ISRAEL JOURNAL OF MATHEMATICS, Vol. 54, No. 3, 1986

SYMPLECTIC MODULES

BY

J. P. TIGNOL[a] AND S. A. AMITSUR[b]

[a] *Department of Mathematics, Université Catholique de Louvain, B-1348 Louvain-la-Neuve, Belgium; and* [b] *Institute of Mathematics, The Hebrew University of Jerusalem, Jerusalem 91904, Israel*

ABSTRACT

A symplectic module is a finite group with a regular antisymmetric form. The paper determines sufficient conditions for the invariants of the maximal isotropic subgroups (Lagrangians), and asymptotic values for a lower bound of a group which contains Lagrangians of all symplectic modules of a fixed order p^n. These results have application to the splitting fields of universal division algebras.

1. Introduction

In a recent paper of the authors on finite-dimensional division algebras and their splitting groups [4], we reduced that subject to problems on abelian groups with skew-symmetric forms (symplectic modules) and their maximal isotropic subgroups, see e.g. [4] theorems 4.2 and 4.4, and asymptotic values of some of the results of sections 7 and 8 of the present paper were already applied in sections 6 and 7 of [4].

The symplectic modules appeared first in connection with classification problems of differential topology, see e.g. [1, §19] and [5, §4], and their structure was easily determined (also in §4).

The main object of the present paper is the study of the maximal isotropic subgroups of a symplectic module G, known as *Lagrangian* subgroups of G. The problem of determining all Lagrangians seems to be very difficult, and in fact we give a complete answer only in the homogeneous case (Corollary 5.5), but we do get some bounds for the elementary divisors of Lagrangians (Theorems 5.5 and 7.5). These are applied to two problems: (1) To obtain a lower bound for an abelian group G_n which contains at least one Lagrangian of every symplectic module of order p^n; it is shown (Theorem 6.1) that $|G_n| \geqq p^{(n/2)\log n + cn + O(\sqrt{n})}$.

Received July 1, 1985 and in revised form October 17, 1985

(2) To get conditions for a group to be contained in two different symplectic modules (Theorem 8.2). Both results were used in [4] Corollaries 6.7 and 6.9 and Theorem 7.4.

2. Basic results

To make this paper independent we repeat some of the required definitions and review some of the basic properties needed. We shall restrict ourselves only to *finite groups.*

2.1. A skew symmetric form on a finite abelian group G is a bilinear skew form: $(\ ,\ ): G \times G \to \mathbf{Q}/\mathbf{Z}$ into the rationals mod 1 (the roots of unity).

We make correspond to this form a homomorphism $\lambda : G \to \hat{G}$, where $\hat{G} = \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$, the dual group of G, given by $\lambda(g)(\xi) = (g, \xi)$ for $g \in G$ and every $\xi \in G$. The form is *regular* if λ is an isomorphism, but since we restrict ourselves to finite groups, and to $\mathbf{Q}/\mathbf{Z}$, regularity is equivalent to injectivity of λ, i.e. $(g, G) = 0$ if and only if $g = 0$.

2.2. Let $P \subseteq G$ be a subgroup of G, we denote by $(\ ,\ )_P$ the restriction of the skew form to P, and by λ_P, the map $\lambda_P : G \to \hat{P}$ obtained by restriction of λ to P.

The group G is called a *symplectic* ($\mathbf{Z}$-) *module* if the skew form defined on G is regular. A subgroup P is a *regular* subgroup if the restricted form $(\ ,\ )_P$ is regular on P.

The orthogonal subgroup of P is defined by $P^{\perp} = \{g \in G; (g, P) = 0\}$, i.e., $P^{\perp} = \mathrm{Ker}\,\lambda_P$.

For subgroups P of G we show:

PROPOSITION. *If G is a symplectic module and $P \subseteq G$ then*
(1) $|P|\,|P^{\perp}| = |G|$ *and* $P^{\perp\perp} = P$;
(2) *if P is regular then $P^{\perp}$ is also regular, $G = P \oplus P^{\perp}$ and*

$$(p_1 + q_1, p_2 + q_2) = (p_1, p_2) + (q_1, q_2) \qquad \textit{for } p_i \in P, \quad q_i \in P^{\perp}.$$

PROOF. Let $\hat{P}$ be the dual of P, then the map $\lambda_P : G \to \hat{P}$ is surjective. Indeed, any character on P can be extended to a character on G, and since G is symplectic, this can be realized by an element $g \in G$, i.e. $\lambda_P(g)(p) = (g, p)$ for every $p \in P$, which means that λ_P is surjective. Clearly, by definition, $\mathrm{Ker}\,\lambda_P = P^{\perp}$; hence $|G| = |P^{\perp}|\,|\hat{P}| = |P^{\perp}|\,|P|$. Finally, $P^{\perp\perp} \supseteq P$, and from the first part we conclude that $|P^{\perp\perp}| = |G|\,|P^{\perp}|^{-1} = |P|$, hence $P^{\perp\perp} = P$.

The second part is well known (e.g., [5] lemma 1), and we repeat the proof: Let $g \in G$, $\lambda_P(g) \in \hat{P}$ and since P is regular there exists $p \in P$ such that $\lambda_P(g) = \lambda_P(p)$, i.e. $\lambda_P(g-p) = 0$, which means that $g - p \in P^\perp$ and that $G = P + P^\perp$. Also if $p \in P \cap P^\perp$, then $\lambda_P(p) = 0$ and since P is regular, $p = 0$, i.e. $G = P \oplus P^\perp$.

Now $P^\perp$ is regular: for any $\chi : P^\perp \to \mathbf{Q}/\mathbf{Z}$ can be extended to a character of G by setting $\chi(P) = 0$. Since G is regular, there is a $g \in G$ such that $\chi(h) = (g, h)$ for $h \in G$. But $\chi(P) = 0$ implies that $g \in P^\perp$, which means that $P^\perp$ is regular.

We refer to a decomposition $G = P_1 \oplus \cdots \oplus P_r$ as an *orthogonal decomposition* if $P_i \subseteq P_j^\perp$ for all $j \neq i$.

2.3. A subgroup $K \subseteq G$ is *isotropic* if $K^\perp \supseteq K$, i.e. $(K, K) = 0$, and it is *Lagrangian* if it is maximal isotropic, equivalently $K^\perp = K$, since otherwise the subgroup generated by K and an element of $K^\perp$ is also isotropic.

PROPOSITION. *The Sylow subgroups $G^{(p)}$ of G are regular subgroups, and $G = \bigoplus G^{(p)}$ is an orthogonal decomposition. Moreover, K is Lagrangian in G if and only $K = \bigoplus K^{(p)}$ and each $K^{(p)} = K \cap G^{(p)}$ is Lagrangian in $G^{(p)}$ for all p.*

Indeed, if $g \in G^{(p)}$ and $h \in G$ is of order m, with $(m, p) = 1$, then let $1 = rp^\alpha + sm$, $(g, h) = (rp^\alpha + sm)(g, h) = r(p^\alpha g, h) + s(g, mh) = 0$. Hence $G^{(p)\perp}$ contains all elements of order relative prime to p, which in the abelian case form a subgroup $G^{(p)'}$, and $|G^{(p)'}| = |G| \cdot |G^{(p)}|$. One then readily shows that $G = G^{(p)} \oplus G^{(p)'}$, and by the earlier observation the sum is orthogonal. The rest of the proof follows now by standard computations.

3. Lagrangian submodules

We begin with a few elementary properties of Lagrangian submodules of a symplectic module G.

3.1. PROPOSITION. *A submodule $H \subseteq G$ is Lagrangian if and only if the following sequence is exact:*

$$0 \longrightarrow H \xrightarrow{i_H} G \xrightarrow{\lambda_H} \hat{H} \longrightarrow 0 \tag{3.1.1}$$

where i_H is the injection, and λ_H the induced map by the skew form of G.

PROOF. If H is isotropic, then $(h, H) = \lambda_h(H) = 0$ for $h \in H$, and hence $\operatorname{Ker} \lambda_H \supseteq H$. The map λ_H is also onto, since the sequence $0 \to H \to G$ yields the surjection $\hat{G} \to \hat{H} \to 0$, and λ_H is the product $G \xrightarrow{\lambda} \hat{G} \to \hat{H}$, and therefore it is also a projection. If $g \in \operatorname{Ker} \lambda_H$ then $(g, H) = 0$ and the maximality of H implies that $g \in H$ which proves the exactness. The rest of the proof is clear.

Immediate corollaries of the exactness of (3.1) are:

Corollary. (a) *If H is Lagrangian in G, then $|G| = |H|^2$ and*

$$\operatorname{rk} H \leqq \operatorname{rk} G \leqq 2 \operatorname{rk} H.$$

(b) *If H is isotropic and $|G| = |H|^2$, then H is Lagrangian.*

The result (a) is immediate, and for (b) we note that since H is isotropic the sequence of (3.1.1) is a zero sequence, and $|G| = |H|^2 = |H| \cdot |\hat{H}|$ yield that it is exact.

Later we shall see in §8 that the inequality of the corollary cannot be improved.

3.2. The following will be needed later:

Lemma. (a) *Let H be Lagrangian in G and $M \supseteq H$, then $M \supseteq H \supseteq M^{\perp}$ and the form of G induces a regular skew form on $M/M^{\perp}$ in which $H/M^{\perp}$ is Lagrangian.*

(b) *If $G = P_1 \oplus P_2$ is an orthogonal decomposition into regular submodules of G, and H is Lagrangian in G, $H \cap P_1$ is Lagrangian in P_1 then $H \cap P_2$ is Lagrangian in P_2.*

Proof. Since $M \subseteq H$, $H = H^{\perp} \supseteq M^{\perp}$, and in $\bar{M} = M/M^{\perp}$ define the form $(\bar{p}, \bar{q}) = (p, q)$ for all $p, q \in M$ and where $\bar{p}, \bar{q}$ denote their class in $\bar{M}$. The proof of (a) is then straightforward.

To prove (b), we note that if $h \in H$ and $h = p_1 + p_2$, $p_i \in P_i$. Then

$$0 = (h, H \cap P_1) = (p_1, H \cap P_1) + (p_2, H \cap P_1) = (p_1, H \cap P_1)$$

since $p_2 \in P_1^{\perp}$, but $H \cap P_1$ is Lagrangian in P_1, hence $p_1 \in H \cap P_1$. Consequently $p_2 = h - p_1 \in H \cap P_2$, and thus $H = (H \cap P_1) \oplus (H \cap P_2)$. Clearly $H \cap P_2$ is isotropic and its maximality follows by computing the order of $|H \cap P_2|$ and applying the preceding corollary.

3.3. An attempt at determining the Lagrangian of a symplectic module G will be made in the last section, but at this stage we can give some sufficient conditions.

PROPOSITION. *If H and K are two Lagrangians of G, then $H/(H\cap K)\cong K/(H\cap K)$; namely, both are extensions of the same group by $H\cap K$.*

PROOF. Since H,K are Lagrangians in G, we have two exact sequences.

$$(3.3.1)\qquad 0\longrightarrow K\xrightarrow{i_K} G\xrightarrow{\lambda_K}\hat{K}\longrightarrow 0,\qquad 0\longrightarrow H\xrightarrow{i_H} G\xrightarrow{\lambda_H}\hat{H}\longrightarrow 0.$$

Consider the map $\varphi=\lambda_H i_K$, then clearly $\operatorname{Ker}\varphi=K\cap H$. Now

$$\varphi(K)=\{\hat{h}\in\hat{H};\exists k\in K,(k,\eta)=\hat{h}(\eta)\text{ for every }\eta\in H\}.$$

Since K is isotropic and $K\supseteq K\cap H$, we have $(K,K\cap H)=0$ and, therefore,

$$\varphi(K)\subseteq\lambda_H(K\cap H)^{\perp}=\{\hat{h}\in\hat{H};\hat{h}(K\cap H)=0\}\subseteq\hat{H}.$$

Consider $\lambda_H(K\cap H)^{\perp}$ $(\subseteq\hat{H})$, and we show that it is isomorphic with $(H/H\cap K)$. Indeed, these are the characters of $\hat{H}$ which vanish on $H\cap K$, and as such they can be identified naturally with a subgroup of $(\widehat{H/H\cap K})$. Moreover, any element of $(\widehat{H/H\cap K})$ can be extended to H and vanishes on $H\cap K$ and therefore will belong to $\lambda_H(K\cap H)^{\perp}$. Hence,

$$|\lambda_H(K\cap H)^{\perp}|=|\widehat{H/(K\cap H)}|=|H/(K\cap H)|\geqq|\varphi(K)|.$$

But $|H/(K\cap H)|=|K/(K\cap H)|=|K/\operatorname{Ker}\varphi|=|\varphi(K)|$. Hence we have the equality, from which it follows that $\varphi(K)\cong H/(H\cap K)\cong H/(H\cap K)$ and thus φ induces the isomorphism $K/(H\cap K)\cong H/(H\cap K)$.

Note that this isomorphism is not canonical since it is a composition in which one of the maps is between an abelian group and its dual, which is not canonical.

4. Constructions

Given a finite abelian group H, it is easy to construct a symplectic module, denoted by $S_1(H)$ in which H is Lagrangian.

Let $\hat{H}$ be the dual group of H and consider $S_1(H)=H\oplus\hat{H}$. In $S_1(H)$ we define a bilinear form:

$$(h_1+\varphi_1,h_2+\varphi_2)=\varphi_1(h_2)-\varphi_2(h_1);\qquad h_i\in H,\quad\varphi_i\in\hat{H}.$$

4.1. THEOREM. *$S_1(H)$ is a symplectic module and H is Lagrangian in $S_1(H)$; conversely if G is a symplectic module then $G\cong S_1(H)$ for some Lagrangian submodule H, and the isomorphism is an isometry.*

The proof of the first part is immediate. The second part is well known ([1],[5]), and for completeness we indicate the proof:

Let G be of exponent m, and let $g \in G$ be an element of order m, then $\hat{G} = (g) \oplus G_1$. We then have $\hat{g} \in \hat{G}$ which satisfies $\hat{g}(g) = 1/m$, $\hat{g}(G_1) = 0$; since G is regular, let $g' \in G$ such that $(g', \eta) = \hat{g}(\eta)$ for all $\eta \in G$. One easily shows that $(g) \oplus (g') = G_0$ is a regular subgroup of G, with (g) a Lagrangian subgroup. Hence by Proposition 2.2, $G = G_0 \oplus G_0^\perp$ and the rest of the proof follows easily by induction by showing $G_0^\perp = S_1(H_0)$ and $G = S_1(H_0 + (g))$.

An immediate consequence is:

COROLLARY. *A finite abelian group G can be defined to be a symplectic module if and only if* rk *G is even, and its elementary divisors appear in pairs. Moreover, if G, G' are two symplectic modules which are isomorphic as groups, then there is an isometric isomorphism between them.*

The first part of the theorem follows from the theorem, since $G \cong S_1(H) = H \oplus \hat{H} \cong H \oplus H$ and so $\operatorname{rk} G = 2\operatorname{rk} H$. Conversely, if G has even rank, with elementary divisors which appear in pairs, then $G \cong H \oplus H$ for a subgroup H whose elementary divisors take one of each of G's, and finally $G \cong H \oplus \hat{H} = S_1(H)$ and the isomorphism can be used to turn G into a symplectic module.

The second part follows from the fact that if $G \cong G'$ and $G \cong S_1(H)$, $G' \cong S_1(H')$, where the last two are isometric maps. Then clearly $H \cong H'$ and this isomorphism can be extended to an isometry between $S_1(H)$ and $S_1(H')$ as required.

4.2. A description of all Lagrangians of $S_1(H) = G$, which is complementary to Proposition 3.3, is the following:

Let $Q \subseteq H$ be a given subgroup of H, and let $\Psi : Q \times Q \to \mathbf{Q}/\mathbf{Z}$ a *symmetric* bilinear form on Q (not necessarily regular), and let $P = \operatorname{Ker} \Psi = \{q \in Q, \Psi(Q, q) = 0\}$.

Consider the subset $K_\Psi \subseteq S_1(H)$, consisting of all $g = q + \varphi$, $q \in Q$, $\varphi \in \hat{H}$ such that $\varphi(\xi) = \Psi(q, \xi)$ for all $\xi \in Q$. Since $\Psi(q, P) = 0$ it follows that necessarily $\varphi \in P^\perp = \{\varphi \in \hat{H}; \varphi(P) = 0\}$. One readily observes that K_Ψ is a subgroup of $S_1(H)$, and we prove:

THEOREM. (a) *K_Ψ is Lagrangian in $S_1(H)$ and $P = K_\Psi \cap H$.*

Conversely,

(b) *If K is Lagrangian in $S_1(H)$, then there exists a subgroup $Q \subseteq K$ and a symmetric form Ψ on Q, such that $K = K_\Psi$ and $K \cap H = \operatorname{Ker} \Psi$.*

PROOF. Let $q_i + \varphi_i \in K_\Psi$, $i = 1, 2$, since Ψ is symmetric:

$$\varphi_1(q_2) = \Psi(q_1, q_2) = \Psi(q_2, q_1) = \varphi_2(q_1).$$

Hence, $(q_1 + \varphi_1, q_2 + \varphi_2) = \varphi_1(q_2) - \varphi_2(q_1) = 0$ which proves that K_Ψ is isotropic. To prove it is maximal, it suffices to show, in view of (b), Corollary 3.1, that $|K_\Psi| = |H|$. To this end, we consider the map $\varepsilon : K_\Psi \to \hat{H}$ given by $\varepsilon(g + \varphi) = \varphi$. First, we observe that $\operatorname{Ker} \varepsilon = P$. Indeed, let $q \in \operatorname{Ker} \varepsilon$, then $q + 0 \in K_\Psi$, which yields $0 = (q, Q)$, i.e. $q \in \operatorname{Ker} \varepsilon = P$. The same argument in the opposite direction leads to $\operatorname{Ker} \varepsilon \supseteq P$, and thus $\operatorname{Ker} \varepsilon = P$, and clearly $P = K_\Psi \cap H$. Next, $\operatorname{Im} \varepsilon = P^\perp$: the definition of K_Ψ implies immediately that $\operatorname{Im} \varepsilon \subseteq P^\perp$. Let $\varphi \in P^\perp \subseteq \hat{H}$, then $\varphi \mid Q$ vanishes on P so $\varphi \mid Q$ induces a well-defined character on Q/P. Since Ψ induces a regular symmetric form on Q/P, it follows that there exists $\bar{q} \in Q/P$ such that $\Psi(\bar{q}, \bar{\xi}) = \bar{\varphi}(\bar{\xi})$ for all $\xi \in Q/P$. By definition $\Psi(\bar{q}, \bar{\xi}) = \Psi(q, \xi)$ and $\bar{\varphi}(\bar{\xi}) = \varphi(\xi)$, hence $q + \varphi \in K_\Psi$. This proves that ε induces the exact sequence $0 \to P \to K_\Psi \to P^\perp \to 0$, and hence $|K| = |P||P^\perp|$. Noting that $P^\perp \cong (H/P)$, we finally obtain that $|K| = |P| = |H/P| = |H|$ as required.

Conversely, let K be Lagrangian in $S_1(H)$, then every element of K can be written $k = q + \varphi$, $q \in H$, $\varphi \in \hat{H}$. Let $Q = \varepsilon_1(K)$ where ε_1 is the projection: $S_1(H) \to H$, on the first component of $H \oplus \hat{H}$, i.e. $\varepsilon_1(q + \varphi) = q$. Let $q_i + \varphi_i \in K$, $i = 1,2$, then since K is isotropic, we have

$$(q_1 + \varphi_1, q_2 + \varphi_2) = \varphi_1(q_2) - \varphi_2(q_1) = 0.$$

We define $\Psi(q_1, q_2) = \varphi_1(q_2) = \varphi_2(q_1)$ and prove that Ψ is a well-defined symmetric form on Q (independent of φ_1 or φ_2). For, if $q_1 + \varphi_1$ and $q_1 + \varphi_1' \in K$, then $k = \varphi_1 - \varphi_1' \in K$, hence for every $q \in Q$, we have $q + k \in K$ and by the isotropy of K, we have

$$0 = (q + k, \varphi_1 - \varphi_1') = -\varphi_1(q) + \varphi_1'(q),$$

which proves that $\Psi(q_1, q_2)$ is independent of φ_1. Clearly the definition also implies that Ψ is symmetric.

To prove that $K \cap H = \operatorname{Ker} \Psi$, let $q \in \operatorname{Ker} \Psi$, then $q + \varphi \in K$ for some $\varphi \in \hat{H}$, for every $\xi \in Q$ there exists $\xi + \rho \in K$, and hence $\Psi(q, \xi) = \varphi(\xi) = 0$, i.e. $\varphi \in Q^\perp$. But then in $S_1(H)$, $(0 + \varphi, \xi + \rho) = \varphi(\xi) = 0$, so $\varphi \in K^\perp = K$. Consequently $q = q + \varphi - \varphi \in K$, and this proves that $\operatorname{Ker} \Psi \subseteq K \cap H$. Conversely, if $q \in K \cap H$ then for any $\xi + \rho \in K$, $(q, \xi + \rho) = 0$ since K is isotropic, but $(q, \xi + \rho) = -\rho(q) = \Psi(q, \xi) = 0$, i.e. $q \in \operatorname{Ker} \Psi$.

Finally, $K = K_\Psi$ because for every $q + \varphi \in K$ and $\xi + \rho \in K$, $0 = (q + \varphi, \xi + \rho)$ we have $\rho(q) = \varphi(\xi) = \Psi(q, \xi)$ as required.

Remark. The previous method shows how to construct Lagrangians $K \subseteq S_1(H)$, and one such that $K \cap H$ is a prescribed subgroup $P \subseteq H$. To this end one has to find a subgroup $Q \subset H$ for which one can find a symmetric regular form on Q/P. If this is possible, then the form induces a symmetrical form on Q and apply the previous result.

Unfortunately, the last result gives very little information on the structure of the various Lagrangians of $S_1(H)$, and in particular their elementary divisors which are the major tool in the applications in [4]. We turn to two different methods to obtain such information:

5. Almost homogeneous symplectic modules

In view of Proposition 2.2 we can focus our attention on abelian p-groups. We use the following notation: Let $K = (k_1) \oplus \cdots \oplus (k_2)$ be the decomposition of K into cyclic p-groups in which (k_i) is cyclic of order p^{f_i}; we arrange them in the order $f_1 \geqq f_2 \geqq \cdots \geqq f_r$; the integers p^{f_i} are the elementary divisors of K. We shall deal with the ordered set $(f_1, f_2, \ldots, f_r)$ and refer to them as the invariants of K and write $\operatorname{inv}(K) = (f_1, f_2, \ldots, f_r)$. Often we allow one to increase the number of invariants by adding zeros, which is equivalent to adding generators $k_j = 1$, which generates the trivial group.

5.1. If $K = (k_1) \oplus \cdots \oplus (k_r)$ we shall denote by $\{\hat{k}_j\}$ the dual generators of $\hat{K}$, where $\hat{k}_i$ is given by $\hat{k}_i(k_j) = \delta_{ij} p^{-f_i}$. If G is a p-symplectic module, then by 4.1 its invariants come in pairs, and we shall write its invariant set as $\operatorname{inv} G = 2(e_1, \ldots, e_r)$. Note that if $G = S_1(H)$ then $\operatorname{inv} H = (e_1, e_2, \ldots, e_r)$.

Remark. We quote a well-known result which will be used in the context: If $\operatorname{inv} G = (f_1, \ldots, f_r)$ then the invariants of subgroups and of homomorphic images are not greater than the respective invariants of K.

5.2. Denote $G_m = \{g \in G ; p^m g = 0\}$.

Proposition. *Let G be a p-symplectic module with invariants* $\operatorname{inv} G = 2(e_1, e_2, \ldots, e_r)$, *then*:

(a) $\operatorname{inv} G_m = 2(m, m, \ldots, m, e_{j+1}, \ldots, e_r)$ *where* $e_j > m \geqq e_{j+1}$.

(b) $\operatorname{inv} p^m G = 2(e_1 - m, \ldots, e_j - m, 0, \ldots, 0)$.

(c) *If* $G_m \supseteq p^s G$ *then* $\operatorname{inv}(G_m / p^s G) = \operatorname{inv} G_m - \operatorname{inv} p^s G$ *as vectors.*

(d) $G_m^\perp = p^m G$; $(p^m G)^\perp = G_m$.

Proof. Let $\{g_\lambda\}$ be a set of independent generators of G, then $\{p^m g_\lambda\}$ is a set of such generators of $p^m G$, and $\{p^{e_\lambda - m} g_\lambda\}$ for $e_\lambda > m$ is a set of independent generators of G_m. This readily proves (a), (b) and (c).

To prove (d), we consider the equality $(p^m g, G) = (g, p^m G)$, for $g \in G$, hence $(g, p^m G) = 0$ if and only if $p^m g = 0$. Hence $(p^m G)^\perp = G_m$.

Taking the orthogonal of both sides of the preceding equality, we get $(p^m G)^{\perp\perp} = G_m^\perp$, hence $G_m^\perp = p^m G$ by Proposition 2.2(1).

5.3. Let G be a symplectic module with $\operatorname{inv} G = 2(e_1, \dots, e_r)$ ($\operatorname{rk} G = 2r$), and let K be a Lagrangian submodule of G. If $\operatorname{rk} K = s$ then by Corollary 3.1, $s \leqq 2r$, so we henceforth write $\operatorname{inv} K = (f_1, f_2, \dots, f_{2r})$, $f_1 \geqq \cdots \geqq f_{2r}$ and set $f_j = 0$ for all $j > s$.

LEMMA. $e_1 \geqq f_1$; $G_{f_1} \supseteq K \supseteq p^{f_1} G$; $p^{f_{2r}} G \supseteq K \supseteq G_{f_{2r}}$.

PROOF. $e_1 \geqq f_1$ since e_1 is the exponent of G and f_1 the exponent of a subgroup.

Next, $p^{f_1} K = 0$, i.e. $K \subseteq G_{f_1}$ and passing to the orthogonal of these groups, we obtain $K = K^\perp \supseteq G_{f_1}^\perp \supseteq p^{f_1} G$ by (5.2).

The last relation is trivial if $f_{2r} = 0$, so assume $f_{2r} > 0$. In this case, $K \cap G_{f_{2r}} = K_{f_{2r}}$ is a homogeneous abelian group of rank $2r$ and exponent $p^{f_{2r}}$. This is also true for $G_{f_{2r}}$ since $e_r \geqq f_{2r}$ by the remark of 5.1. Since $K_{f_{2r}} \subseteq G_{f_{2r}}$, we must have equality, which yields $K \supseteq G_{f_{2r}}$. Passing to the orthogonal we obtain, as before, $p^{f_{2r}} G \supseteq K$.

COROLLARY. $f_1 + f_{2i} \geqq e_i \geqq f_{2i-1} + f_{2r}$, $i = 1, 2, \dots, r$.

Indeed, from (5.2) we have

$$\operatorname{inv} p^{f_{2r}} G = (e_1 - f_{2r}, e_1 - f_{2r}, \dots, e_r - f_{2r}, e_r - f_{2r}),$$

then by Remark 5.1, the relation $p^{f_{2r}} G \supseteq K$ yields $f_{2i-1} \leqq e_i - f_{2r}$. Similarly, the relation $K \supseteq p^{f_1} G$ yields $f_{2i} \geqq e_i - f_1$.

The last result yields a classification of all Lagrangians of symplectic modules of rk 2 and rk 4:

PROPOSITION. (1) *If G is symplectic and* $\operatorname{inv} G = 2(e_1)$ *then K is Lagrangian in G if and only if* $\operatorname{inv} K = (f_1, f_2)$ *with* $f_1 + f_2 = e_1$.

(2) *Let* $\operatorname{inv} G = 2(e_1, e_2)$ *and* $\operatorname{inv} K = (f_1, f_2, f_3, f_4)$ *then K is Lagrangian in G if and only if*

$$f_1 + f_2 + f_3 + f_4 = e_1 + e_2, \qquad f_1 + f_2 \geqq e_1 \geqq f_1 + f_4 \geqq e_2.$$

PROOF. For the first part, it follows immediately from the lemma and its corollary that necessarily $f_1 + f_2 = e_1$. The existence of Lagrangians with invariant (f_1, f_2) was shown in the proof of 5.2.

The "only if" part of (2) follows from the lemma and its corollary. The group $K \subseteq S_1(H) = G$ which is Lagrangian with the required invariant is the following: Let $H = (h_1) \oplus (h_2)$, then K is generated by:

$$k_1 = p^{e_1 - f_1} h_1 - p^{f_4} h_2, \qquad k_2 = p^{e_1 - f_2} \hat{h}_1 + p^{f_3} \hat{h}_2,$$
$$k_3 = p^{e_2 - f_3} h_2, \qquad k_4 = p^{e_2 - f_4} \hat{h}_2.$$

(Note that $e_2 \geqq f_3$ and even $e_2 \geqq f_3 + f_4$ follows from the equality and inequality hypothesis of (2) of the proposition.)

5.4. The following is fundamental for an induction process to be used in proving the main result of this section:

Lemma. *Let $h \in K \cap p^{e_1 - f_1} G$ be of maximal exponent p^{f_1}, then there exists f_j $j \neq 1$, such that $e_1 = f_1 + f_j$; and there exists an orthogonal decomposition $G = G_1 \oplus G_2$ with the following properties: G_i are regular submodules,* $\operatorname{inv} G_1 = 2(e_1)$, $\operatorname{inv} G_2 = 2(e_2, \ldots, e_r)$; *$K_i = K \cap G_i$ is Lagrangian in G_i and* $\operatorname{inv} K_1 = (f_1, f_j)$, $\operatorname{inv} K_2 = (\hat{f}_1, f_2, \ldots, \hat{f}_j, \ldots, f_{2r})$ *(where $\hat{f}$ means f is omitted).*

Proof. Let $h = p^{e_1 - f_1} g$ and as h is of order p^{f_1}, g must be of order e_1. G is symplectic so there is $g' \in G$ such that $(g, g') = p^{-e_1}$, hence $(g) \oplus (g') = G_1$ is readily shown to be a direct sum and a regular submodule. It follows now by Proposition 2.2 that $G = G_1 \oplus G_2$, with G_i regular submodules. Let $h' = p^{f_1} g' \in p^{f_1} G'$ which is also an element of K by the lemma of 5.3. Moreover, h' must be of order $p^{e_1 - f_1}$ and thus $(h) \oplus (h') \subseteq K \cap G_1$ is an isotropic submodule of order $p^{f_1 + (e_1 - f_1)} = p^{e_1}$. Consequently $K \cap G_1 = (h) \oplus (h')$ and it is Lagrangian in G_1 by Corollary 3.1. Apply Lemma 3.2 and we have $K = (K \cap G_1) \oplus (K \cap G_2)$ and $K \cap G_2$ is Lagrangian in G_2. The invariants of K are uniquely determined and are equal to $\operatorname{inv}(K \cap G_1) \cup \operatorname{inv}(K \cap G_2)$, and since $\operatorname{inv}(K \cap G_1) = (f_1, e_1 - f_1)$ there exists f_j such that $e_1 - f_1 = f_j$. The rest of the lemma follows now easily.

5.5. A symplectic module G will be said to be almost homogeneous if $\operatorname{inv} G = 2(e_1, e, \ldots, e)$ where $e_1 \geqq e$: i.e. all its invariants are equal with the possible exception of the first invariant e_1.

Our main result in this section is:

Theorem. *If G is almost homogeneous and K Lagrangian in G with* $\operatorname{inv} K = (f_1, f_2, \ldots, f_{2r})$ *then for* $k = 1, 2, \ldots, r$

$$e_1 \geqq f_k + f_{2r-k+1} \geqq e.$$

Remark. Since $|K|^2 = p^{2(f_1 + \cdots + f_{2r})}$, it follows that $\Sigma f_i = e_1 + (r-1)e$ and, therefore, we can have at most $e_1 - e$ inequalities $f_k + f_{2r-k+1} > e$.

In the proof we will show simultaneously:

COROLLARY. *If G is almost homogeneous (as in the preceding theorem) and $e_1 = e$ or $e_1 = e + 1$ then there is an orthogonal decomposition $G = G_1 \oplus \cdots \oplus G_r$ with* $\operatorname{inv} G_1 = 2(e_1)$, $\operatorname{inv} G_i = 2(e)$, *and a decomposition $K = K_1 \oplus \cdots \oplus K_r$, where $K_i = K \cap G_i$ is Lagrangian in G_i. Furthermore,* $\operatorname{inv} K_i = (f_{\lambda_i}, f_{\mu_i})$, *$\lambda_i > \mu_i$ and $e_1 = f_{\lambda_1} + f_{\mu_1}$ $(\lambda_1 = 1)$, $e = f_{\lambda_i} + f_{\mu_i}$ for $i > 1$.*

Let $c = e_1 - e$; we prove both results by induction on the pairs (r, c) arranged lexicographically. The case $r = 1$ (and necessarily $e_1 = e$) is simple, since $\operatorname{rk} K \leqq 2$ by Corollary 3.1, $\operatorname{inv}(K) = (f_1, f_2)$; and as $|K|^2 = |G|$ it follows that $f_1 + f_2 = e_1$ $(= e)$.

Assume $r > 1$, then we have from Corollary 5.3 that $f_1 + f_{2r} \leqq e_1$ and $K \subseteq p^{f_{2r}}G$ by 5.3. Consider first the case that $f_1 + f_{2r} = e_1$, and choose $h \in K$ of maximal order; then we have $h \in p^{f_{2r}}G = p^{e_1 - f_1}G$ and we can apply Lemma 5.4 to conclude that $G = G_1 \oplus G_2$, and $\operatorname{inv}(K \cap G_1) = (f_1, f_j)$, $f_1 + f_j = e_1$.

The main lemma 5.4 yields also that $K = (K \cap G_1) \oplus (K \cap G_2)$, $K \cap G_2$ is Lagrangian in G_2, and $\operatorname{inv} G_2 = 2(e, \ldots, e)$. We apply now the induction on G_2 whose rank is $2(r-1)$, and prove both the theorem and the corollary.

Next we assume that $f_1 + f_{2r} < e_1$, and that $e_1 - e = c \geqq 2$:

We notice that the relation $G_{f_1} \supseteq K \supseteq p^{f_1}G$ yields $G_{e_1 - 1} \supseteq K \supseteq p^{e_1 - 1}G$ since $f_1 \leqq e_1 - 1$. We apply the relation $p^{e_1 - 1}G = (G_{e_1 - 1})^{\perp}$ to (a) of Lemma 3.2 and obtain that $K / p^{e_1 - 1}G$ is Lagrangian in $G_{e_1 - 1} / p^{e_1 - 1}G$. Now by Proposition 5.2,

$$\operatorname{inv}(G_{e_1 - 1} / p^{e_1 - 1}G) = 2(e_1 - 1, e, \ldots, e) - 2(1, 0, \ldots) = 2(e_1 - 2, e, \ldots, e).$$

Induction can be applied to these groups, since $e_1 - 2 \geqq e$ and $(e_1 - 2) - e < e_1 - e$ by assumption. Let $\operatorname{inv}(K / p^{e_1 - 1}G) = (f'_1, \ldots, f'_{2r})$; by Remark 5.1, $f_i \geqq f'_i$, and thus

$$f_k + f_{2r-k+1} \geqq f'_k + f'_{2r-k+1} \geqq e.$$

To prove that $f_k + f_{2r-k+1} \leqq e_1$ we note that $\Sigma f_k = \Sigma f'_k + 2$ from the equality

$$|K| = |K / p^{e_1 - 1}G| \, |p^{e_1 - 1}G|$$

and therefore $\Sigma (f_k - f'_k) = 2$. Thus

$$f_k + f_{2r-k+1} = (f_k - f'_k) + (f_{2r-k+1} - f'_{2r-k+1}) + f'_k + f'_{2r-k+1} \leqq 2 + (e_1 - 2) = e_1$$

and the proof is completed.

Finally, we have to consider the case $e_1 - e = 0, 1$:

Corollary 5.3 yields $e_1 \geqq f_1 + f_{2r} \geqq e$, hence either $f_1 + f_{2r} = e_1$ or $f_1 + f_{2r} = e$. In case $f_{2r} = e_1 - f_1$, we are in the first case of our proof which was carried out in the beginning. We are thus left with the case $f_1 + f_{2r} = e$, and $e_1 = e + 1$.

Let $h \in K \subseteq p^{f_{2r}}G$ of the form $h = p^{f_{2r}}g$ and h be of order p^{f_1}. Consider two cases: (1) $g \in pG$, (2) $g \not\in pG$. In the first case $h \in p^{f_{2r}+1}G$ and $f_{2r} + 1 = e - f_1 + 1 = e_1 - f_1$ and we are again in the situation $h \in p^{e_1 - f_1}G$ which was dealt with in the beginning. Finally, we assume $g \not\in pG$; if $p^{e-1}g \in p^e G$ then $p^{e-1}g = p^e g'$ and so $g - pg' \in G_{e-1}$. Our group G is almost homogeneous, then necessarily $G_{e-1} \subseteq pG$ and therefore $g - pg' \in pG$ so $g \in pG$ which contradicts our case. Hence, $p^{e-1}g \not\in p^e G$ and consequently, $G_e = (p^e G)^\perp \not\subseteq (p^{e-1}g)^\perp$, or else $G_e^\perp = p^e G \supseteq (p^{e-1}g)^{\perp\perp} \ni p^{e-1}g$, a contradiction. We have therefore $g' \in G_e$ with $(g', p^{e-1}g) \neq 0$; and hence g' must be of order p^e exactly. Moreover $(g', g) = p^{-e}d$ for some $d \not\equiv 0 (\mathrm{mod}\ p)$.

Consider now the group $G_1 = (g) \oplus (g')$ where the sum must be a direct sum; it is a regular subgroup with $\mathrm{inv}\, G_1 = 2(e)$. Furthermore, the chosen element $h = p^{f_{2r}}g$ has order $e - f_{2r}$, which is equal to f_1 by assumption and $h' = p^{f_1}g' \in p^{f_1}G \subseteq K$ will generate a Lagrangian $(h) \oplus (h')$ in $K \cap G_1$, with $\mathrm{inv}(K \cap G_1) = (f_1, e - f_1) = (f_1, f_{2r})$. At last we apply (b) of Lemma 3.2 and obtain $K = (K \cap G_1) \oplus (K \cap G_2)$, $K \cap G_2$ is Lagrangian in G_2 whose rank is $2(r - 1)$ and $\mathrm{inv}(G_2) = 2(e_1, e, \ldots, e)$. The rest will follow now by straightforward induction, which proves both the theorem and the corollary.

6. Bound for a universal group

We apply the previous result to give a lower bound for the order of an abelian group which contains for each symplectic module G of order $(p^n)^2$ at least one Lagrangian of G. The bound is important for applications in [4] Theorem 7.4.

6.1. As we are unable to use all symplectic modules of this order, it suffices for our purpose to confine ourselves only to almost homogeneous symplectic modules of order $(p^n)^2$.

Let $1 \leqq q \leqq n$ be an integer, then $n = c_q + [n/q]q$, $0 \leqq c_q < q$. For each q we construct the almost homogeneous symplectic module $G_q = G_1(H_q)$, where H_q is the abelian group with

$$\mathrm{inv}\, H_q = \left(c_q + \left[\frac{n}{q}\right], \left[\frac{n}{q}\right], \ldots, \left[\frac{n}{q}\right] \right)$$

and $\mathrm{rk}\, H_q = q$, so $\mathrm{rk}\, G_q = 2q$, $\mathrm{inv}\, G_q = 2\, \mathrm{inv}\, H_q$.

Let $\mathcal{G}_n = \mathcal{G}_{n,p}$ be a p-abelian group with the property:

For every symplectic p-module G of order $(p^n)^2$,

(6.1n) there exists a Lagrangian subgroup K of G, such that $K \subseteq \mathcal{G}_n$.

Note that $\operatorname{rk}\mathscr{G}_n \geqq n$. Indeed, there exists a symplectic module $G = S_1(H)$ of $\operatorname{rk} 2n$, where H is p-elementary of $\operatorname{rk} n$. Since $\mathscr{G}_n \supseteq H$, it follows that $\operatorname{rk}\mathscr{G}_n \geqq n$. We denote the first $2n$ invariants of $\mathscr{G}_n$ by $(f_1, f_2, \ldots, f_{2n})$, $f_1 \geqq \cdots \geqq f_{2n}$ where some of the last f_i may be zero.

Lemma. *$f_q + f_{q+1} \geqq [n/q]$, and hence $f_q \geqq \frac{1}{2}[n/q]$.*

Indeed, consider the symplectic module G_q defined above, and K_q its Lagrangian which is included in $\mathscr{G}_n$. Since $\operatorname{rk} K_q \leqq \operatorname{rk} G_q = 2q$ let $\operatorname{inv} K_q = (f'_1, \ldots, f'_{2q})$, with possibly $f'_{2q} \geqq 0$. By Theorem 5.5, $f'_k + f'_{2q-k+1} \geqq [n/q]$ for $k = 1, \ldots, q$, and together with Remark 5.1 we obtain for $k = q$

$$f_q + f_{q+1} \geqq f'_q + f'_{q+1} \geqq \left[\frac{n}{q}\right]$$

and since $f_q \geqq f_{q+1}$ we obtain $f_q \geqq \frac{1}{2}[n/q]$.

Let $\{\alpha\}$ denote the first integer $\geqq \alpha$ for $\alpha > 0$, then our lemma yields:

Theorem. *Let $|\mathscr{G}_n| = p^{N(n)}$, then $N(n) \geqq \Sigma_{q \leqq n} \{\frac{1}{2}[n/q]\}$.*

Indeed, $N(n) = \Sigma f_q$ and $f_q \geqq \frac{1}{2}[n/q] > 0$ for $q \leqq n$ and thus $f_q \geqq \{\frac{1}{2}[n/q]\}$ and this completes the proof.

Remark. A slightly better lower bound can be obtained from the relation $f_1 + f_2 \geqq n$, and where we do not use $f_1 \geqq \{n/2\}$ and $f_2 \geqq \{\frac{1}{2}[n/2]\}$. With this we obtain (quoted in [4] p. 141)

$$N(n) \geqq f_1 + f_2 + \sum_{q \geqq 3} f_q \geqq n + \sum_{q \geqq 3} \{\tfrac{1}{2}[n/q]\}.$$

The second lower bound is greater than the one of the theorem in $n - \{n/2\} - \{\frac{1}{2}[n/2]\}$ which one readily proves to be $[n/4]$. The proof is done by considering the various cases of $n = 4m + k$, $k = 0, 1, 2, 3$.

6.2. Next we obtain an asymptotic value for the sum $S = \Sigma_q \{\frac{1}{2}[n/q]\}$. We can write the sum for all q since for $q \geqq n$ the terms are zero:

Theorem. *$S = \Sigma_q \{\frac{1}{2}[n/q]\} = \Sigma_{j=1}^{\infty} [n/(2j-1)] = \frac{1}{2} n(\log n + 2\gamma - 1 + \log 2) + O(\sqrt{n})$, γ the Euler constant.*

Proof. For $j \geqq 1$, consider all integers q in the interval:

$$\frac{n}{2j+1} < q \leqq \frac{n}{2j-1} \qquad \text{or equivalently} \qquad 2j - 1 \leqq \frac{n}{q} < 2j + 1.$$

For these q's we have $2j - 1 \leqq [n/q] < 2j + 1$, and therefore $[n/q] = 2j - 1$ or $2j$.

Hence, $\{\frac{1}{2}[n/q]\} = j$. The number of these q's is $[n/(2j-1)] - [n/(2j+1)]$. Thus:

$$S = \sum_{j=1}^{\infty} j\left(\left[\frac{n}{2j-1}\right] - \left[\frac{n}{2j+1}\right]\right)$$
$$= \sum_{j=1}^{\infty} j\left[\frac{n}{2j-1}\right] - \sum_{j=1}^{\infty} (j+1)\left[\frac{n}{2j+1}\right] + \sum_{j=1}^{\infty}\left[\frac{n}{2j+1}\right] = \sum_{j=1}^{\infty}\left[\frac{n}{2j-1}\right].$$

To compute an asymptotic formula for the last sum, we use Dirichlet computation of $\Sigma[n/\nu] = n\log n + (2\gamma - 1)n + O(\sqrt{n})$ (e.g. [3] theorem 320):

$$\sum_j \left[\frac{n}{2j-1}\right] = \sum_{\nu}\left[\frac{n}{\nu}\right] - \sum_{\nu}\left[\frac{n}{2\nu}\right]$$
$$= [n\log n + (2\gamma-1)n] - \left[\frac{n}{2}\log\frac{n}{2} + (2\gamma-1)\frac{n}{2}\right] + O(\sqrt{n})$$

which completes the proof.

Noticing that $[n/4] = n/4 + O(1)$, we obtain from the last remark that:

Corollary. *Let* $|\mathcal{G}_n| = p^{N(n)}$, *then* $N(n) \geqq \frac{1}{2}n(\log n + 2\gamma - \frac{1}{2} + \log 2) + O(\sqrt{n})$ *and note that* $2\gamma - \frac{1}{2} + \log 2 \geqq 1.347 > 1$.

7. Relations and generators

Let G be a p-symplectic module and K a Lagrangian submodule. Let $K = (k_1) \oplus \cdots \oplus (k_r)$ be the cyclic decomposition of K, where (k_i) is cyclic of order p^{f_i}, and $\operatorname{inv} K = (f_1, \ldots, f_r)$, $f_i \geqq f_2 \geqq \cdots \geqq f_r$. We note that f_i may be zero and then the corresponding group is a trivial group.

7.1. We aim to describe $\mathcal{G}$ by a set of generators and relations using the exact sequence:

$$(*) \qquad 0 \longrightarrow K \longrightarrow G \xrightarrow{\lambda_K} \hat{K} \longrightarrow 0$$

of (3.1):

Theorem. *A symplectic module G, with a Lagrangian K whose invariants are $(f_1, f_2, \ldots, f_r)$ has a set of $2r$ generators k_i, $i = 1, \ldots, 2r$ with the relations:*

(7.1.1) (i) $p^{f_i}k_i = 0$ *for* $i = 1, 2, \ldots, r$,

(ii) $p^{f_i}k_{r+i} = \Sigma_{j=1}^{r} s_{ij}k_j$, $i = 1, \ldots, r$,

(iii) $S = (s_{ij})$ *is a skew symmetric integral matrix with* $|s_{ij}| \leqq \frac{1}{2}\min(p^{f_i}, p^{f_j})$.

The skew form on G is given by:

(iv) $(k_i, k_j) = 0$; $(k_{r+i}, k_j) = -(k_j, k_{r+i}) = \delta_{ij} p^{-f_i}$.
$(k_{r+i}, k_{r+j}) = -s_{ij} p^{-(f_i+f_j)}$ $i, j = 1, \ldots, r$.

Conversely, if G is an abelian group with the relations and generators given by (i)–(iii) *then G is a p-group, and the definition* (iv) *makes G a symplectic module with Lagrangian K generated by* $\{k_1, \ldots, k_r\}$.

Proof. Let G be symplectic, with Lagrangian $K = (k_1) \oplus \cdots \oplus (k_r)$ and let $\hat{K} = (\hat{k}_1) \oplus \cdots \oplus (\hat{k}_r)$ be its dual decomposition; then consider the exact sequence (∗) mentioned above.

Since λ_K is a surjection, let $k'_{r+i} \in G$ be inverse images of the dual base $\hat{k}_i$, i.e. $\lambda_K(k'_{r+i}) = \hat{k}_i$. Then, by definition $(k'_{r+1}, k_j) = \delta_{ij} p^{-f_i}$, and since $\hat{k}_i$ has order p^{f_i}, we have $p^{f_i} k'_{r+i} \in \operatorname{Ker} \lambda_K = K$. Hence,

$$p^{f_i} k'_{r+i} = \sum s'_{ij} k_j.$$

We have some freedom in choosing k'_{r+i}, so let $k''_{r+i} = k'_{r+i} + \Sigma_{j=1}^{r} x_{ij} k_j$ where x_{ij} will be determined later, then we have for arbitrary y_{ij} the relation

$$p^{f_i} k''_{r+i} = \sum_{j=1}^{r} (s'_{ij} + x_{ij} p^{f_i} + y_{ij} p^{f_j}) k_j, \qquad i = 1, \ldots, r$$

since $p^{f_j} k_j = 0$, and we still have $\lambda_K(k''_{r+i}) = \hat{k}_i$, since $\Sigma\, x_{ij} k_j \in K = \operatorname{Ker} \lambda_K$.

Next, we choose the integers x_{ij}, y_{ij} so that

$$s_{ij} = s'_{ij} + x_{ij} p^{f_i} + y_{ij} p^{f_i}$$

will satisfy $|s_{ij}| \leqq \frac{1}{2}\min(p^{f_i}, p^{f_j})$, which is clearly possible. Note also that if the chosen element s_{ij} satisfies $|s_{ij}| = \frac{1}{2}\min(p^{f_i}, p^{f_j})$, we do have the choice of the sign, and then we set $s_{ij} > 0$ if $i > j$ and $s_{ij} < 0$ if $i < j$. Thus we obtain (i)–(iii), except the skewness of S. Since K is isotropic we have $(k_i, k_j) = 0$, for $1 \leqq i, j \leqq r$. From the fact that $\lambda_K(k''_{r+i}) = \hat{k}_i$, we obtain two parts of (iv).

To compute (k''_{r+i}, k''_{r+j}) we observe that

$$p^{f_j}(k''_{r+i}, k''_{r+j}) = (k''_{r+i}, p^{f_j} k''_{r+j}) = \sum s_{j\lambda}(k''_{r+i}, k_\lambda) = s_{ji} p^{-f_i} (\operatorname{mod} \mathbf{Z}).$$

Hence,

$$p^{f_j}(k''_{r+i}, k''_{r+j}) - s_{ji} p^{-f_i} = m_{ji}, \qquad m_{ji} \in \mathbf{Z},$$

$$(k''_{r+i}, k''_{r+j}) = s_{ji} p^{-(f_i+f_j)} + m_{ji} p^{-f_i}.$$

The form is skew symmetric, i.e. $(k''_{r+i}, k''_{r+j}) = -(k''_{r+j}, k''_{r+i})$; we get by multiplying with $p^{f_i+f_j}$

$$s_{ij} + s_{ji} = -m_{ji}p^{f_i} - m_{ij}p^{f_j}.$$

If $|s_{ij}| = |s_{ji}| = \frac{1}{2}\min(p^{f_i}, p^{f_j})$, then we have already chosen above $s_{ij} + s_{ji} = 0$. In other cases $|s_{ij}| < \frac{1}{2}\min(p^{f_i}, p^{f_j})$ and therefore

$$|m_{ji}p^{f_i} + m_{ij}p^{f_j}| = |s_{ij} + s_{ji}| \leqq |s_{ij}| + |s_{ji}| < \min(p^{f_i}, p^{f_j})$$

implies that $s_{ij} + s_{ji} = 0$, i.e. $S = (s_{ij})$ is skew symmetric and also

$$(**) \qquad m_{ji}p^{f_i} = -m_{ij}p^{f_j}.$$

Finally we set $k_{r+i} = k''_{r+i} + \Sigma_{i \leqq \lambda} m_{\lambda i}k_\lambda$. This leads to

$$p^{f_i}k_{r+i} = \sum s_{ij}k_j + \sum_{i \leqq \lambda} m_{\lambda i}p^{f_i}k_\lambda = \sum s_{ij}k_j$$

since (**) yields that $m_{\lambda i}p^{f_i}k_\lambda = -m_{i\lambda}p^{f_\lambda}k_\lambda = 0$. Also by (**):

$$\begin{aligned}(k_{r+i}, k_{r+j}) &= \left(k''_{r+i} + \sum_\lambda m_{\lambda i}k_\lambda, k''_{r+j} + \sum_\mu m_{\mu i}k_\mu\right)\\ &= s_{ji}p^{-(f_i+f_j)} + m_{ij}p^{-f_i} - m_{ji}p^{-f_j}\\ &= s_{ji}p^{-(f_i+f_j)}. \qquad \text{q.e.d.}\end{aligned}$$

The converse of our theorem follows by straightforward computations.

7.2. The preceding result, though it determines G with the aid of K and a skew-symmetric integral matrix S, is hardly useful in dealing with problems about G, its invariants or its other Lagrangians. Nevertheless, it will suffice to give some necessary conditions for the invariants of the Lagrangians of a symplectic module of the form $S_1(H)$.

To this end we recall relations between finitely generated abelian groups given by generators and relations and integral matrices.

Let G be an abelian group generated by r elements $g_1, \ldots, g_r$. Consider the projection $\varepsilon : \mathbf{Z}^r \to G$ given by $\varepsilon(e_i) = g_i$ where e_i is the standard basis of $\mathbf{Z}^r$. It is well known that $\operatorname{Ker}\varepsilon$ is a subgroup generated by r elements $\alpha_i = \Sigma_{k=1}^r a_{ik}e_k$, $i = 1, \ldots, r$. (Note that if G is not a torsion group, some of the α_i's may be zero.) We refer to the integral matrix $A = (a_{ik}) \in \mathcal{M}_r(\mathbf{Z})$ as the *matrix of relations* (with respect to the basis $g_1, \ldots, g_r$) (e.g. [6] Ch. III, p. 117). If G is a finite group, the matrix A is regular.

7.3. Two relation matrices A, B belong to the same group if and only if they are equivalent in $\mathcal{M}_r(\mathbf{Z})$, i.e. $B = PAQ$ where P, Q are invertible matrices in $\mathcal{M}_r(\mathbf{Z})$.

REMARK. Among all equivalent matrices A there is a unique diagonal matrix $D = \operatorname{diag}(d_1, d_2, \dots, d_r)$ where $d_i \mid d_{i+1}$ $(d_i > 0)$. The *elementary divisors* d_j are determined by the condition that $D_j = d_1 d_2 \cdots d_j$ is the greatest common divisor of all $j \times j$ subdeterminants of the matrix A.

Furthermore, G is then isomorphic to a direct sum of cyclic groups of orders $d_r, d_{r-1}, \dots, d_1$ (some d_j may be 1).

If G is a finite p-group, then each d_i is a p-th power, i.e. $d_i = p^{g_i}$, $g_1 \leqq g_2 \leqq \cdots \leqq g_r$.

7.4. Let $G = S_1(H)$ be a symplectic p-module, and K be a Lagrangian submodule with $\operatorname{inv} K = (f_1, f_2, \dots, f_s)$, $f_1 \geqq f_2 \geqq \cdots \geqq f_s \geqq 1$ and let $\operatorname{inv} H = (e_1, e_2, \dots, e_r)$ with $e_1 \geqq \cdots \geqq e_r \geqq 1$.

For our matrix calculation we make the following notational changes:

NOTATIONS. Since $r = \operatorname{rk} H \leqq \operatorname{rk} K = s$ by Corollary 3.1, we add to H invariants $e_{r+1} = \cdots = e_s = 0$, thus both $\operatorname{inv} H = (e_1, e_2, \dots, e_s)$ and $\operatorname{inv} K$ will be vectors of the same length.

We also denote by p^E the diagonal matrix $\operatorname{diag}(p^{e_1}, p^{e_2}, \dots, p^{e_s})$ and similarly $p^F = (p^{f_1}, \dots, p^{f_s})$.

These conventions yield for $G = S_1(H)$ two different types of sets of generators with two possibly different relation matrices in $\mathcal{M}_{2s}(\mathbf{Z})$:

The form $G = S_1(H) = H \oplus \hat{H}$ yields $2s$ generators $\{h_i, \hat{h}_i\}$ and a relation diagonal matrix

$$\mathcal{N} = \begin{pmatrix} P^E & 0 \\ 0 & P^E \end{pmatrix}.$$

On the other hand, Theorem 7.1 gives $2s$ generators $\{k_i\}$ and the relation matrix

$$\mathcal{M} = \begin{pmatrix} P^F & 0 \\ S & P^F \end{pmatrix}.$$

These two sets of generators and their matrices will be used in proving:

7.5. THEOREM. *If K with $\operatorname{inv} K = (f_1, \dots, f_s)$ is Lagrangian in $S_1(H)$ and $\operatorname{inv}(H) = (e_1, \dots, e_s)$, then*:

(a) $e_s + e_{s-1} + \cdots + e_\mu \leqq f_s + f_{s-1} + \cdots + f_\mu$, *for* $1 \leqq \mu \leqq s$.

(b) $e_s + e_{s-1} + \cdots + e_{\mu-1} + \frac{1}{2} e_\mu \leqq f_s + f_{s-1} + \cdots + f_{\mu-1} + \frac{1}{2} f_\mu$, *for* $1 \leqq \mu \leqq s$.

(c) $f_s + \cdots + f_{2\rho+1} \leqq e_{\rho+1} + e_{\rho+2} + \cdots + e_{s-\rho}$, *for* $2\rho + 1 \leqq s$.
(d) $f_s + \cdots + f_{2\rho} \leqq e_{\rho+1} + \cdots + e_{s-\rho} + \frac{1}{2}(e_\rho + e_{s-\rho+1})$, *for* $2\rho \leqq s$.

From the equality $|H| = |K|$, we shall obtain respective inequalities.

COROLLARY. (a′) $f_1 + \cdots + f_\mu \leqq e_1 + \cdots + e_\mu$.
(b′) $f_1 + \cdots + f_{\mu-1} + \frac{1}{2}f_\mu \leqq e_1 + \cdots + e_{\mu-1} + \frac{1}{2}e_\mu$.
(c′) $f_1 + \cdots + f_{2\rho} \geqq (e_1 + \cdots + e_\rho) + (e_{s-\rho+1} + e_{s-\rho} + \cdots + e_s)$.
(d′) $f_1 + \cdots + f_{2\rho-1} \geqq (e_1 + \cdots + e_{\rho-1}) + \frac{1}{2}(e_\rho + e_{s-\rho+1}) + (e_{s-\rho} + \cdots + e_s)$.

Note that the order of G yields equality for $\mu = 1$ in (7.5a).

PROOF. The matrices of relation $\mathcal{M}, \mathcal{N}$ of 7.4 are of the same order $2s$, hence, by Remark 7.3, they have the same elementary divisors $d_j(\mathcal{M}), d_j(\mathcal{N})$. Also, the greatest common divisors $D_j(\mathcal{M})$, $D_j(\mathcal{N})$ of all $i \times j$ subdeterminants of $\mathcal{M}$ and $\mathcal{N}$ respectively are the same (when taken positive). Moreover, since G is a p-group, the elementary divisors are p-th powers, and we can restrict all our calculation to the p-th exponents of various subdeterminants we shall be considering.

Denote $D_j(\mathcal{N}) = p^{\delta_j(\mathcal{N})}$; $D_j(\mathcal{M}) = p^{\delta_j(\mathcal{M})}$.

The matrix $\mathcal{N}$ is diagonal and therefore its $j \times j$ subdeterminants are the product of j powers $p^{e_{\lambda_1}} p^{e_{\lambda_2}} \cdots p^{e_{\lambda_j}}$. Hence the g.c.d. of all these subdeterminants is the minimum product: $p^{e_s} \cdot p^{e_s} \cdot p^{e_{s-1}} \cdot \cdots$, and thus one readily observes that:

(7.5.1) For $j = 2\nu$, $\delta_{2\nu}(\mathcal{N}) = 2(e_s + \cdots + e_{s-\nu+1}) = 2\sum_{i=s-\nu+1}^{s} e_i$, $\nu = 1, 2, \ldots, s$.

For $j = 2\nu - 1$, $\delta_{2\nu-1}(\mathcal{N}) = 2(e_s + \cdots + e_{s-\nu+2}) + e_{s-\nu+1}$

$$= 2(e_s + \cdots + e_{s-\nu+1}) - e_{s-\nu+1}.$$

We have $\delta_{2\nu-1}(\mathcal{N}) = \delta_{2\nu}(\mathcal{N}) - e_{s-\nu+1} = \delta_{2(\nu-1)}(\mathcal{N}) + e_{s-\nu+1}$. We point out that $\delta_1(\mathcal{N}) = e_s$ and the sum in the brackets is taken to be empty, and we set $\delta_0(\mathcal{N}) = 0$.

We can take the same subdeterminants in the matrix $\mathcal{M}$ which will give us determinants in which the diagonals will be $p^{f_s}, p^{f_s}, p^{f_{s-1}}, p^{f_{s-1}}, \ldots$ and possibly there are non-zero elements below the diagonal. These may not give the g.c.d., but only an exponent $\geqq \delta_j(\mathcal{M}) = \delta_j(\mathcal{N})$.

Consequently for $j = 2\nu$ we obtain $2(f_s + \cdots + f_{s-\nu+1}) \geqq 2(e_s + \cdots + e_{s+\nu-1})$ which yields (a), and a similar computation for $j = 2\nu - 1$ proves (b).

Next we consider subdeterminants of order $j = s + \nu$, $\nu \leqq s$ of $\mathcal{M}$ and $\mathcal{N}$. The formulas (7.5.1) for $\delta_j(\mathcal{N})$ remain the same. A $j \times j$ subdeterminant $\mathcal{M}$ must contain at least ν rows $\{i_\lambda\}$ out of the first s rows, i.e. of the submatrix $(p^F\ 0)$. Similarly, also ν columns $\{j_\lambda\}$ out of the submatrix $\binom{0}{p^F}$. Since the elements of p^F

are in the diagonal, in order to obtain a non-zero subdeterminant of $\mathcal{M}$, we must take in this subdeterminant the same $\{i_\lambda\}$ columns, and the same $\{j_\lambda\}$ rows of the matrix $\mathcal{M}$. Let $1 \leqq i_1 < i_2 < \cdots < i_\nu \leqq s$ and similarly $1 \leqq j_1 < j_2 < \cdots < j_\nu \leqq s$. Thus the subdeterminant considered has the form:

$$D_{(i,j)} = \left[\begin{array}{cccccc} 0 & \cdots p^{f_{i_1}} \cdots\cdots & 0 & 0 & & 0 \\ & & & & & \\ 0 & \cdots p^{f_{i_\nu}} \cdots\cdots & 0 & 0 & & 0 \\ & & & & & \\ & & & 0 & \cdots p^{f_{i_1}} \cdots & 0 \\ & * & & & & \\ & & & 0 & \cdots p^{f_{i_\nu}} \cdots & 0 \end{array}\right]$$

As we are interested only in the power of p dividing $D_{(i,j)}$, we know also that for some $D_{(i,j)}$ the highest power of p dividing the g.c.d. $D_{s+\nu}(\mathcal{M})$ will appear for some $D_{(i,j)}$. Taking this particular determinant and developing it with respect to the first ν rows and last ν columns we will get by setting $D_{(i,j)} = p^{\delta(ij)}c$, $c \not\equiv O(p)$:

$$\delta_{(ij)} = (f_{i_1} + \cdots + f_{i_\nu}) + (f_{j_1} + \cdots + f_{j_\nu}) + \delta'$$

where $p^{\delta'}$ is the highest power of p dividing a subdeterminant or order $(s+\nu) - 2\nu = s - \nu$. By taking a lower bound for δ' and for the sums in the bracket, we get

$$\delta_{s+\nu}(\mathcal{M}) \geqq 2(f_s + f_{s-1} + \cdots + f_{s-\nu+1}) + \delta_{s-\nu}(\mathcal{M})$$

since $f_{i_\lambda} \geqq f_{s-\lambda+1}$ and $\delta' \geqq \delta_{s-\nu}(\mathcal{M})$.

Combining this inequality with the fact that $\delta_j(\mathcal{M}) = \delta_j(\mathcal{N})$:

$$2(f_s + f_{s-1} + \cdots + f_{s-\nu+1}) \leqq \delta_{s+\nu}(\mathcal{N}) - \delta_{s-\nu}(\mathcal{N}),$$

we change notations and put $\mu = s - \nu$; then

$$f_s + f_{s-1} + \cdots + f_{\mu+1} \leqq \tfrac{1}{2}(\delta_{2s-\mu}(\mathcal{N}) - \delta_\mu(\mathcal{N})).$$

The values of $\delta_j(\mathcal{N})$ are given in (7.5.1), from which we deduce:

For $\mu = 2\rho$, $2s - \mu = 2(s - \rho)$ and note that $2\rho \leqq s$:

$$f_s + \cdots + f_{2\rho+1} \leqq \tfrac{1}{2}(\delta_{2(s-\rho)}(\mathcal{N}) - \delta_{2\rho}(\mathcal{N})) = \sum_{i=\rho+1}^{s-\rho} e_i.$$

For $\mu = 2\rho - 1$, $2s - \mu = 2(s - \rho) + 1$ and note that $2\rho - 1 \leqq s$:

$$\begin{aligned} f_s + \cdots + f_{2\rho} &\leqq \tfrac{1}{2}(\delta_{2(s-\rho)+1}(\mathcal{N}) - \delta_{2\rho-1}(\mathcal{N})) \\ &= \tfrac{1}{2}(\delta_{2(s-\rho)}(\mathcal{N}) - \delta_{2\rho}(\mathcal{N})) + \tfrac{1}{2}(e_\rho + e_{s-\rho+1}) \\ &= \sum_{i=\rho+1}^{s-\rho} e_i + \tfrac{1}{2}(e_\rho + e_{s-\rho+1}) \end{aligned}$$

which completes the proof of the theorem.

The corollary follows from the fact that $n = f_1 + \cdots + f_s = e_1 + \cdots + e_s$, where $p^n = |K| = |H|$, and noting that left sides of (a)–(d) are n minus the sides of (a′)–(d′).

8. An application

A problem suggested in [4] led to the question of determining the common Lagrangian of various symplectic modules. We shall be able to answer a question of this type later. First we deal with the converse: constructing various symplectic modules in which H is Lagrangian. One module of this type is $S_1(H) = H \oplus \hat{H}$ of Theorem 4.1. Another type is the following:

Let $\operatorname{inv} H = (e_1, e_2, \ldots, e_r)$, and assume $r = 2\rho$ is even (if not, set $e_{r+1} = 0$), and consider the abelian group H_0 with $\operatorname{inv} H_0 = (e_1 + e_2, e_3 + e_4, \ldots, e_{r-1} + e_r)$. We prove.

8.1. Theorem. *$S_1(H_0)$ is a symplectic module of*

$$\operatorname{rk} S_1(H_0) = 2\left[\frac{\operatorname{rk} H + 1}{2}\right],$$

in which the original group H is Lagrangian.

Proof. Clearly $\operatorname{rk} S_1(H_0) = 2 \operatorname{rk} H_0 = 2[(\operatorname{rk} H + 1)/2]$. If $H_0 = (u_1) \oplus \cdots \oplus (u_\rho)$ then $S_1(H_0) = (u_1) \oplus \cdots \oplus (u_\rho) \oplus (\hat{u}_1) \oplus \cdots \oplus (\hat{u}_\rho)$, and

$$|S_1(H_0)| = (p^{\Sigma e_i})^2 = |H|^2.$$

Hence, in view of 3.1, Corollary (b), it suffices to identify H with an isotropic subgroup of $S_1(H_0)$.

Indeed, consider the group

$$H_1 = (p^{e_2}u_1) \oplus (p^{e_1}\hat{u}_1) \oplus (p^{e_4}u_2) \oplus (p^{e_3}\hat{u}_2) \oplus \cdots \oplus (p^{e_r}u_r) \oplus (p^{e_{r-1}}\hat{u}_r).$$

Its invariants are readily seen to be $(e_1, e_2, \ldots, e_{r-1}, e_r)$, and, therefore, it is isomorphic with H. Next H_1 is isotropic and clearly we have only to check

$$(p^{e_{2i}}u_i, p^{e_{2i-1}}\hat{u}_i) = -p^{e_{2i}+e_{2i-1}}\hat{u}_i(u_i) = -1 \equiv 0 \operatorname{mod}(\mathbf{Z})$$

since $\hat{u}_i(u_i) = p^{-(e_i+e_{2i-1})}$. The other relations are trivial.

NOTATION. Denote by $S_2(H)$ the symplectic module $S_1(H_0)$.

REMARK 1. The examples $S_1(H)$ and $S_2(H)$ show that in Corollary 3.1a, the even rank of the symplectic modules G in which H is Lagrangian can be either equal to $2\operatorname{rk} H$ or as low as $2[(\operatorname{rk} H + 1)/2]$.

Moreover, we can get various ranks in between by extending the construction of the last theorem.

REMARK 2. Let $H = H' \oplus H''$ and construct the symplectic module $G' = S_1(H') \oplus S_2(H'')$. It is not difficult to show as before that there is a Lagrangian in G' isomorphic with H.

Note also that in the construction of H_0 in our theorem, we could have used any pairing of the invariants of H to obtain the corresponding H_0 and a symplectic module in which H is Lagrangian.

8.2. In our next result, which is an application of the last theorem, we make the convention $s = r = 2k$, and $\operatorname{inv} K = (f_1, \dots, f_s)$, $\operatorname{inv} H = (e_1, \dots, e_s)$. Since $r \geqq k$, it means that if $\operatorname{rk} K \equiv 1 \pmod 2$ we add $f_s = 0$, and also all $e_j = 0$ for $r < j$ where $r = \operatorname{rk} H$.

In this context we prove

THEOREM. *The group K is Lagrangian in both $S_1(H)$ and $S_2(H)$ if and only if* $\operatorname{rk} K = \operatorname{rk} H$, *or* $\operatorname{rk} K = \operatorname{rk} H + 1$ *and then necessarily* $\operatorname{rk} H$ *is odd, and the following holds*:

$$e_{2i-1} \geqq f_{2i-1} \geqq \tfrac{1}{2}(f_{2i-1} + f_{2i}) = \tfrac{1}{2}(e_{2i-1} + e_{2i}) \geqq f_{2i} \geqq e_{2i}.$$

PROOF. Since K is Lagrangian in $S_1(H)$, we have by (a′) of the last corollary that

$$f_1 + \cdots + f_\mu \leqq e_1 + \cdots + e_\mu.$$

K is assumed to be Lagrangian in $S_2(H) = S_1(H_0)$ with

$$\operatorname{inv} H_0 = (e_1 + e_2, e_3 + e_4, \dots, e_{2k-1} + e_{2k}, 0, \dots, 0) \qquad \text{where } s = 2k.$$

Hence, it follows by (c′) of the last corollary that for $\rho \leqq k$,

$$f_1 + \cdots + f_{2\rho} \geqq (e_1 + e_2) + \cdots + (e_{2\rho-1} + e_{2\rho}) + 0$$

since $s - \rho + 1 > k$. Applying the two inequalities for $\rho = 1, \dots, k$ shows that $f_{2i-1} + f_{2i} = e_{2i-1} + e_{2i}$.

In view of this equality it follows from (a′) by Corollary 7.5 choosing $\mu = 2i - 1$, that $f_{2i-1} \leqq e_{2i-1}$. Finally, from (b′) Corollary 7.5 put $\mu = 2i$; we get $-\frac{1}{2} f_{2i} \leqq -\frac{1}{2} e_{2i}$, since

$$\sum_{\nu=1}^{2i-1} f_\nu + \frac{1}{2} f_{2i} = \sum_{\nu=1}^{2i} f_\nu - \frac{1}{2} f_{2i},$$

and similarly for the e's. Consequently $f_{2i} \geqq e_{2i}$.

The relation between the ranks is proved as follows: if $\operatorname{rk} K \neq \operatorname{rk} H$, since K is Lagrangian in $S_1(H)$, then $\operatorname{rk} K \geqq \operatorname{rk} H$ by Corollary 3.1. This, in view of the inequality of the theorem, means that the last ν for which $f_\nu > 0$ must be even, and then we may have $e_\nu = 0$, which proves that then $\operatorname{rk} K = \operatorname{rk} H + 1 \equiv 0 (\operatorname{mod} 2)$.

To prove the converse it suffices to consider the case of two invariants, $\operatorname{inv} H = (e_1, e_2)$, $\operatorname{inv} K = (f_1, f_2)$ (the case $s = 2$) satisfying the theorem, i.e., $e_1 + e_2 = f_1 + f_2$, $e_1 \geqq f_1 \geqq f_2 \geqq e_2$.

We observe that in $\mathcal{M}_4$ $(\mathbf{Z})$ the diagonal matrix $\mathcal{N} = \operatorname{diag}(p^{e_1}, p^{e_1}, p^{e_2}, p^{e_2})$ is equivalent to the matrix

$$\mathcal{M} = \begin{bmatrix} p^{f_1} & 0 & 0 & 0 \\ 0 & p^{f_2} & 0 & 0 \\ 0 & p^{e_2} & p^{f_1} & 0 \\ -p^{e_2} & 0 & 0 & p^{f_2} \end{bmatrix}.$$

One proves easily that $\mathcal{M}$ can be transformed to $\operatorname{diag}(p^{e_2}, p^{e_2}, p^{f_1+f_2-e_2}, p^{f_1+f_2-e_2})$ by elementary operations on rows and columns noting that $e_2 \leqq f_2$. The matrix obtained is equivalent to $\mathcal{N}$, since $f_1 + f_2 - e_2 = e_1$. In view of 7.3 and Theorem 7.1, it follows that K, whose invariants are (f_1, f_2), is isomorphic with a Lagrangian of $S_1(H)$.

One can also obtain this by exhibiting this group K, i.e. the subgroup of $S_1(H)$ generated by the elements:

$$k_1 = p^{e_1 - f_1} \hat{h}_1 + h_2, \qquad k_2 = p^{e_1 - f_2} h_1 + \hat{h}_2$$

and indeed, $p^{f_1} k_1 = 0$, $p^{f_2} k_2 = p^{f_2} \hat{h}_2 = 0$ since $f_2 \geqq e_2$; and

$$(k_1, k_2) = p^{2e_1 - f_1 - f_2} (\hat{h}_1, h_1) + (h_2, \hat{h}_2) = p^{e_1 - f_1 - f_2} - p^{-e_2} = 0,$$

because $f_1 + f_2 = e_1 + e_2$.

The fact that K is also Lagrangian in $S_2(H)$ follows since both H_0 and K_0 are cyclic of order $p^{e_1 + e_2} = p^{f_1 + f_2}$, so $S_2(H) = S_1(K_0)$, and the latter contains K as Lagrangian subgroup.

REMARK. The converse of our theorem follows also from the classification of Lagrangians of rk 4 symplectic modules, given in the last proposition of 5.3.

An immediate consequence is:

8.3. COROLLARY. *If H is a p-group whose invariants appear in pairs, then H is the only common Lagrangian of $S_1(H)$ and $S_2(H)$.*

9. p-regular groups

9.1. The problem of a lower bound for the order of a p-group G satisfying $(6.1n)$ seems to be difficult. In [4] p. 139 we have given the bound p^{2n-2}, which is used to show that the Galois field splitting the universal division algebra of degree p^n must be of dimension $\geqq p^{2n-2}$. But this seems to be a too small bound. If G is abelian, a far more higher bound is given in Section 6.

In the following we show that this bound is also valid for some general p-groups: the regular p-groups.

A p-group G is a regular p-group if for every integer m and every $a, b \in G$:

$$(ab)^{p^m} = a^{p^m} b^{p^m} S_1^{p^m} \cdots S_t^{p^m}$$

for appropriate elements S_i from the commutator subgroup ([2] p. 183). A large set of such groups are the p-groups of class $< p$, which include the abelian groups which are trivially regular. For these groups which satisfy $(6.1n)$ we shall prove also the theorem of 6.1.

9.2. NOTATION. Let $|G| = p^g$, we denote $g = |G|_{(p)}$.

Given an abelian group K of order p^n and $\mathrm{inv}\, K = (f_1, \ldots, f_s)$, $f_i \geqq f_{i+1}$, we consider the partition $n = f_1 + f_2 + \cdots + f_s$ as a Young diagram D_f having f_j squares in the j-th row; and the corresponding dual partition of $n = f_1^* + \cdots + f_{f_1}^*$ where f_i^* is the length of the i-th column of the corresponding Young diagram D_f; in other words f_i^* is the number of $f_j \geqq i$.

Let G be a finite p-group containing a set of groups $\{K_\lambda\}$ and let

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_s \rhd G_{s+1} = (e)$$

be a composition series such that G_i / G_{i+1} is an elementary p-abelian group. Then:

PROPOSITION. $|G|_{(p)} \geqq \Sigma_i \, \mathrm{Max}_\lambda \, \mathrm{rk}((K_\lambda \cap G_i)/(K_\lambda \cap G_{i+1}))$.

PROOF. By induction on s. The quotient group G_1/G_2 is a vector space over a finite field of p elements and $G_1/G_2 \supseteq K_\lambda G_2/G_2 \cong K_\lambda/(K_\lambda \cap G_2)$ for all λ; hence,

$$|G_1/G_2|_{(p)} = \operatorname{rk}(G_1/G_2) \geqq \operatorname*{Max}_{\lambda} \operatorname{rk}(K_\lambda/(K_\lambda \cap G_2)).$$

On the other hand $|G|_{(p)} = |G_1/G_2|_{(p)} \cdot |G_2|_{(p)}$ and $G_2 \supseteq K_\lambda \cap G_2$ for all λ. The rest follows now easily.

9.3. One of the main properties of regular p-groups is that

$$G_m = \{g \in G; g^{p^m} = e\}$$

form a normal subgroup of G ([2]). This is used in proving:

THEOREM. *Let G be a regular p-group containing a set of abelian groups* $\{K_\lambda\}$ *such that* $\operatorname{inv} K_\lambda = (f_{\lambda 1}, \ldots, f_{\lambda s})$, $f_{\lambda i} \geqq f_{\lambda i+1} \geqq 0$; *then*

$$|G|_{(p)} \geqq \sum_i \operatorname*{Max}_{\lambda} (f_{\lambda i}) = \sum_i \operatorname*{Max}_{\lambda} (f^*_{\lambda i}).$$

Indeed, consider the sequence $G = G_\mu \rhd G_{\mu\;1} \rhd \cdots \rhd G_1 \rhd G_0 = (e)$ with G_i defined above. Note that in this case

$$K_\lambda \cap G_j = (K_\lambda)_j = \{g \in K_\lambda, g^{p^j} = e\}.$$

Also $\operatorname{rk}((K_\lambda)_j/(K_\lambda)_{j-1})$ = number of $f_{\lambda\nu}$ which are $\geqq j$, i.e.,

$$\operatorname{rk}((K_\lambda)_j/(K_\lambda)_{j-1}) = f^*_{\lambda j},$$

since if $K_\lambda = (k_{\lambda 1}) + \cdots + (k_{\lambda s})$ then

$$(K_\lambda)_j = (p^{f_{\lambda 1}-j}k_{\lambda 1}) \oplus \cdots \oplus (p^{f_{\lambda t}-j}k_{\lambda t}) \oplus (k_{\lambda t+1}) \oplus \cdots,$$

where $f_{\lambda t} > j \geqq f_{\lambda t+1}$ and so

$$(K_\lambda)_j/(K_\lambda)_{j-1} = (p^{f_{\lambda 1}-j}\bar{k}_{\lambda 1}) \oplus \cdots \oplus (p^{f_{\lambda t}-j}\bar{k}_{\lambda t}) \oplus \cdots \oplus (\bar{k}_{\lambda r})$$

where $f_{\lambda r} > j - 1 \geqq f_{\lambda r+1}$. It follows, therefore, by the preceding proposition that $|G|_{(p)} \geqq \Sigma_i \operatorname{Max}_\lambda f^*_{\lambda i}$.

It remains to prove the equality of $\Sigma_i \operatorname{Max}_\lambda f^*_{\lambda i} = \Sigma \operatorname{Max}_\lambda f_{\lambda i}$. To this end, set $F_i = \operatorname{Max}_\lambda f_{\lambda i}$, then clearly $F_1 \geqq F_2 \geqq \cdots \geqq F_s$. Let $m = F_1 + \cdots + F_s$. This partition of m yields a Young diagram D_F which is clearly characterized as the minimal Young diagram containing all diagrams D_λ corresponding to the partition $n = f_{\lambda 1} + \cdots + f_{\lambda s}$. But from this point of view, considering the D_F to be determined by their columns $f^*_{\lambda j}$, D_F will have columns of order $F^*_j = \operatorname{Max}_\lambda f^*_{\lambda j}$, and then $m = F^*_1 + \cdots + F^*_s$ proves our assertion.

9.4. We can now extend Theorem 6.1 to regular p-groups.

THEOREM. *If G is a regular p-group containing a Lagrangian of every symplectic module of order p^n, then*

$$|G|_{(p)} \geqq \sum \left[\frac{n}{2i-1}\right] = \frac{n}{2}(\log n + c) + o(\sqrt{n}).$$

Indeed, consider the set of symplectic modules $\{G_q\}$ defined in the beginning of 6.1. By assumption, the group G contains a Lagrangian K_q of G_q. Let $\operatorname{inv} K_q = (f_{q_1}, f_{q_2}, \ldots, f_{q_q}, \ldots)$, then as in Lemma 6.1 we obtain $f_{q_q} \geqq \{\frac{1}{2}[n/q]\}$. It follows now from the previous theorem (in 9.3) that

$$|G|_{(p)} \geqq \sum_i \operatorname*{Max}_q f_{qi} \geqq \sum_q f_{qq} = \sum_q \left\{\frac{1}{2}\left[\frac{n}{q}\right]\right\}.$$

The rest follows now from Theorem 6.2.

In the application of [4] theorem 7.4, it was noted that the Galois group of a splitting field of the generic division algebra of degree p^n contains a Lagrangian of every simplectic module of order p^n. Since every p-group of order $\leqq p^p$ is p-regular, one readily verifies that:

COROLLARY. *Galois splitting fields of the universal division algebra* $\mathrm{UD}(p^n, k)$ *with $n \leqq p$ have dimension over the center $\geqq p^{n(\log n + c)/2 + o(\sqrt{n})}$.*

REMARK. One can replace the undetermined $O(\sqrt{n})$ in the theorems of 6.2 and 9.4 and their corollaries by $-2(\sqrt{n}+1)$. This can be obtained by a closer analysis of the Dirichlet approximation of $\Sigma[n/v]$, e.g. in [3] theorem 320, used in these theorems.

REFERENCES

1. G. de Rham, *Sur l'analysis situs des variétés à n dimension*, J. Math. Pure Appl. **10** (1931), 115–200.

2. M. Hall, *The Theory of Groups*, MacMillan Co., 1959.

3. G. H. Hardy and E. M. Wright, *Theory of Numbers*, Oxford, 1954.

4. J. P. Tignol and S. A. Amitsur, *Kummer subfields of Malcev–Neumann division algebras*, Isr. J. Math. **50** (1985), 114–144.

5. C. T. C. Wall, *Quadratic forms on finite groups and related topics*, Topology **2** (1963), 281–298.

6. H. Zassenhaus, *The Theory of Groups*, Chelsea, New York, 1949.