in another way using (16). For $\lambda \in \mathbb{F}_q$, it is clear that $\dim(M \cap W^\lambda) \leq 2$. Moreover, $\dim(M \cap W^\lambda) = 2$ if and only if

$$\mathrm{tr}(\lambda) = \mathrm{tr}(\lambda e) = \mathrm{tr}(\lambda e^2) = 0. \tag{17}$$

(Recall that we have chosen $\alpha_1 = 1$ and $\alpha_2 = e \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$.) Since $\mathbb{F}_p(e) = \mathbb{F}_{p^2}$, (17) holds for exactly p^{n-2} values of $\lambda \in \mathbb{F}_q$. Denote $\mathcal{X} = \{\lambda \in \mathbb{F}_q \mid \dim(M \cap W^\lambda) = 2\}$, $\mathcal{Y} = \mathbb{F}_q \setminus \mathcal{X}$. By the choice of α_1 and α_2, $M \cap W^\lambda = 0$ for any $\lambda \in \mathcal{Y}$.

2e) It is easy to check that $[M, W^\lambda] = 1$ for any $\lambda \in \mathcal{X}$. In particular,

$$\sum_{\lambda\in\mathcal{X}} (v(M), v(W^\lambda)) = p^{n-1}C_2.$$

Similarly, $[M, W^\lambda] = \left(\frac{\det A(\lambda)}{p}\right)$ for any $\lambda \in \mathcal{Y}$, where

$$A(\lambda) := \begin{pmatrix} \mathrm{tr}(\lambda) & \mathrm{tr}(\lambda e) \\ \mathrm{tr}(\lambda e) & \mathrm{tr}(\lambda e^2) \end{pmatrix}.$$

Now we fix a non-square element σ in $\mathbb{F}_{p^2}$. Then λ satisfies (17) if and only if $\lambda\sigma$ does. This means that the multiplication by σ leaves $\mathcal{Y}$ fixed. On the other hand, observe that $[M, W^\lambda] = -[M, W^{\lambda\sigma}]$ for any $\lambda \in \mathcal{Y}$. (Indeed,

$$\det A(\lambda) = \sum_{i,j=0}^{n-1} \lambda^{p^i+p^j} \left(e^{2p^j} - e^{p^i+p^j}\right).$$

Clearly, if $i-j$ is even, then $e^{2p^j} = e^{p^i+p^j}$. If $i-j$ is odd, then $\sigma^{p^i+p^j} = \sigma^{p+1}$. This argument shows that $\det A(\lambda\sigma) = \sigma^{p+1}\det A(\lambda)$. Now σ^{p+1} is a non-square in $\mathbb{F}_p$; hence the claim follows.) Consequently,

$$\sum_{\lambda\in\mathcal{Y}} (v(M), v(W^\lambda)) = \frac{1}{2}\sum_{\lambda\in\mathcal{Y}} \left((v(M), v(W^\lambda)) + (v(M), v(W^{\lambda\sigma}))\right)$$

$$= \frac{C_0}{2}\sum_{\lambda\in\mathcal{Y}} \left([M, W^\lambda] + [M, W^{\lambda\sigma}]\right) = 0.$$

2f) As a result of the computations in pp. 2c), 2d) and 2e), we obtain

$$p^{n/2-1}C_{n-2} = (v(M), v(W^\infty))$$

$$= \left(\sum_{\lambda\in\mathcal{X}} (v(M), v(W^\lambda)) + \sum_{\lambda\in\mathcal{Y}} (v(M), v(W^\lambda))\right) = p^{n/2-1}C_0C_2,$$

i.e. $C_0 = C_2C_{n-2}$, as stated.

3) Finally, we prove (12) by induction on n. Because of the descent $n \rightsquigarrow n-1$ used in Theorem 4.4, we can restrict ourselves to the case n is *odd*. The induction base $n = 1, 3$ has already been established, since we have proved (12) for $k = n, n-2$. For the induction step, observe that the descent $n \rightsquigarrow n-2$ used in the proof of Proposition 3.4 allows us to state that $C_k = \epsilon^{(n-k)/2}$ for any odd $k \geq 3$. According to (14),

$$C_1 = C_3 \cdot C_{n-2} = \epsilon^{(n-3)/2} \cdot \epsilon = \epsilon^{(n-1)/2},$$

and the induction step is over. □

Recall that $(v(L), v(M))$ is 0 if $n - \dim(L \cap M)$ is odd. Therefore, Theorem 5.3 completely determines the Gram matrix of the lattice $\Delta(p, n)$.

Corollary 5.4. *Let p be any odd prime and n any odd integer. Relative to the generating system $\{v(L) \mid L \in \mathcal{L}(W)\}$ the unimodular lattice $\Delta(p, n)$ has the following Gram matrix:*

$$(v(L), v(M)) = \begin{cases} \epsilon^{(n-k)/2}p^{(k-1)/2}[L, M], & \dim(L\cap M) = k \equiv 1 \bmod 2, \\ 0, & \dim(L\cap M) \equiv 0 \bmod 2. \end{cases} \quad \square$$

Example 5.5. Let $p = n = 3$. Then the Gram matrix for $\Delta(3, 3)$ produced by Corollary 5.4 is the same as given in [BaV].

Corollary 5.6. *Let p be any odd prime and n any even integer. Relative to the generating system $\{v(L) \mid L \in \mathcal{L}(W)\}$ the p-modular lattice $\Delta(p, n)$ has the following Gram matrix:*

$$(v(L), v(M)) = \begin{cases} \epsilon^{(n-k)/2}p^{k/2}[L, M], & \dim(L\cap M) = k \equiv 0 \bmod 2, \\ 0, & \dim(L\cap M) \equiv 1 \bmod 2. \end{cases} \quad \square$$

Example 5.7. Let p be any odd integer. Then the p-modular (p^2+1)-dimensional lattice $\Delta(p,2)$ is generated by $2(p+1)(p^2+1)$ vectors $v(L)$, L any oriented Lagrangian in $\mathbb{F}_p^4$. Here, $v(-L)=-v(L)$, $(v(L),v(L))=p$, and $(v(L),v(M))$ equals $\epsilon[L,M]$ if $L\cap M=0$ and 0 if $\dim(L\cap M)=1$. Taking $p=5$, we get the 26-dimensional 5-modular lattice with minimum 5 constructed by Nebe.

Clearly, $(u(L),u(M))=p(v(L),v(M))$. Now we want to compute the scalar products $(u(L),v(M))$. Since σ is determined up to sign, the scalar products $(u(L),v(M))$ are determined also up to sign. Recall that $(u(L),v(M))=\pm p^{[n/2]}$ if $\dim(L\cap M)=n-1$ (cf. Lemma 3.6). For definiteness, we choose σ such that

$$(u(L),v(M))=p^{[n/2]}[L,M] \tag{18}$$

for oriented Lagrangians L,M with $\dim(L\cap M)=n-1$.

Theorem 5.8. *Let p be any odd prime and n any integer. Under the convention (18) one has*

$$(u(L),v(M))=(\epsilon/p)^{(n-1-k)/2}p^{[n/2]}[L,M]$$

for any oriented Lagrangians L,M with $k=\dim(L\cap M)$ and $n-k$ odd.

Proof. 1) By Lemma 3.6, Theorem 4.4 and Proposition 5.2, there are constants $D_k=\pm1$ such that $[L,M](u(L),v(M))=p^{[n/2]-(n-1-k)/2}D_k$ for any oriented Lagrangians L,M with $k=\dim(L\cap M)$ and $n-k$ odd. We want to show that

$$D_k=\epsilon^{(n-1-k)/2}. \tag{19}$$

Clearly, (19) holds for $k=n-1$, due to (18). Because of the descent $n\rightsquigarrow n-1$ used in Theorem 4.4, it suffices to prove (19) for odd n.

2) Consider the standard spread of $W=\mathbb{F}_p^{2n}$ (recall n is odd). In the notation of p. 1) of the proof of Theorem 5.3 we set $L=W^\infty$, $M=(e_1,f_2,\dots,f_n)$. Since $L\cap W^\infty$ has odd dimension, $(u(L),v(W^\infty))=0$. Furthermore, for any $\lambda\in\mathbb{F}_q$, $L\cap W^\lambda=0$ and $[L,W^\lambda]=\epsilon^n$. Therefore, $(u(L),v(W^\lambda))=\epsilon^nD_0$, yielding

$$u(L)=\epsilon^nD_0p^{(1-n)/2}\sum_{\lambda\in\mathbb{F}_q}v(W^\lambda).$$

On the other hand, by Theorem 5.3 we have

$$v(M)=\epsilon^{(n-1)/2}p^{(1-n)/2}\sum_{\lambda\in\mathbb{F}_q,\mathrm{tr}(\lambda(\alpha_1)^2)=0}v(W^\lambda).$$

Hence $(u(L),v(M))=\epsilon^{(n+1)/2}p^{(n-1)/2}D_0$. But $\dim(L\cap M)=n-1$ and $[L,M]=\epsilon$; therefore we get $D_0=\epsilon^{(n-1)/2}$. This establishes (19) for $k=0$.

Now we can prove (19) by induction on odd n. The induction base $n=1,3$ has already been established, since we have proved (19) for $k=n-1,0$. For the induction step, observe that the descent $n\rightsquigarrow n-2$ used in the proof of Proposition 3.4 allows us to state that $D_k=\epsilon^{(n-1-k)/2}$ for any even $k\geq 2$, and so the induction step is over. ☐

Next, let $p\equiv 1 \bmod 4$. We determine the Gram matrices for the lattices $\Delta^-(p,n)$. Recall (cf. §2) that $\Delta^-(p,n)$ has the same generating system as of $\Delta(p,n)$. But if $(\cdot,\cdot)$ is the scalar product on $\Delta(p,n)$, then $\Delta^-(p,n)$ is endowed with the scalar product $(\cdot,\cdot)^-$, where $(u,v)^-=p\mathbf{b}(u,v)+\mathbf{a}(\sigma u,v)$. Here $\mathbf{a},\mathbf{b}$ are integers such that $\mathbf{a}^2-p\mathbf{b}^2=-1$. Also, here we have $\epsilon=1$. Bearing this in mind, from the above results we immediately obtain:

Corollary 5.9. *Let $p \equiv 1 \bmod 4$ be a prime and n any even integer. Relative to the generating system $\{v(L) \mid L \in \mathcal{L}(W)\}$ the unimodular lattice $\Delta^-(p,n)$ has the following Gram matrix:*

$$(v(L), v(M)) = \begin{cases} \mathbf{b}p^{k/2}[L,M], & \dim(L \cap M) = k \equiv 0 \bmod 2, \\ \mathbf{a}p^{(k-1)/2}[L,M], & \dim(L \cap M) = k \equiv 1 \bmod 2. \end{cases} \qquad \square$$

Corollary 5.10. *Let $p \equiv 1 \bmod 4$ be a prime and n any odd integer. Relative to the generating system $\{v(L) \mid L \in \mathcal{L}(W)\}$ the p-modular lattice $\Delta^-(p,n)$ has the following Gram matrix:*

$$(v(L), v(M)) = \begin{cases} \mathbf{b}p^{(k+1)/2}[L,M], & \dim(L \cap M) = k \equiv 1 \bmod 2, \\ \mathbf{a}p^{k/2}[L,M], & \dim(L \cap M) = k \equiv 0 \bmod 2. \end{cases} \qquad \square$$

Example 5.11. Let $p \equiv 1 \bmod 4$. Then the p-modular $(p+1)$-dimensional lattice $\Delta^-(p,1)$ has a basis consisting of the vectors e_λ, $\lambda \in \mathbb{F}_p \cup \{\infty\}$. These vectors are of norm $p\mathbf{b}$; furthermore, $(e_\lambda, e_\infty) = \mathbf{a}$ for any $\lambda \in \mathbb{F}_p$. Finally, for $\lambda \neq \mu \in \mathbb{F}_p$ we have $(e_\lambda, e_\mu) = \mathbf{a}$ if $\lambda - \mu$ is a square, and $-\mathbf{a}$ otherwise. Thus $\Delta^-(p,1)$ is just the lattice $M_{p+1,2}$ constructed in Theorem (V.2) of [NPl].

Example 5.12. Let $p \equiv 1 \bmod 4$. Then the unimodular (p^2+1)-dimensional lattice $\Delta^-(p,2)$ is generated by $2(p+1)(p^2+1)$ vectors $v(L)$, L any oriented Lagrangian in $\mathbb{F}_p^4$, with the following Gram matrix:

$$(v(L), v(M)) = \begin{cases} \mathbf{b}p[L,M], & \dim(L \cap M) = 2, \\ \mathbf{a}[L,M], & \dim(L \cap M) = 1, \\ \mathbf{b}[L,M], & \dim(L \cap M) = 0. \end{cases}$$

Taking $p = 5$ (and $\mathbf{a} = 2$, $\mathbf{b} = 1$), we get the 26-dimensional unimodular lattice with minimum 3 constructed by Nebe.

As we have mentioned above, the lattices $\Delta = \Delta(p,n)$ (n even), $\Delta^-(p,n)$ ($p \equiv 1 \bmod 4$ and n even) are p-modular. But they are *not* (self-dual) $\mathfrak{o}$-lattices (where $\mathfrak{o} = \langle 1, (1+\theta)/2 \rangle_{\mathbb{Z}}$ and $\theta = \sqrt{\epsilon p}$) by the following reason. The multiplication by θ should be given as $\theta(v) = \sigma(v)$, $v \in \Delta$. If Δ is an $\mathfrak{o}$-lattice, then Δ contains $\frac{1+\theta}{2} v(L) = (v(L) + u(L))/2$, L a Lagrangian. On the other hand, $((v(L) + u(L))/2, v(L)) = p^{[n/2]}/2$ is not integral, a contradiction.

However, if we restrict ourselves to the S_n-stable lattices, then in some cases we can get self-dual $\mathfrak{o}$-lattices. Recall that an integral lattice Γ is called a *2-neighbour* of a given integral lattice Λ if the intersection $\Gamma \cap \Lambda$ has index 2 in both of Λ and Γ.

Proposition 5.13. *Let Δ denote any of the lattices $\Delta(p,n)$, $\Delta^-(p,n)$. Then the following assertions hold.*

(i) *If $p \equiv 1 \bmod 4$, then Δ has no 2-neighbours.*

(ii) *Let $p \equiv 3 \bmod 4$. Then Δ has exactly two 2-neighbours, namely $\Delta^\delta = \langle \Delta^0, \frac{1}{2}(v(L) + \delta u(L)) \rangle_{\mathbb{Z}}$, where $\delta = \pm 1$, Δ^0 the even part of Δ and L a fixed Lagrangian. These neighbours are S_n-stable. If $p \equiv 7 \bmod 8$, then they are self-dual $\mathfrak{o}$-lattices (w.r.t. the Hermitian form $u \circ v$ defined in (3)) if n is even, and even unimodular (Euclidean) $\mathfrak{o}$-stable lattices if n is odd.*

Proof. It is easy to see (cf. Lemma 6.5) that Δ^0 is the unique sublattice of index 2 in Δ. Hence, if Γ is an arbitrary 2-neighbour of Δ, then $\Gamma = \langle \Delta^0, w \rangle_{\mathbb{Z}}$ with $2w \in \Delta$. By definition, $2w \in \Delta \cap 2(\Delta^0)^\# = \Delta^1$ (see also the discussion before Lemma 6.5).

Now $\Delta^1/2\Delta^0$ contains exactly 3 nontrivial cosets, namely those with representatives $v(L)$, and $w^\delta(L) := v(L)+\delta u(L)$, $\delta = \pm 1$ and L a fixed Lagrangian. The first coset is contained in Δ; hence we can avoid it. Thus we can take $w = \frac{1}{2}w^\delta(L)$ and then $\Gamma = \Delta^\delta$. Observe that this w has (squared) norm $p^{[n/2]}(p+1)/4$ if $\Delta = \Delta(p,n)$, $(\mathbf{b}(p+1)+2\mathbf{a})p^{(n+1)/2}$ if $\Delta = \Delta^-(p,n)$ and n is odd, and $(\mathbf{b}(p+1)+2\mathbf{a})p^{n/2}$ if $\Delta = \Delta^-(p,n)$ and n is even (cf. Theorems 5.3 and 5.8). Therefore, Γ is integral (w.r.t. $(\cdot,\cdot)$) if and only if $p \equiv 3 \bmod 4$, and even if and only if $p \equiv 7 \bmod 8$.

Clearly, G_n permutes the two cosets with representatives $w^\delta(L)$ in $\Delta^1/2\Delta^0$. But S_n has no subgroups of index 2; hence S_n stabilizes each of Δ^δ. On the other hand, G_n permutes the lattices Δ^δ transitively. (For recall that $u(L) = \sigma(v(L))$. Choose $g \in G_n \setminus S_n$ such that $g(L) = L$. Then $g(w^\delta(L)) = g(v(L)) - \delta\sigma(g(v(L))) = \pm w^{-\delta}(L)$.)

Observe that Δ^0, Δ^1 are always $\mathfrak{o}$-stable. Indeed, put $w^\delta(M) = v(M)+\delta u(M)$ for any oriented Lagrangian M. For any $s \in S_n$ with $s(L) = M$ one has $s(w^\delta(L)) = \pm w^\delta(M)$. But we already know that s fixes the coset $w^\delta(L)+2\Delta^0$. Hence $w^\delta(L)+w^\delta(M) \in 2\Delta^0$. In other words, $(1+\sigma)(v(L)+v(M)) \in 2\Delta^0$. This means Δ^0 is $\mathfrak{o}$-stable, since we have $\theta v = \sigma(v)$ by definition and Δ^0 is generated by the $v(L)+v(M)$'s. Next, $\frac{1-\delta\sigma}{2}(w^\delta(L)) = \frac{1-\epsilon p}{2}v(L) \in \Delta^1$, as $\epsilon p \equiv 1 \bmod 4$. This implies that Δ^1 is $\mathfrak{o}$-stable. This computation also convinces us that Δ^δ is $\mathfrak{o}$-stable if and only if $p \equiv \pm 1 \bmod 8$.

Finally, assume $p \equiv 3 \bmod 4$. If n is odd, then Δ is unimodular; hence Δ^δ is unimodular, and even if $p \equiv 7 \bmod 8$. Suppose n is even and $p \equiv 7 \bmod 8$. Then direct computation shows that $\Delta^\delta \circ \Delta^\delta \subseteq \mathfrak{o}$. On the other hand, $\Delta = \theta\Delta^\# = \Delta^\perp$ and Δ, Δ^δ are neighbours. Consequently, Δ^δ is a self-dual $\mathfrak{o}$-lattice. ∎

6. Classification of invariant lattices

The aim of this section is to prove Theorem 1.3. The case $p^n = 3$ is trivial (see [SchT], §5), so throughout this section we suppose that $p^n > 3$.

Let H, Γ, Δ be as in Theorem 1.3. Let ρ denote the H-character afforded by Γ and θ any irreducible constituent of ρ restricted to $S := Sp_{2n}(p)$. If $n \geq 2$, then the condition $1 < \theta(1) \leq p^n+1$ implies by Theorem 5.2 [TZa 1] that $\theta \in \{\psi, \overline{\psi}\}$; hence ρ is absolutely irreducible. The same is true if $n = 1$, except for the cases $p = 3$ or $p \equiv 1 \bmod 6$, where $\rho|_S$ can be irreducible. Thus, under the assumptions of Theorem 1.3, ρ satisfies the assumptions of Lemma 2.1. Hence, $G := H/K$ is as defined in Theorem 1.3, and ρ is afforded by Δ, i.e. $\rho = \chi$, $\Gamma \otimes \mathbb{C} = \Delta \otimes \mathbb{C}$. By the Deuring-Noether Theorem, the $\mathbb{Q}H$-modules $\Gamma \otimes \mathbb{Q}$ and $\Delta \otimes \mathbb{Q}$ are equivalent. Therefore, without loss of generality one may suppose that Γ is a G-invariant sublattice in Δ. Thus the proof of Theorem 1.3 reduces to the classification of G-invariant sublattices Γ in Δ.

For any Lagrangian L, let $S(L)$ be as defined in (5) and $R(L) = S \cap S(L)$. We start with the following observation.

Lemma 6.1. *Let $n \geq 2$. Then the restriction of $\chi \bmod p$ to $R(L)$ contains the trivial character with multiplicity ≤ 4.*

Proof. Consider the standard embedding $T := SL_n(p) \hookrightarrow R(L) \subseteq Sp_{2n}(p)$. It suffices to show that 1_T enters $(\chi \bmod p)|_T$ with multiplicity at most 4. Let θ denote the S-character of the Weil representation $\mathcal{W}$ (then θ is the sum of ψ and another character of degree $(p^n-1)/2$). If $n \geq 3$, then Zalesskii's formula for

$(\theta \bmod p)|_T$ [Zal] tells us that this character contains 1_T with multiplicity 2. Since $\chi|_S = \psi + \overline{\psi}$, we are done. Now let $n = 2$. Then due to [Tiep 4], §3,

$$\theta|_T = 2 \cdot 1_T + \xi_1 + \xi_2 + St + 2(\chi_1 + \ldots + \chi_{(p-3)/2}),$$

where ξ_s, St, χ_s are irreducible characters of T of degree $(p+1)/2$, p, and $p+1$, respectively. All the nontrivial characters occurring in this formula remain absolutely irreducible, being reduced modulo p. Hence $(\theta \bmod p)|_H$ contains 1_T with multiplicity 2, and so we are done. □

Lemma 6.2. *The module $V_p = \Delta/p\Delta$ has a unique nonzero proper G-submodule, and this submodule coincides with $\phi(\Delta)/p\Delta$.*

Proof. 1) Let A be any nonzero proper submodule in V_p. By Proposition 2.2, the Brauer character afforded by A is η_i for some $i = 1, 2$. In particular, A is absolutely irreducible. An example of such a submodule A is $\phi(\Delta)/p\Delta$. Therefore, the lemma is equivalent to saying that V_p is indecomposable. Assume the contrary: V_p is decomposable: $V_p = A \oplus B$. Clearly, A and B are isomorphic as S-modules. Hence, due to Lemma 2.5, in the case $p \equiv 1 \bmod 4$, it suffices to prove the lemma for one of the isoclinic groups $C_2 \times G_n^+$ and G_n^-. In what follows, we take $G = G_n^-$ if n is odd, and $G = G_n^+$ if n is even; furthermore, $\Delta = \Delta(p, n)$.

If $n = 1$, then due to [Ward 2], A is a unique nonzero submodule of V_p (and A is called the *modular quadratic residue code*). This forces V_p to be indecomposable, a contradiction. Therefore from now on we suppose that $n \geq 2$.

2) Let L be any Lagrangian. By Proposition 3.1, the subgroup $S(L)$ fixes the vector $v(L)$. Observe that $v(L) \notin p\Delta$; hence one can view $v(L)$ as a nonzero vector in V_p. Set

$$W(L) = \{v \in V_p \mid \forall \varphi \in S(L), \varphi(v) = v\}.$$

Without loss of generality one may suppose that $\vartheta_n \in S(L)$, and so $S(L) = \langle R(L), \vartheta_n \rangle$. For brevity, we denote by χ_S the restriction of $\chi \bmod p = \eta_1 + \eta_2$ to $S(L)$, by χ_R the restriction of $\chi \bmod p$ to $R(L)$, by α the trivial character of $S(L)$, by β the nontrivial character of degree 1 of $S(L)$ with $\operatorname{Ker} \beta = \langle R(L), \vartheta_n^2 \rangle$. Write $v(L) = a + b$ for $a \in A$, $b \in B$. Remark that $a, b \neq 0$. (Assume the contrary: $a = 0$. Then $v(L) \in B$ for any Lagrangian L. As Δ is generated by the vectors $v(M)$, which are acted on transitively by S, B must be equal to the whole of V_p, a contradiction.) Now $S(L)$ fixes each of the subspaces A, B; therefore in fact $a, b \in W(L)$.

3) First consider the case n is odd. Then η_i is not self-dual by Proposition 2.2; hence A and B are totally singular relative to $(\cdot, \cdot)_p$, the reduction modulo p of the scalar product. In particular, $(a, a)_p = (b, b)_p = 0$. As $n \geq 3$, we have:

$$0 = (v(L), v(L))_p = (a + b, a + b)_p = (a, a)_p + (b, b)_p + 2(a, b)_p = 2(a, b)_p,$$

which implies that $(a, b)_p = 0$. We have just shown that $C := \langle a, b \rangle_{\mathbb{F}_p} \subseteq W(L)$ is totally singular with respect to $(\cdot, \cdot)_p$: $C \subseteq C^\perp$. Besides, the $S(L)$-modules $V_p/C^\perp$ and C^* are isomorphic. (Recall that $\det \Delta = 1$ in the case n is odd.) From this it follows that $V_p/C^\perp$ affords the $S(L)$-character 2α. Thus χ_S contains α with multiplicity at least 4. In the proof of Proposition 3.1 we have singled out some subspace U of V, which is acted on by $S(L)$ with character $\alpha + \beta$. From this it follows that χ_S contains $4\alpha + \beta$, and so χ_R contains $1_{R(L)}$ with multiplicity at least 5, contrary to Lemma 6.1.

4) Finally, let n be even. Then both η_1, η_2 are of type $+$. Namely, the form $(\cdot,\cdot)_p$ is non-degenerate on B, since $A = p\Delta^{\#}/p\Delta$ is the radical of the form $(\cdot,\cdot)_p$. Also, A carries the non-degenerate symmetric form $(x+p\Delta, y+p\Delta)'_p = \frac{1}{p}(x,y) \bmod p$. Now $(b,b)_p = (v(L),v(L))_p = 0$. Thus $C := \langle b\rangle_{\mathbb{F}_p} \subseteq W(L)$ is totally singular with respect to $(\cdot,\cdot)_p|_B$: $C \subseteq C^{\perp}$. Besides, the $S(L)$-modules $B/C^{\perp}$ and C^* are isomorphic. From this it follows that $B/C^{\perp}$ and of course $\langle a\rangle_{\mathbb{F}_p}$ afford the $S(L)$-character α. Thus χ_S contains α with multiplicity at least 3.

On the other hand, χ_S contains β with multiplicity at least 2. (For set $D = \langle u(L)\rangle_{\mathbb{F}_p}$. Since $(u(L),u(L)) = p^{n/2+1}$, D is totally singular with respect to $(\cdot,\cdot)'_p$: $D \subseteq D^{\perp}$. Besides, the $S(L)$-modules $A/D^{\perp}$ and D^* are isomorphic. From this it follows that $A/D^{\perp}$ affords the $S(L)$-character β.)

As a consequence, χ_R contains $1_{R(L)}$ with multiplicity at least 5, contradicting Lemma 6.1. □

Lemma 6.3. *Let r be a prime, G a finite group, and Λ an integral G-invariant lattice with the following properties:*

(i) *The $\mathbb{F}_rG$-module module $U = \Lambda/r\Lambda$ is uniserial, that is, it has a unique composition series $U = U_0 \supset U_1 \supset \ldots \supset U_m = 0$;*

(ii) *Let Λ_i be the inverse image of U_i in Λ, $0 \le i \le m-1$. Then the $\mathbb{F}_rG$-module $\Lambda_i/r\Lambda_i$ is also uniserial for any $i > 0$.*

Suppose that Γ is any G-invariant sublattice in Λ whose index is an r-power. Then Γ is similar to one of the lattices Λ_i, $0 \le i \le m-1$.

Proof. Denote $\Lambda_m = r\Lambda_0$, $\Lambda_{m+1} = r\Lambda_1$ and, more generally, $\Lambda_{k+m} = r\Lambda_k$, $k = 2, 3, \ldots$. Our assumptions imply that

$$\Lambda_k/r\Lambda_k \supset \Lambda_{k+1}/r\Lambda_k \supset \ldots \supset \Lambda_{k-1+m}/r\Lambda_k \supset 0$$

is the unique composition series of the $\mathbb{F}_rG$-module $\Lambda_k/r\Lambda_k$. In particular, if Γ lies between Λ_k and $r\Lambda_k$, then $\Gamma = \Lambda_{k+j}$ for some j, $0 \le j \le m$, and our claim follows.

Since $(\Lambda : \Gamma)$ is an r-power,

$$\Lambda_0 = \Lambda \supseteq \Gamma \supseteq r^n\Lambda = \Lambda_{nm}$$

for some non-negative integer n. Let ℓ be the minimal non-negative integer such that $\Lambda_i \supseteq \Gamma \supseteq \Lambda_{i+\ell}$ for some i. We prove by induction on ℓ that Γ is equal to some Λ_k. If $\ell \le m$, we are done due to the above observation. Assume $\ell > m$. Without loss of generality we may suppose that $i = 0$. Since $\Lambda_0 \supseteq \Gamma + \Lambda_{\ell-m} \supseteq \Lambda_{\ell-m}$, by the induction hypothesis we get $\Gamma + \Lambda_{\ell-m} = \Lambda_k$ for some k, $0 \le k \le \ell - m$. Now it is clear that $\Lambda_k \supseteq \Gamma \supseteq \Lambda_\ell$. By the minimality of ℓ we must have $k = 0$, i.e., $\Gamma + \Lambda_{\ell-m} = \Lambda_0$. This implies

$$\Lambda_0 \supseteq \Gamma \supseteq p(\Gamma + \Lambda_{\ell-m}) = p\Lambda_0 = \Lambda_m,$$

contrary to the choice of ℓ. The induction step is over. □

Corollary 6.4. *If Γ is any G_n-invariant sublattice of Δ with the index $(\Delta : \Gamma)$ being a power of p, then there exists an integer $k \ge 0$ such that $\Gamma = \phi^k(\Delta)$.*

Proof. By Lemma 6.2, $\phi(\Delta)/p\Delta$ is the unique nonzero proper submodule of V_p; hence V_p is uniserial. Suppose that $\phi(\Delta) \supset \Lambda \supset p\phi(\Delta)$ for some G_n-invariant sublattice Λ. Since $g\phi g^{-1} = \pm\phi$ for all $g \in G_n$, $\phi^{-1}(\Lambda)$ is a G_n-stable sublattice lying between Δ and $p\Delta$, which implies that $\phi^{-1}(\Lambda) = \phi(\Delta)$, $\Lambda = p\Delta$. Thus the module $\phi(\Delta)/p\phi(\Delta)$ is also uniserial. Now we can apply Lemma 6.3. □

Since Δ is an odd lattice, the even part Δ^0 is a G-invariant sublattice of index 2 containing 2Δ. Also, $\Delta^1 = \Delta \cap 2(\Delta^0)^{\#}$ is another G-invariant sublattice containing 2Δ.

Lemma 6.5. *The $\mathbb{F}_2G$-module $V_2 = \Delta/2\Delta$ has precisely two nontrivial proper submodules, namely, $\Delta^i/2\Delta$ with $i = 0, 1$. Moreover, if Γ is any G-invariant sublattice of Δ with the index $(\Delta : \Gamma)$ being a power of two, then there exists an integer $k \geq 0$ such that*

$$\Gamma \in \{2^k\Delta, 2^k\Delta^0, 2^k\Delta^1\}.$$

Proof. Observe that $\mathbf{a}$ is even and $\mathbf{b}$ is odd. Hence the lattices $\Delta(p, n)$ and $\Delta^-(p, n)$ have the same Gram matrix *modulo* 2. In particular, in calculating scalar products modulo 2 we can restrict ourselves to $\Delta(p, n)$.

1) At this point we show that $S := Sp_{2n}(p)$ fixes a unique nonzero vector w in V_2, and $w = v(L) + u(L)$ for any Lagrangian L. To this end, we first observe that $\det \Delta$ is odd; hence the reduction $(\cdot, \cdot)_2$ of the scalar product is non-degenerate on V_2. Next, putting $w(L) = v(L) + u(L)$, by Theorems 5.3 and 5.8 we see that $(w(L), v(M))_2 = 1$ for any arbitrary Lagrangian M. If $\varphi \in G$ and $\varphi(L) = L'$, then $\varphi(w(L)) = w(L')$ (in V_2). Hence $(\varphi(w(L)) - w(L), v(M))_2 = 0$. But V_2 is generated by the vectors $v(M)$ and $(\cdot, \cdot)_2$ is non-degenerate. Therefore, $\varphi(w(L)) = w(L)$. Thus $w := w(L)$ is G-stable. Conversely, let $w' \in V_2$ be a nonzero vector which is fixed by S. Since S acts transitively on the vectors $v(M)$, M any Lagrangian, there exists $\lambda \in \mathbb{F}_2$ such that $(w', v(M))_2 = \lambda$ for all M. If $\lambda = 0$, then the non-degeneracy of $(\cdot, \cdot)_2$ implies that $w' = 0$, contrary to the choice of w'. If $\lambda = 1$, then $(w - w', v(M))_2 = 0$, yielding $w' = w$.

2) Set $U_0 = \Delta^0/2\Delta$, $U_1 = \langle w \rangle_{\mathbb{F}_2}$. Clearly, Δ^0 and so U_0 are generated by the vectors of the form $v(L) + v(M)$, L, M any Lagrangians. Since $(w, v(L) + v(M))_2 = 0$, we see that $U_1 = \Delta^1/2\Delta$. Also, $w \in U_0$. By Proposition 2.2 (ii), $0 \subset U_1 \subset U_0 \subset V_2$ is a composition series of the $\mathbb{F}_2G$-module V_2, with two trivial composition factors and one (absolutely) irreducible factor of dimension $p^n - 1$. Clearly, U_0 and U_1 are dual to each other w.r.t. $(\cdot, \cdot)_2$.

Now let U be any nonzero proper G-submodule in V_2. Then $\dim U \in \{1, 2, p^n - 1, p^n\}$. If $\dim U = 1$, then U must be generated by a nonzero G-stable vector; hence $U = U_1$ due to 1). If $\dim U = p^n$, then the dual module $U^\perp$ has dimension 1; therefore $U^\perp = U_1$, which implies that $U = U_0$. Assume $\dim U = 2$. Then the action of S on U induces a homomorphism from S to $GL(U) = GL_2(2) \simeq \mathbb{S}_3$. But $S = Sp_{2n}(p)$ is perfect (as $p^n > 3$); therefore this homomorphism is trivial, i.e. S acts trivially on U. In this case, V_2 has at least three (distinct) S-stable vectors, contrary to 1). If $\dim U = p^n - 1$, then the dual module $U^\perp$ has dimension 2, again a contradiction.

We have shown that V_2 has just two nontrivial proper submodules: U_0 and U_1.

3) Next we consider any nontrivial proper submodule U in $V_4 = \Delta/4\Delta$, and suppose that $U \not\subseteq 2V_4$. Then $(U + 2V_4)/2V_4$ is a nonzero submodule in $V_4/2V_4 \simeq V_2$. By the results of 2), $(U + 2V_4)/2V_4$ contains U_1. From this it follows that U contains a vector $w' = w + 2x$ for a certain $x \in V_4$. Pick an element $\varphi \in G(L)$ such that $\varphi : v(L) \mapsto v(L)$, $u(L) \mapsto -u(L)$. Then $w' + \varphi(w') = 2y$, where $y = v(L) + x + \varphi(x)$. Since $x + \varphi(x) \in U_0 = \langle w \rangle^\perp$, we get $(w, y)_2 = (w, v(L))_2 = 1$, which means that $y \notin U_0$. We have seen that $U' = (U \cap 2V_4)/4V_4$ is a G-submodule in $2V_4/4V_4 \simeq 2V_2$, which contains a vector $2y \notin 2U_0$. By the results of 2), $U' = 2V_4/4V_4$, i.e. $U \supseteq 2V_4$. This means: if U is any G-submodule of V_4, then either $U \supseteq 2V_4$, or $U \subseteq 2V_4$.

4) Finally, let Γ be any G-invariant sublattice of Δ with $(\Delta : \Gamma) = 2^m$. Then $\Delta \supseteq \Gamma \supseteq 2^m\Delta$. We prove by induction on $m \geq 0$ that there exists an integer $k \geq 0$ such that $\Gamma \in \{2^k\Delta, 2^k\Delta^0, 2^k\Delta^1\}$. This claim is obvious if $m = 0$ or 1 (see item 2)). Now assume $m \geq 2$. Then $\Delta \supseteq \Gamma + 4\Delta \supseteq 4\Delta$. Due to 3), either $\Gamma + 4\Delta \subseteq 2\Delta$, or $\Gamma + 4\Delta \supseteq 2\Delta$. In the former case, $2\Delta \supseteq \Gamma \supseteq 2^m\Delta$; therefore $\Delta \supseteq \frac{1}{2}\Gamma \supseteq 2^{m-1}\Delta$, and one can now use the induction hypothesis. In the latter case,

$$2^{m-1}\Delta \subseteq 2^{m-2}(\Gamma + 4\Delta) = 2^{m-2}\Gamma + 2^m\Delta \subseteq \Gamma,$$

and one can again use the induction hypothesis. □

Proof of Theorem 1.3. Consider any G-invariant lattice Γ lying in Δ. We may suppose that $\Gamma \not\subseteq k\Delta$ for any integer $k > 1$. Clearly, $\Gamma \supseteq l\Delta$ for some natural l. Choose minimal natural ℓ with the property $\Gamma \supseteq \ell\Delta$. If $\ell = 1$, then $\Gamma = \Delta$. Assume that $\ell > 1$. Claim that $\ell = 2^a p^b$ for some non-negative integers a, b. (For assume the contrary: ℓ is divisible by an odd prime r, $r \neq p$. Observe that $(\Gamma + r\Delta)/r\Delta$ is a nonzero G-module in $V_r = \Delta/r\Delta$. By Proposition 2.2 (i), $(\Gamma + r\Delta)/r\Delta = V_r$, $\Gamma + r\Delta = \Delta$. Hence,

$$\frac{\ell}{r}\Delta = \frac{\ell}{r}(\Gamma + r\Delta) = \frac{\ell}{r}\Gamma + \ell\Delta \subseteq \Gamma,$$

contradicting the minimality of ℓ.)

Setting $\widetilde{\Gamma} = \Gamma + p^b\Delta$, one has

$$\Delta \supset \widetilde{\Gamma} \supseteq p^b\Delta, \ \widetilde{\Gamma} \supseteq \Gamma \supseteq 2^a\Gamma + \ell\Delta = 2^a\widetilde{\Gamma}.$$

By Corollary 6.4, $\widetilde{\Gamma} = \phi^k(\Delta)$. Replacing Γ by $\phi^{-k}(\Gamma)$, which is isometrically similar to Γ, we can suppose that $k = 0$, i.e. $\widetilde{\Gamma} = \Delta$. In this case, $\Delta \supset \Gamma \supseteq 2^a\Delta$. By Lemma 6.5, Γ is similar to one of the lattices Δ, Δ^0, Δ^1. □

7. Properties of $\Delta(p, n)$

This section is very sketchy, because a detailed exposition has been given in [SchT], §§4, 6. It turns out that the arguments, given there for the case $p^n \equiv 3 \bmod 4$, are also applicable to the case $p^n \equiv 1 \bmod 4$. Hence we restrict ourselves to exposing the results, which hold for any odd prime p, but omitting the proofs.

For short we denote $G = G_n^-$ if n is odd, and $G = G_n^+$ if n is even. Furthermore, p is any odd prime and $\Delta = \Delta(p, n)$.

First we consider the G-invariant odd unimodular lattice $\Delta = \Delta(p, 3)$ obtained in Theorem 3.9. The generating vectors $v(L)$ now have norm $(v(L), v(L)) = p$, and Δ contains a p-scaled unit lattice Γ, spanned by $N := p^3 + 1$ pairwise orthogonal vectors of norm p (for instance, the $v(L)$, where L runs over a symplectic spread). Therefore, Δ can be described (non-canonically) by a subspace $C := \Delta/\Gamma \subset \Gamma^\#/\Gamma = \frac{1}{p}\Gamma/\Gamma \simeq \mathbb{F}_p^N$, that is, by a linear code over $\mathbb{F}_p$. In this way we obtain an injective mapping $\pi \mapsto C = C(\pi)$ from the set $\mathcal{S}$ of all isomorphism classes of symplectic spreads π of $W = \mathbb{F}_p^6$ to the set $\mathcal{C}$ of all equivalence classes of self-dual codes C of length p^3+1 over $\mathbb{F}_p$. Moreover, $\mathrm{Aut}(C(\pi)) = \mathrm{Aut}(\pi)/C_{(p-1)/2}$. Observe that the definition of $\mathrm{Aut}(\pi)$ used in this paper differs from the one given in [SchT]. In particular, the central subgroup $C_{(p-1)/2}$ of $\mathrm{Aut}(\pi)$ acts trivially on every vector $v(L)$, hence on $C(\pi)$.

Now we turn to the case $n \geq 5$ and n is odd. Let

$$\pi = \{W_i \mid 1 \leq i \leq p^n + 1\}$$

be a symplectic spread of $W = \mathbb{F}_p^{2n}$. Set

$$v_i = v(W_i), \quad \Gamma = \Delta(\pi) = \langle v_i \mid 1 \le i \le p^n + 1 \rangle_{\mathbb{Z}}.$$

For brevity we denote $\ell = (n-1)/2$. Then

$$\Gamma \subset \Delta = \Delta^{\#} \subset \Gamma^{\#} = p^{-\ell}\Gamma.$$

For each j, $1 \le j \le \ell+1$, one can view $H_j = p^{j-1}\Gamma^{\#}/p^j\Gamma^{\#}$ as standard orthogonal space over $\mathbb{F}_p$, with the basis $(p^{j-1-\ell}v_i \mid 1 \le i \le p^n+1)$ and with the form $(x,y)_{(j)} = p^{\ell+2-2j}(x,y) \bmod p$. (Here and below, we identify the coset $x + p^j\Gamma^{\#}$ with x.) Clearly, the H_j's are isometric to each other, and so one can identify them canonically with $H = H_{\ell+1}$. Keeping this identification in mind, we can view every factor-group

$$C_j = ((\Delta \cap p^{j-1}\Gamma^{\#}) + p^j\Gamma^{\#})/p^j\Gamma^{\#}$$

as a linear code of length p^n+1 over $\mathbb{F}_p$, with the ambient space H. It is obvious that $C_1 \subseteq C_2 \subseteq \ldots \subseteq C_\ell$. One shows that $C_j^{\perp} = C_{\ell+1-j}$ for $1 \le j \le \ell$. In particular, C_j is self-orthogonal if $1 \le j \le (\ell+1)/2$; and $C_{(n+1)/4}$ is self-dual if $n \equiv 3 \bmod 4$.

Now we take π to be the standard symplectic spread π_D. Then the same arguments as in the proof of Proposition 4.6 [SchT] assure that *all the codes C_j, $1 \le j \le \ell$, are among the $GL_2(q)$-codes having a $\mathbb{F}_p$-form, which have been introduced by Ward in* [Ward 2]. (Actually, Ward uses an irreducible representation of $H = GL_2(q)$ with kernel $T = C_{(q-1)/2}$, where $q = p^n$. But $H/T \simeq R/K$, where $R = SL_2(q)\cdot C_{p-1}$ and $K = R \cap T \simeq C_{(p-1)/2}$, cf. page 1 of the proof of Proposition 2.3. Now Ward's representation coincides with the action of R/K on Δ.) He has shown that the lattice of his $GL_2(q)$-codes is inversely isomorphic to the lattice of the so-called closed subsets of $\mathbb{F}_2^n$. He has also distinguished the following analogues of Reed-Muller codes. View elements of $\mathbb{F}_2^n$ as binary words of length n and take B_w to be the set of all binary words of length n and weight $\le w$. Then B_w is closed and cyclic (in the sense of [Ward 2]), and Ward's correspondence gives us a $GL_2(q)$-code $\mathcal{C}_{n,w}$ over $\mathbb{F}_p$, $0 \le w \le n-1$. The middle code is just $\mathcal{C}_{n,(n-1)/2}$; more generally, $\mathcal{C}_{n,w}^{\perp} = \mathcal{C}_{n,n-1-w}$. We conjecture that the above codes C_j are equal to $\mathcal{C}_{n,n-2j}$ for j, $1 \le j \le \ell = (n-1)/2$. Without this conjecture, we can only give the following lower bound for the minimum of Δ which is unfortunately independent of n. A proof of the conjecture would lead to a lower bound $(p^{[n/2]}+1)/2$ instead of $(p+1)/2$.

Proposition 7.1. *Let p be any odd prime and $n \ge 2$ arbitrary. Then*

$$\max\left\{3, \frac{p+1}{2}\right\} \le \min \Delta(p,n) \le p^{[n/2]}.$$

For the proof, observe that $\Delta(p,n)$ with even n is a sublattice of $\Delta(p,n+1)$; hence it suffices to prove Theorem 7.1 for odd n. The inequality $\min \Delta(p,n) \ge 3$ has been mentioned in Theorem 1.1. Now one repeats the proof of Proposition 6.4 [SchT].

Remark 7.2. Observe that the lattices $\Delta(p,n)$, $n > 1$ odd, are unimodular lattices with *relatively short shadow*. More precisely, recall that a *characteristic vector* of a unimodular lattice Λ is any vector $w \in \Lambda$ such that $(v,w) \equiv (v,v) \bmod 2$ for all

$v \in \Lambda$, and the coset $\frac{1}{2}w + \Lambda$ is called the *shadow* of Λ in [CoS 2]. It is known that $(w,w) \equiv \operatorname{rank}\Lambda \bmod 8$ for any characteristic vector w. Define

$$e(\Lambda) = \frac{1}{8}(\operatorname{rank}\Lambda - \min\{w \mid w \text{ any characteristic vector of } \Lambda\}).$$

Clearly, $e(\Lambda) = \frac{1}{8}\operatorname{rank}\Lambda$ if and only if Λ is an even (unimodular) lattice. Elkies [Elk] has shown that $\Lambda = \mathbb{Z}^m$ is the unique unimodular lattice with $e(\Lambda) = 0$; all other lattices have $e \geq 1$. Moreover, he has described all the unimodular lattices Λ with $e(\Lambda) = 1$.

Clearly, $e(\Delta(p,1)) = 0$. We observe that $e(\Delta) = 2$, if $\Delta = \Delta(3,3)$ or $\Delta^-(5,2)$. More generally, we claim that

$$\frac{1}{8}(p^k - 1)(p^{k+1} - 1) \leq e(\Delta) \leq \frac{1}{8}p^{k+1}(p^k - 1)$$

if $\Delta := \Delta(p, 2k+1)$, which means in particular that Δ has a relatively short shadow. (For, from Theorems 5.3 and 5.8, it follows that $v(L)+u(L)$ is a characteristic vector of norm $p^k(p+1)$, L any Lagrangian. On the other hand, if w is any characteristic vector, then $(w, v(M)) \equiv 1 \bmod 2$ for any Lagrangian M. Hence, if π is a symplectic spread in $\mathbb{F}_p^{2k+1}$ and $w = \sum_{M\in\pi} a_M v(M)$, then $a_M \neq 0$. But $p^k a_M = (v(M), w) \in \mathbb{Z}$; hence $a_M \geq p^{-k}$. As a consequence, $(w,w) \geq p^{-2k}\sum_{M\in\pi}(v(M), v(M))$, and so $(w,w) \geq p^{k+1} + 1$.) Specializing $p = 3$ and $k = 1$, one gets $e(\Delta(3,3)) = 2$. Next, let $p = 5$ and $k = 2$. Then again $v(L) - u(L)$ is a characteristic vector, of norm 10, yielding $e(\Delta) \geq 2$ for $\Delta = \Delta^-(5,2)$. On the other hand, if $e(\Delta) > 2$, then $e(\Delta) = 3$ and Δ would have a (characteristic) vector of norm $26 - 3 \cdot 8 = 2$, contrary to the fact that $\min\Delta = 3$.

References

[BaV] R. Bacher and B. Venkov, Lattices and association schemes: A unimodular example without roots in dimension 28, *Annales Inst. Fourier* **45** (1995), 1163 − 1176. MR **96j:**11093

[BRW] B. Bolt, T. G. Room and G. E. Wall, On the Clifford collineation, transform and similarity groups. I, *J. Austral. Math. Soc.* **2** (1961 − 62), 60 − 79. MR **23:**A3171

[BuS] P. Buser and P. Sarnak, On the period matrix of a Riemann surface of large genus (with an Appendix by J. H. Conway and N. J. A. Sloane), *Invent. Math.* **117** (1994), 27 − 56. MR **95i:**22018

[Coh] H. Cohn, “A Classical Invitation to Algebraic Numbers and Class Fields”, Springer-Verlag, 1978. MR **80c:**12001

[Atlas] J.H. Conway et al., “An ATLAS of Finite Groups”, Oxford University Press, 1985. MR **88g:**20025

[CoS 1] J. H. Conway and N. J. A. Sloane, On lattices equivalent to their duals, *J. Number Theory* **48** (1994), 373 − 382. MR **95j:**11063

[CoS 2] J. H. Conway and N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (1990), 1319 − 1333. MR **91m:**94024

[CoT] A. M. Cohen and Pham Huu Tiep, Splitting fields for Jordan subgroups, in: ‘Finite Reductive Groups, Related Structures and Representations’, ed. by M. Cabanes, Progress in Math., vol. **141**, 1996, Birkhäuser, pp. 165 − 183. MR **98a:**20044

[DiM] F. Digne and J. Michel, “Representations of Finite Groups of Lie Type”, London Math. Soc. Student Texts **21**, Cambridge Univ. Press, 1991, 159 pp. MR **92g:**20063

[Dum] N. Dummigan, Symplectic group lattices as Mordell-Weil sublattices, *J. Number Theory* **61** (1996), 365 − 387. MR **98h:**11088

[Elk] N. Elkies, A characterization of the $\mathbf{Z}^n$ lattice, *Math. Res. Letters* **2** (1995), 321 − 326. MR **96h:**11064

[Gow] R. Gow, Even unimodular lattices associated with the Weil representation of the finite symplectic group, *J. Algebra* **122** (1989), 510 − 519. MR **90f:**20009

[GoW] R. Gow and W. Willems, On the geometry of some simple modules in characteristic 2, *J. Algebra* **195** (1997), 634–649.

[Gro] B. H. Gross, Group representations and lattices, *J. Amer. Math. Soc.* **3** (1990), 929 − 960. MR **92a:**11077

[Isa] I. M. Isaacs, Characters of solvable and symplectic groups, *Amer. J. Math.* **95** (1973), 594 − 635. MR **48:**11270

[KoT] A. I. Kostrikin and Pham Huu Tiep, "Orthogonal Decompositions and Integral Lattices", Walter de Gruyter, Berlin et al, 1994, 535 pp. MR **96f:**17001

[LiV] G. Lion and M. Vergne, "The Weil Representation, Maslov Index and Theta Series", Progress in Math. v. **6**, Birkhäuser, Boston, Mass., 1980, 337 pp. MR **81j:**58075

[NPl] G. Nebe and W. Plesken, "Finite Rational Matrix Groups", Mem. Amer. Math. Soc. **116** (1995), no. 556, 144 pp. MR **95k:**20081

[Que] H.-G. Quebbemann, Modular lattices in Euclidean spaces, *J. Number Theory* **54** (1995), 190 − 202. MR **96i:**11072

[SchHem] R. Scharlau, B. Hemkemeier, Classification of integral lattices with large class number, *Math. Comp.* **67** (1998), 737–749. MR **98g:**11042

[SchT] R. Scharlau and Pham Huu Tiep, Symplectic groups, symplectic spreads, codes and unimodular lattices, *J. Algebra* **194** (1997), 113–156. MR **98g:**20075

[Sei] G. M. Seitz, Some representations of classical groups, *J. London Math. Soc.* (2) **10** (1975), 115 − 120. MR **51:**5789

[Tiep 1] Pham Huu Tiep, Weil representations of finite symplectic groups, and Gow lattices, *Mat. Sb.* **182** (1991), no. 8, 1161 − 1183; English transl. in *Math. USSR-Sb.* **73** (1992), no. 2, 535 − 555.

[Tiep 2] Pham Huu Tiep, Globally irreducible representations of finite groups and integral lattices, *Geometriae Dedicata* **64** (1997), 85 − 123. MR **98e:**20011

[Tiep 3] Pham Huu Tiep, Globally irreducible representations of the finite symplectic group $Sp_4(q)$, *Commun. Algebra* **22** (1994), 6439 − 6457.

[Tiep 4] Pham Huu Tiep, Weil representations as globally irreducible representations, *Math. Nachr.* **184** (1997), 313 − 327. MR **98b:**20010

[TZa 1] Pham Huu Tiep and A. E. Zalesskii, Minimal characters of the finite classical groups, *Commun. Algebra* **24** (1996), 2093 – 2167. MR **97f:**20018

[TZa 2] Pham Huu Tiep and A. E. Zalesskii, Some characterizations of the Weil representations of the symplectic and unitary groups, *J. Algebra* **192** (1997), 130–165. CMP 97:13

[Ward 1] H. N. Ward, Representations of symplectic groups, *J. Algebra* **20** (1972), 182 − 195. MR **44:**4116

[Ward 2] H. N. Ward, Quadratic residue codes in their prime, *J. Algebra* **150** (1992), 87 − 100. MR **94a:**11194

[Zal] A. E. Zalesskii, Decompositions numbers modulo p of certain representations of the groups $SL_n(p^k)$, $SU_n(p^k)$, $Sp_{2n}(p^k)$, in: 'Topics in Algebra', Banach Center Publications, vol. **26**, pt. 2, Warsaw 1990, pp. 491 − 500. MR **93e:**20022

Department of Mathematics, University of Dortmund, 44221 Dortmund, Germany
E-mail address: rudolf.scharlau@mathematik.uni-dortmund.de

Department of Mathematics, Ohio State University, Columbus, Ohio 43210
Current address: Department of Mathematics, University of Florida, Gainseville, Florida 32611
E-mail address: tiep@math.ufl.edu