Conjugacy Classes in Finite Symplectic Groups

D. E. Taylor

Version of 28 April, 2021
TEXed: 21 August, 2021

The definitive and very general treatment of the conjugacy classes of the unitary, symplectic and orthogonal groups was given by Wall [16] in 1963 building on the work of Williamson [17, 18] for perfect fields of characteristic other than 2.

The following sections describe Magma code implementing the construction of conjugacy classes for the special case of the finite symplectic groups defined over a Galois field GF(q). The approach given here follows Milnor [10] and Huppert [5, 6]. For other approaches with more emphasis on the theory of algebraic groups see Springer–Steinberg [15] (based on Springer's thesis [14] of 1951), Humphreys [4] and the recent book of Liebeck and Seitz [7]. For fields of characteristic 2 see Riehm [12], Hesselink [3] and Xue [19].

The conjugacy classes are obtained by first computing a complete collection of invariants and then determining a representative matrix for each invariant.

A partial analysis of similar algorithms for unitary groups can be found in [2]. There are some remarks about the symplectic groups in the unpublished draft [11].

1 Symplectic groups

The 'standard' alternating form $J = J_{2n}$ is the $2n \times 2n$ matrix $\begin{pmatrix} 0 & \Lambda_n \\ -\Lambda_n & 0 \end{pmatrix}$, where Λ_n is the $n \times n$ matrix

$$\Lambda_n = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ & & \iddots & & \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

The symplectic group $\mathrm{Sp}(2n, q)$ considered here is the set of $2n \times 2n$ matrices A over the field $k = \mathrm{GF}(q)$ such that $AJA^{\mathrm{tr}} = J$, where A^{tr} is the transpose of A.

The description of the conjugacy classes of $\mathrm{Sp}(2n, q)$ closely parallels the description of the conjugacy classes of $\mathrm{GL}(2n, q)$.

The group $\mathrm{GL}(2n, q)$ acts on $V = k^{2n}$ and for $g \in \mathrm{GL}(2n, q)$, the space V becomes a $k[t]$-module V_g by defining $vf(t) = vf(g)$ for all $v \in V$ and all $f(t) \in k[t]$.

The alternating form $\beta(u, v) = uJv^{\mathrm{tr}}$ defines an isomorphism $\theta : V \to V^* : v \mapsto \beta(-, v)$. An element $g \in \mathrm{GL}(2n, q)$ acts on V^* according to the rule $v(\psi g) = (vg^{-1})\psi$ for all $v \in V$ and all $\psi \in V^*$; that is, $\psi g = g^{-1}\psi$. With this action V^* becomes a $k[t]$-module V_g^* and g belongs to $\mathrm{Sp}(2n, q)$ if and only if $\theta : V_g \to V_g^*$ is an isomorphism of $k[t]$-modules.

If $g, h \in \mathrm{GL}(2n, q)$, then $T : V_g \to V_h$ is a $k[t]$-isomorphism if and only if $gT = Th$ if and only if $T^{-1}g^{-1} = h^{-1}T^{-1}$ if and only if $T : V_g^* \to V_h^*$ is an isomorphism. Since $T \in \mathrm{Sp}(2n, q)$ if and only if $T\theta = \theta T$ it follows that $g, h \in \mathrm{Sp}(2n, q)$ are conjugate in $\mathrm{Sp}(2n, q)$ if and only if there is a $k[t]$-isomorphism $T : V_g \to V_h$ such that the diagram

$$\begin{array}{ccc} V_g & \xrightarrow{T} & V_h \\ {\scriptstyle\theta}\big\downarrow & & \big\downarrow{\scriptstyle\theta} \\ V_g^* & \xrightarrow[T]{} & V_h^* \end{array}$$

commutes.

As shown in Macdonald [9, Chap. IV], if $\mathcal{P}$ is the set of all partitions and Φ is the set of all monic irreducible polynomials (other than t), then for $g \in \mathrm{GL}(2n, q)$ there is a function $\mu : \Phi \to \mathcal{P}$ such that

$$V_g = \bigoplus_{f \in \Phi, i} k[t]/(f)^{\mu_i(f)} \tag{1.1}$$

and $\mu(f) = (\mu_1(f), \mu_2(f), \dots,)$ is a partition such that

$$\sum_{f \in \Phi} \deg(f)|\mu(f)| = 2n.$$

If $g \in \mathrm{Sp}(2n, q)$ there are restrictions—to be determined in the sections which follow—on the polynomials and partitions that can occur in this decomposition.

The following functions, defined later in this document, are needed in the code for conformal symplectic groups. Therefore we write them to the file `common.m` and import them into the main files. We shall also write the intrinsics DualPolynomial and StarIrreduciblePolynomials to `common.m`. All code written to `common.m` will be coloured brown.

```
import "common.m" : convert, primaryParts, stdJordanBlock, centralJoin,
    getSubIndices, restriction, homocyclicSplit, type3Companion, addSignsSp;
import "Classes/translate/translateSp.m" : tagToNameSp;
```

Definition 1.1. The *adjoint* of $\alpha \in \mathrm{End}_k(V)$ with respect to the alternating form $\beta(u, v) = uJv^{\mathrm{tr}}$ is the linear transformation α^* such that

$$\beta(u\alpha, v) = \beta(u, v\alpha^*) \quad \text{for all } u, v \in V.$$

Proposition 1.2. *If A is the matrix of α, then $A^* = JA^{\mathrm{tr}}J^{-1}$ and the bilinear form $\gamma(u, v) = \beta(u\alpha, v)$ is alternating if and only if $A = A^*$. Moreover if $g \in \mathrm{GL}(V)$ preserves β, then g preserves γ if and only if $g\alpha = \alpha g$.*

Definition 1.3.

(i) Let $f(t) \in k[t]$ be a monic polynomial of degree d such that $f(0) \neq 0$. The *dual* of $f(t)$ is the polynomial
$$f^*(t) = f(0)^{-1} t^d f(t^{-1}).$$

(ii) The polynomial $f(t)$ is $*$-*symmetric* if $f^*(t) = f(t)$.

(iii) A polynomial $f(t)$ is $*$-*irreducible* if it is $*$-symmetric and has no proper $*$-symmetric factors.

The monic polynomial $f(t) = a_0 + a_1 t + \cdots + a_{d-1}t^{d-1} + t^d$ is $*$-symmetric if and only if
$$a_0^2 = 1 \quad \text{and} \quad a_{d-i} = a_0 a_i \quad \text{for } 0 < i < d. \tag{1.2}$$

It follows that $a_0 = \pm 1$ and an element a in an extension field of k is a root of a $*$-symmetric polynomial $f(t)$ if and only if a^{-1} is also a root with the same multiplicity.

It is clear from the definition that for monic polynomials f and g we have $f^{**} = f$ and $(fg)^* = f^*g^*$.

Remark 1.4. Both Riehm [12] and Huppert [5] define the dual of $f(t)$ to be $f^*(t) = t^d f(t^{-1})$ and Huppert declares f to be symmetric when f and f^* are equal up to a unit in $k[t]$; that is, when $f(t) = a_d^{-1} a_0 f^*(t)$. For monic polynomials this agrees with the definition given above.

```
declare attributes GrpMat: Labels_A, Labels_S;
intrinsic DualPolynomial(f :: RngUPolElt) -> RngUPolElt
{The dual of the polynomial f}
  eseq := Coefficients(f);
  require eseq[1] ne 0 : "Polynomial must have non-zero constant term";
  return eseq[1]^-1 * Parent(f) ! Reverse(eseq);
end intrinsic;
```

If g preserves the alternating form β introduced above, then for all $u, v \in V$ we have
$$\beta(ug, v) = \beta(u, vg^{-1})$$
and thus for $f(t) \in k[t]$ we have
$$\beta(uf(g), v) = \beta(u, vf(g^{-1})). \tag{1.3}$$

In particular, if $m(t)$ is the minimal polynomial of g, then $vm(g^{-1}) = 0$ for all v and therefore $g^d m(g^{-1}) = 0$, where d is the degree of $m(t)$. Thus $m^*(g) = 0$ and it follows that $m^*(t) = m(t)$; that is, the minimal polynomial of g is $*$-symmetric.

Lemma 1.5. *Let $f(t)$ be a monic $*$-irreducible polynomial.*

(i) *If $f(t)$ is reducible, there exists an irreducible polynomial $g(t)$ such that $f(t) = g(t)g^*(t)$ and $g(t) \neq g^*(t)$.*

(ii) *If the degree of $f(t)$ is even, then $f(0) = 1$.*

(iii) *If the degree of $f(t)$ is odd, $f(t)$ is either $t-1$ or $t+1$.*

(iv) *If $f(t)$ is irreducible of even degree $2d$, there is an irreducible polynomial $g(t)$ of degree d such that $f(t) = t^d g(t + t^{-1})$.*

Proof. (i) Suppose that $g(t)$ is an irreducible factor of $f(t)$. Then $g^*(t)$ divides $f^*(t) = f(t)$ and since $f(t)$ is $*$-irreducible $f(t) = g(t)g^*(t)$ and $g^*(t) \neq g(t)$.

(ii) Suppose that the degree of $f(t)$ is $2d$. We may suppose that the characteristic of the field is not 2. If $a_0 = -1$ it follows from (1.2) that $a_d = 0$ and that $a_{2d-i} = -a_i$ for $1 \leq i < d$. Thus $f(1) = 0$ and so $t-1$ divides $f(t)$. The polynomial $t-1$ is $*$-symmetric and therefore $f(t) = t-1$. But this contradicts the assumption that the degree of $f(t)$ is even. Therefore $a_0 = 1$.

(iii) Suppose that the degree of $f(t)$ is odd. It follows from (1.2) that $f(-a_0) = 0$ where $a_0 = \pm 1$ is the constant term of $f(t)$. It is a consequence of (i) that $f(t)$ is irreducible and therefore $f(t) = t + a_0$, proving (iii).

(iv) Suppose that $f(t)$ is irreducible of degree $2d$. Then from (ii) we have $a_0 = 1$ and it follows by induction — successively subtracting multiples of $(t + t^{-1})^i$ from $t^{-d} f(t)$ — that there exists a polynomial $g(t)$ such that $f(t) = t^d g(t + t^{-1})$. □

```
intrinsic StarIrreduciblePolynomials( F :: FldFin, d :: RngIntElt ) -> SeqEnum
{All monic polynomials of degree d with no proper *-symmetric
 factors}

  P := PolynomialRing(F); t := P.1;

  monicIrreducibles := func< n |
    (n eq 1) select [ t - a : a in F | a ne 0 ]
    else SetSeq(AllIrreduciblePolynomials(F,n)) >;
```

Given a polynomial $g(t)$ of degree d, define $\hat{g}(t) = t^d g(t + t^{-1})$.

```
  hatPoly := function( g )
    R := RationalFunctionField( F ); x := R.1;
    return P ! ( x^Degree(g) * Evaluate( R ! g, x + 1/x ) );
  end function;

  pols := {@ P | @};
  if d eq 1 then
    pols := {@ t + 1, t - 1 @};
  elif IsEven(d) then
    allhalf := monicIrreducibles(d div 2 );
    if d eq 2 and IsOdd(Characteristic(F)) then pols := {@ t^2 + 1 @}; end if;
    pols join:= {@ f : g in allhalf | IsIrreducible(f) where f is hatPoly(g) @}
        join {@ g*gstar : g in allhalf | g ne gstar where gstar is DualPolynomial(g) @};
  end if;
  return IndexedSetToSequence( pols );
end intrinsic;
```

Partitions

A *partition* is a sequence $[\lambda_1, \lambda_2, \ldots,]$ of integers such that $\lambda_1 \geq \lambda_2 \geq \cdots \geq 0$ and $|\lambda| = \sum \lambda_i < \infty$. The nonzero λ_i are the *parts* of λ.

Given a partition in the form $[\lambda_1, \lambda_2, \ldots, \lambda_n]$, convert it to a sequence of multiplicities $[\langle 1, m_1 \rangle, \langle 2, m_2 \rangle, \ldots, \langle n, m_n \rangle]$, omitting the terms with $m_i = 0$.

```
convert := func< λ | Sort([ <i, Multiplicity(λ, i) > : i in Set(λ) ]) >;
```

The function *allPartitions*(d) returns a sequence of length d whose nth term is the list of partitions of n.

```
allPartitions := func<d | [[convert(π) : π in Partitions(n)] : n in [1..d]] >;
```

Definition 1.6. A *signed partition* is a sequence $[\langle 1, m_1 \rangle, \langle \pm 2, m_2 \rangle, \ldots, \langle n, m_n \rangle]$ such that m_i is even for all odd i and with a sign associated to each pair $\langle i, m_i \rangle$ for all even i. Terms with $m_i = 0$ are omitted.

```
addSignsSp := function(plist)
  slist := [];
  for π in plist do
    if forall{ μ : μ in π | IsEven(μ[1]) or IsEven(μ[2])} then
      ndx := { i : i in [1..#π] | IsEven(π[i][1]) };
      for S in Subsets(ndx) do
        λ := π;
        for i in S do
          μ := π[i];
          λ[i] := < −μ[1], μ[2] >;
        end for;
        Append(~slist, λ);
      end for;
    end if;
  end for;
  return slist;
end function;

signedPartitionsSp := func< d | [ addSignsSp(π) : π in allPartitions(d) ] >;
```

It turns out (cf. Shinoda [13, Theorem 1.20]) that when q is odd, the conjugacy classes of $\mathrm{Sp}(2n, q)$ are parametrised by functions $\mu : \Phi^* \to \mathcal{P} \cup \mathcal{S}$, where Φ^* is the set of (monic) $*$-irreducible polynomials and $\mathcal{S}$ is the set of signed partitions such that $\mu(f) \in \mathcal{S}$ if and only if $f(t) = t \pm 1$.

We shall refer to μ as a *conjugacy invariant* and represent it as an indexed set of pairs $\langle f, \pi \rangle$, where f is a $*$-irreducible polynomial and π is either a partition or, when f is $t+1$ or $t-1$, a signed partition. If $k = \mathrm{GF}(11)$, an example of a conjugacy invariant is

```
{@ <t + 1, [< −2,1>]>, <t^4 + 7t^3 + 7t + 1, [<1,2>, <2,1>]> @}.
```

With polynomials and partitions at our disposal it would be possible to present the code to construct all conjugacy invariants for $\mathrm{Sp}(2n, q)$ for q odd. However, we defer this until we have justified the choice of signs.

2 Conjugacy and congruence

Definition 2.1. Suppose that V_1 and V_2 are vector spaces furnished with bilinear forms γ_1 and γ_2. The forms γ_1 and γ_2 are *congruent* if there is an invertible linear transformation $g : V_2 \to V_1$ such that $\gamma_1(ug, vg) = \gamma_2(u, v)$ for all $u, v \in V_2$. If J_1 and J_2 are the matrices of γ_1 and γ_2 and if A is the matrix of g, the condition for congruence becomes $AJ_1A^{\mathrm{tr}} = J_2$.

Suppose that $g \in \mathrm{Sp}(V)$ and that the symplectic geometry on V is defined by the non-degenerate alternating form β. Denote $\mathrm{im}(1-g)$ by $[V, g]$.

Definition 2.2. The *Wall form* of g is the bilinear form χ_g defined on $[V, g]$ by

$$\chi_g(u, v) = \beta(w, v),$$

where $u = w - wg$ for some $w \in V$.

The following properties of χ_g were first proved in [16].

Lemma 2.3. *χ_g is a well-defined non-degenerate bilinear form such that*

$$\chi_g(u, v) - \chi_g(v, u) = \beta(u, v)$$

for all $u, v \in [V, g]$.

Proof. Suppose that $u = w - wg = w' - w'g$. Then $w - w' \in \ker(1-g)$ and a straightforward calculation shows that $\ker(1-g) = [V, g]^{\perp}$. Thus for $v \in [V, g]$ we have $\beta(w - w', v) = 0$ whence $\beta(w, v) = \beta(w', v)$ and χ_g is well-defined.

Suppose that $\chi_g(u, v) = 0$ for all $u \in [V, g]$. Then $\beta(w, v) = 0$ for all $w \in V$ and so $v = 0$. Thus χ_g is non-degenerate.

Finally, suppose that $u = x - xg$ and $v = y - yg$. Then

$$\begin{aligned} \chi_g(u, v) - \chi_g(v, u) &= \beta(x, y - yg) - \beta(y, x - xg) \\ &= \beta(x, y) - \beta(x, yg) - \beta(y, x) + \beta(y, xg) \\ &= \beta(x - xg, y - yg) = \beta(u, v) \end{aligned}$$

□

Theorem 2.4. *The assignment $g \mapsto ([V, g], \chi_g)$ is a one-to-one correspondence between $\mathrm{Sp}(V)$ and the set of pairs (U, χ), where U is a subspace of V and χ is a non-degenerate bilinear form on U such that $\chi(u, v) - \chi(v, u) = \beta(u, v)$ for all $u, v \in U$.*

Proof. Suppose that for $g_1, g_2 \in \mathrm{Sp}(V)$, $[V, g_1] = [V, g_2]$ and $\chi_{g_1} = \chi_{g_2}$. Then for $w \in V$ and $v \in [V, g_1]$ we have $\chi_{g_1}(w - wg_1, v) = \beta(w, v) = \chi_{g_2}(w - wg_2, v)$. Since $\chi_{g_1} = \chi_{g_2}$ is non-degenerate it follows that $w - wg_1 = w - wg_2$ for all $w \in V$ and therefore $g_1 = g_2$.

To see that the correspondence is onto, suppose that U is a subspace of V and that χ is a non-degenerate bilinear form on U such that $\chi(u, v) - \chi(v, u) = \beta(u, v)$ for all $u, v \in U$.

For $w \in V$ we have $\beta(w, -) \in U^*$ and since χ is non-degenerate there is a unique vector $wg' \in U$ such that

$$\chi(wg', v) = \beta(w, v) \quad \text{for all } v \in U.$$

Define $g : V \to V$ by $wg = w - wg'$. Then g is linear and for $u, w \in V$ we have

$$\begin{aligned}\beta(ug, wg) &= \beta(u - ug', w - wg')\\ &= \beta(u, w) - \beta(u, wg') - \beta(ug', w) + \chi(ug', wg') - \chi(wg', ug')\\ &= \beta(u, w) - \beta(u, wg') - \beta(ug', w) + \beta(u, wg') - \beta(w, ug')\\ &= \beta(u, w).\end{aligned}$$

Thus $g \in \mathrm{Sp}(V)$.

Moreover, $ug' = 0$ if and only if $\beta(u, v) = 0$ for all $v \in U$ and so $U = (\ker g')^{\perp} = [V, g]$ and $\chi_g = \chi$. Thus $\chi_g = \chi$ and $[V, g] = U$. □

Lemma 2.5. *For all $g, h \in \mathrm{Sp}(V)$ and all $u, v \in [V, g]$ we have*

$$[V, h^{-1}gh] = [V, g]h \quad \textit{and} \quad \chi_{h^{-1}gh}(uh, vh) = \chi_g(u, v).$$

Proof. If $u \in [V, g]$, then $u = w - wg$ for some w and so $uh = wh - whh^{-1}gh \in [V, h^{-1}gh]$. Thus $[V, g]h \subseteq [V, h^{-1}gh]$ and similarly $[V, h^{-1}gh]h^{-1} \subseteq [V, g]$ whence $[V, h^{-1}gh] \subseteq [V, g]h$ and equality holds.

For $u = w - wg$ we have $\chi_{h^{-1}gh}(uh, vh) = \beta(wh, vh) = \beta(w, v) = \chi_g(u, v)$ and this completes the proof. □

Theorem 2.6. *The elements $g, h \in \mathrm{Sp}(V)$ are conjugate in $\mathrm{Sp}(V)$ if and only if the bilinear forms χ_g and χ_h are congruent.*

Proof. If g and h are conjugate in $\mathrm{Sp}(V)$, it follows from the previous lemma that χ_g and χ_h are congruent.

Conversely, suppose that χ_g and χ_h are congruent. Then there is a linear transformation $\alpha : [V, g] \to [V, h]$ such that $\chi_h(u\alpha, v\alpha) = \chi_g(u, v)$ for all $u, v \in [V, g]$. It follows from the Theorem 2.4 that α is an isometry and hence, by Witt's theorem, it extends to an isometry of V. Then $[V, h] = [V, \alpha^{-1}g\alpha]$ and $\chi_h = \chi_{\alpha^{-1}g\alpha}$ whence $h = \alpha^{-1}g\alpha$. □

Lemma 2.7. *For $g \in \mathrm{Sp}(V)$, $[V, g]$ is g-invariant and $\chi_g(v, u) = \chi_g(ug, v)$.*

Proof. It is clear that $[V, g]$ is g-invariant. If $v \in [V, g]$, then $v = w - wg$ and for $u \in [V, g]$ we have

$$\beta(ug, v) = \chi_g(ug, v) - \chi_g(v, ug)$$

hence

$$\beta(ug, w) - \beta(ug, wg) = \chi_g(ug, v) - \beta(w, ug)$$

and therefore

$$\chi_g(ug, v) = -\beta(u, w) = \beta(w, u) = \chi_g(v, u).$$ □

This lemma and the previous theorem establish the essential link between conjugacy classes of symplectic transformations and congruence classes of non-degenerate bilinear forms, first proved by Wall [16]. This is also the connection between the work of Riehm [12] on congruence classes and the techniques of Milnor [10] classifying conjugacy classes of orthogonal and symplectic transformations.

Suppose that V is a vector space over the field k and that γ is a non-degenerate bilinear form on V. The first step in both Wall [16] and Riehm [12] is to observe that there exists a unique $\sigma \in \mathrm{GL}(V)$ such that $\gamma(u, v\sigma) = \gamma(v, u)$ for all $u, v \in V$. It follows immediately that $\gamma(u\sigma, v\sigma) = \gamma(u, v)$ for all $u, v \in V$ and that the minimal polynomial of σ is $*$-symmetric. Wall calls σ the *multiplier* of γ whereas Riehm calls it the *asymmetry* of γ. If $g \in \mathrm{Sp}(V)$, the multiplier of χ_g is the restriction of g^{-1} to $[V, g]$.

3 A skew-hermitian form

Throughout this section g is an element of $\mathrm{Sp}(2n, q)$ whose minimal polynomial $m(t)$ is irreducible of degree d. We follow the exposition in Milnor [10, §1], modified for symplectic groups.

In this case V is a vector space over the field $E = k[t]/(m(t))$. Then $E = k[\tau]$, where $\tau = t + (m(t))$ and the linear transformation g becomes right multiplication by τ; that is, $g : v \mapsto v\tau$.

We have already seen that $m(t)$ is $*$-symmetric and so $m(\tau^{-1}) = 0$. It follows that there is an automorphism $e \mapsto \bar{e}$ of E such that $\bar{\tau} = \tau^{-1}$. The automorphism is the identity if and only if $\tau^2 = 1$ and so for the remainder of this section we assume that $m(t)$ is neither $t + 1$ nor $t - 1$. Then (1.3) becomes

$$\beta(ue, v) = \beta(u, v\bar{e}).$$

For fixed $u, v \in V$ the map $L : E \to k : e \mapsto \beta(ue, v)$ is k-linear and so there is a unique element $u \circ v \in E$ such that

$$\mathrm{trace}_{E/k}(e(u \circ v)) = L(e) \quad \text{for all } e \in E.$$

Lemma 3.1. *$u \circ v$ is the unique skew-hermitian inner product on V such that*

$$\beta(u, v) = \mathrm{trace}_{E/k}(u \circ v).$$

Moreover $u \circ v$ is non-degenerate.

Proof. By definition

$$\mathrm{trace}_{E/k}(e(u \circ v)) = \beta(ue, v) \tag{3.1}$$

Thus for all $u_1, u_2, v \in V$ we have

$$\begin{aligned} \mathrm{trace}_{E/k}(e((u_1 + u_2) \circ v)) &= \beta((u_1 + u_2)e, v) \\ &= \beta(u_1 e, v) + \beta(u_2 e, v) \\ &= \mathrm{trace}_{E/k}(e(u_1 \circ v)) + \mathrm{trace}_{E/k}(e(u_2 \circ v)) \\ &= \mathrm{trace}_{E/k}(e(u_1 \circ v + u_2 \circ v)) \end{aligned}$$

whence

$$(u_1 + u_2) \circ v = u_1 \circ v + u_2 \circ v.$$

Furthermore,

$$\mathrm{trace}_{E/k}(e_1 e_2 (u \circ v)) = \beta(u e_1 e_2, v) = \mathrm{trace}_{E/k}(e_1(u e_2 \circ v))$$

and therefore

$$u e_2 \circ v = (u \circ v) e_2.$$

In addition

$$\begin{aligned}\operatorname{trace}_{E/k}(e(\overline{u \circ v})) &= \operatorname{trace}_{E/k}(\bar{e}(u \circ v)) \\ &= \beta(u\bar{e}, v) = \beta(u, ve) = -\beta(ve, u) \\ &= -\operatorname{trace}_{E/k}(e(v \circ u))\end{aligned}$$

and therefore $\overline{u \circ v} = -v \circ u$, which completes the proof that $u \circ v$ is skew-hermitian.

Taking $e = 1$ in (3.1) we have $\beta(u, v) = \operatorname{trace}_{E/k}(u \circ v)$ and therefore $u \circ v$ is non-degenerate.

If $u \cdot v$ is another skew-hermitian inner product on V such that $\beta(u, v) = \operatorname{trace}_{E/k}(u \cdot v)$, then $\operatorname{trace}_{E/k}(e(u \cdot v)) = \operatorname{trace}_{E/k}(ue \cdot v) = \beta(ue, v) = \operatorname{trace}_{E/k}(e(u \circ v))$ whence $u \cdot v = u \circ v$. □

Remark 3.2. Suppose that $m(t) \in k[t]$ is an irreducible $*$-symmetric polynomial of degree at least 2.

Let H be a vector space over the field $E = k[t]/(m(t))$ and let $u \circ v$ be a non-degenerate skew-symmetric hermitian form on H. Then $\beta(u, v) = \operatorname{trace}_{E/k}(u \circ v)$ is a non-degenerate symplectic form on the space V obtained by restriction of scalars.

If $\tau = t + (m(t))$, then $m(\tau^{-1}) = 0$ and $\tau \mapsto \tau^{-1}$ extends to an automorphism of E. Then multiplication by τ satisfies $\beta(u\tau, v\tau) = \beta(u, v)$ and hence belongs to the symplectic group.

4 Orthogonal decompositions

In this section we show that for $g \in \mathrm{Sp}(2n, q) = \mathrm{Sp}(V)$ and the corresponding function $\mu : \Phi \to \mathcal{P}$, the direct sum decomposition (1.1)

$$V_g = \bigoplus_{f \in \Phi, i} k[t]/(f)^{\mu_i(f)}$$

can be converted to an orthogonal decomposition and the calculation of the conjugacy class of g can be reduced to studying the restriction of g to each component.

The polynomials f such that $\mu(f)$ is non-trivial are divisors of the minimal polynomial of g, which is $*$-symmetric. Therefore we may restrict μ to the set Φ^* of $*$-irreducible polynomials.

We may represent μ as an indexed set $\{@ \langle f, \lambda \rangle \mid f \in \Phi^*, \lambda = \mu(f) \neq \varnothing @\}$, where $\varnothing$ denotes the trivial partition. Writing λ as a sequence of multiplicities $[\langle 1, m_1 \rangle, \langle 2, m_2 \rangle, \dots]$ the direct sum decomposition becomes

$$V_g = \bigoplus_{f \in \Phi^*,\, i \geq 1} m_i \bullet k[t]/(f)^i, \tag{4.1}$$

where for any $k[t]$-module M and natural number m, the notation $m \bullet M$ denotes the direct sum of m copies of M.

4.1 Primary components

Definition 4.1. For each irreducible polynomial $f(t)$, the f-primary component of (4.1) is

$$V_{(f)} = \bigoplus_{i \geq 1} m_i \bullet k[t]/(f)^i = \{\, v \mid vf(g)^i = 0 \text{ for sufficiently large } i \,\}.$$

Lemma 4.2. *$V_{(f)}$ is orthogonal to $V_{(h)}$ unless $h(t) = f^*(t)$.*

Proof. (Milnor [10]) Choose i large enough so that $uf(g)^i = 0$ for all $u \in V_{(f)}$. Then for all $u \in V_{(f)}$ and $v \in V$

$$\beta(u, vf(g^{-1})^i) = \beta(uf(g)^i, v) = 0,$$

whence $V_{(f)}$ is orthogonal to $Vf^*(g)^i$.

If $f^*(t) \neq h(t)$, then by irreducibility there are polynomials $r(t)$ and $s(t)$ such that $1 = r(t)h(t)^i + s(t)f^*(t)$. It follows that for large i and $v \in V_{(h)}$ we have $v = vs(g)f^*(g)$ and therefore the map

$$V_{(h)} \to V_{(h)} : v \mapsto vf^*(g)$$

is a bijection. Hence $V_{(f)}$ is orthogonal to $V_{(h)}$. □

Corollary 4.3. *$V_g = \perp_f \widetilde{V}_{(f)}$, where f ranges over all $*$-irreducible polynomials and where*

$$\widetilde{V}_{(f)} = \begin{cases} V_{(h)} \oplus V_{(h^*)} & f = hh^* \text{ and } h \neq h^*; \\ V_{(f)} & f = f^* \text{ is irreducible.} \end{cases}$$

Corollary 4.4. *If $h(t)$ is irreducible but not $*$-symmetric, then $V_{(h)}$ and $V_{(h^*)}$ are totally isotropic and $V_{(h)} \oplus V_{(h^*)}$ is non-degenerate.*

Proof. It follows from the lemma that $V_{(h)}$ and $V_{(h^*)}$ are totally isotropic and from the previous corollary $V_{(h)} \oplus V_{(h^*)}$ is non-degenerate. □

The PRIMARYRATIONALFORM(X) intrinsic returns the rational form C of X, a transformation matrix T such that $TXT^{-1} = C$ and the primary invariant factors *p*FACT. The entries in *p*FACT are pairs $\langle f, e \rangle$, where f is an irreducible polynomial and e is an integer. If the polynomials are $f_1, f_2, \ldots, f_r$ and if the entries with polynomial f_i are $\langle f_i, e_{i1} \rangle, \langle f_i, e_{i2} \rangle, \ldots, \langle f_i, e_{is} \rangle$, then we rely on the return value *p*FACT to group all pairs with the same irreducible polynomials and to order them so that $e_{i1} \leq e_{i2} \leq \cdots \leq e_{ir}$.

Assuming this is the case, the function *primaryParts* returns the list of $*$-irreducible polynomials, the corresponding list of partitions and a list of row indices giving the location of each primary component. This is almost all that is needed to construct the conjugacy class invariant for X. The complete invariant needs signs attached to the partitions associated with $t-1$ and $t+1$.

By Corollary 4.3, we have an orthogonal splitting $V = \perp_f \widetilde{V}_{(f)}$. The subspaces $V_{(t-1)}$ and $V_{(t+1)}$ can be found using the matrix T from the primary rational form. Suppose, for example, that $t+1$ occurs in the decomposition and that the corresponding portion of the rational form occupies rows $a+1, a+2, \ldots, a+m$ of C. Since $TX = CT$ the rows $T[a+1]$, $T[a+2], \ldots, T[a+m]$ of T are a basis for $V_{(t+1)}$.

```
primaryParts := function(pFACT)
  P := PARENT(pFACT[1][1]);
  pols := [P| ];
  parts := [];
  duals := [P| ];
  rows := [];
  j := 1;
```

```
    rownum := 0;
    for i := 1 to #pFact do
      f := pFact[i][1]; ndx := pFact[i][2];
      if f eq DualPolynomial(f) then
        if j eq 1 or pols[j−1] ne f then
          pols[j] := f;
          parts[j] := [];
          rows[j] := [];
          j +:= 1;
        end if;
        r := j − 1;
        Append(~parts[r], ndx);
      elif f notin duals then    // skip if in duals
        h := DualPolynomial(f);
        if IsEmpty(duals) or h ne duals[#duals] then
          Append(~duals, h);
          pols[j] := h∗f;
          parts[j] := [];
          rows[j] := [];
          j +:= 1;
        end if;
        r := j − 1;
        Append(~parts[r], ndx);
      else
        h := DualPolynomial(f);
        r := Index(pols, f∗h);
      end if;
      m := Degree(f)∗ndx;
      rows[r] cat:= [rownum + i : i in [1..m]];
      rownum +:= m;
    end for;
    return pols, parts, rows;
  end function;
```

As in Milnor [10] we divide the primary components $\widetilde{V}_{(f)}$, where $f(t)$ is $*$-irreducible, into three types:

Type 1. $f(t) = f^*(t)$ is irreducible and the degree of $f(t)$ is even.

Type 2. $f(t) = f^*(t) = t \pm 1$.

Type 3. $f(t) = h(t)h^*(t)$ and $h(t) \neq h^*(t)$.

It follows from the orthogonal decomposition of V_g in Corollary 4.3 that the problem of determining the conjugacy class of g reduces to solving the problem for the restriction of g to each primary component $\widetilde{V}_{(f)}$.

Type 3 companion matrices

For $V = \widetilde{V}_{(f)}$ of type 3, we choose a basis $v_1, v_2, \dots, v_r$ for $V_{(h)}$ and then the basis $w_1, w_2, \dots, w_r$ for $V_{(h^*)}$ such that $\beta(v_i, w_{r-j+1}) = \delta_{ij}$, The matrices of β and g with respect to this basis of V are

$$\begin{pmatrix} 0 & \Lambda \\ -\Lambda & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} A & 0 \\ 0 & \Lambda A^{-\mathrm{tr}} \Lambda \end{pmatrix}.$$

The minimal polynomial of A is $h(t)^s$ for some s and the minimal polynomial of A^{-1} is $h^*(t)^s$. If $\mu(h) = (\mu_1, \mu_2, \dots)$ is the partition determined by A (in the general linear group), the conjugacy class of g is completely determined by the pair $\langle f, \mu(h) \rangle$, where $f(t) = h(t)h^*(t)$. Note that $\Lambda^{-1} = \Lambda^{\mathrm{tr}} = \Lambda$. In the MAGMA code in section 5 we shall construct the matrix of $\langle f, \mu(h) \rangle$ as a direct sum of type 3 companion matrices for $f(t)^{\mu_i}$.

```
type3Companion := function(h)
  d := Degree(h);
  A := CompanionMatrix(h);
  Λ := ZeroMatrix(BaseRing(h), d, d);
  for i := 1 to d do Λ[i, d−i+1] := 1; end for;
  return DiagonalJoin(A, Λ∗Transpose(A^−1)∗Λ);
end function;
```

Orthogonal splitting of a primary component of type 1 or 2

Throughout this section we suppose that $V = V_g = V_{(f)}$ is a primary component of type 1 or 2; that is, the minimal polynomial of g is a power of the $*$-symmetric irreducible polynomial $f(t)$.

Lemma 4.5. *If f is $*$-symmetric, $V_{(f)}$ splits as an orthogonal sum $V_{(f)} = V^1 \perp V^2 \perp \cdots \perp V^r$, where each V^i is annihilated by $f(g)^i$ and is free as a module over $k[t]/(f^i)$.*

Proof. (Milnor [10]) The primary rational decomposition of $V_{(f)}$ is $V_{(f)} = W_1 \oplus W_2 \oplus \cdots \oplus W_r$ with W_i free as a $k[t]/(f^i)$-module but where the decomposition may not be orthogonal. Suppose that $W_r \cap W_r^\perp \neq 0$. Since $W_r \cap W_r^\perp$ is g-invariant we may choose $u \in W_r \cap W_r^\perp$ such that $u \neq 0$ and $uf(g) = 0$. But then $u = vf(g)^{r-1}$ for some $v \in W_r$. For $i < r$ and $w \in W_i$ we have

$$\beta(u, w) = \beta(vf(g)^{r-1}, w) = \beta(v, wf(g^{-1})^{r-1}) = 0$$

because $f = f^*$ and $i < r$. Thus u is in the radical of β, which is a contradiction. It follows that $V_{(f)} = W_r^\perp \perp W_r$ and the proof is complete by induction. □

Definition 4.6. The direct sum of copies of a cyclic module is *homocyclic*. The $k[t]$-modules V^i are the *homocyclic* components of $V_{(f)}$.

On writing $V^i = m_i \bullet k[t]/(f)^i$ the primary component $V_{(f)}$ corresponds to the partition $[\langle 1, m_1 \rangle, \langle 2, m_2 \rangle, \dots, \langle r, m_r \rangle]$.

4.2 Primary components of type 1

Recall that for primary components $V_{(f)}$ of type 1, the degree of $f(t)$ is even.

Lemma 4.7. *Suppose that $V_{(f)}$ is a primary component of type 1 and define $s(t) = f(t)t^{-d}$, where the degree of $f(t)$ is $2d$. Then for all $u, v \in V_{(f)}$ we have $\beta(us(g), v) = \beta(u, vs(g))$.*

Proof. For $u, v \in V_{(f)}$ it follows from equation (1.3), and the assumption $f(t) = f^*(t)$ that

$$\begin{aligned}\beta(us(g), v) &= \beta(uf(g)g^{-d}, v) = \beta(u, vg^d f(g^{-1}))\\ &= \beta(u, vg^{-d} f(g) = \beta(u, vs(g)).\end{aligned}$$

□

Corollary 4.8. *If V^{2i} is a homocyclic component of type 1, then $V^{2i}s(g)^i$ is a maximal totally isotropic subspace.*

Proof. For all $u, v \in V^{2i}$ we have $\beta(us(g)^i, vs(g)^i) = \beta(u, vs(g)^{2i}) = 0$.

If v is a generator of a cyclic direct summand of V^{2i} and if $2d$ is the degree of $f(t)$, the vectors $vs(g)^i$, $vs(g)^i g$, $\ldots$, $vs(g)^i g^{2di-1}$ are linearly independent. Thus $\dim V^{2i}s(g)^i = \frac{1}{2}\dim V^{2i}$, as claimed. □

Theorem 4.9 (Milnor [10])**.** *Suppose that $V_{(f)} = V^1 \perp V^2 \perp \cdots \perp V^r$ is a primary component of type 1 where V^i is free as a $k[t]/(f(t)^i)$-module and $E = k[t]/(f(t))$. Then for all i the E-space $H^i = V^i/V^i f(g)$ carries a unique skew-hermitian form $(u) \circ (v)$ such that*

$$\beta(us(g)^{i-1}, v) = \mathrm{trace}_{E/k}((u) \circ (v)).$$

Proof. If $V(i) = \{v \in V \mid vf(g)^i = 0\}$, then

$$V(i) = V^1 \perp \cdots \perp V^i \perp V^{i+1} f(g) \perp V^{i+2} f(g)^2 \perp \cdots \perp V^r f(g)^{r-i}.$$

Therefore $V^i/V^i f(g) \cong V(i)/(V(i-1) + V(i+1) f(g))$ and so the E-space H^i depends only on V and g. Furthermore, since $f(t)$ is the minimal polynomial of the induced action of g on H^i, the results of section 3 apply to H^i.

From the previous lemma, for $u, v \in V(i)$ the bilinear form $\beta(us(g)^{i-1}, v)$ is alternating and depends only on the images (u) and (v) of u and v modulo $V(i-1) + V(i+1) f(g)$. Thus the result follows from Lemma 3.1. □

When $V_g = V_{(f)}$ Milnor [10] shows that the orthogonal splitting of Lemma 4.5 is unique and the sequence of skew-hermitian spaces H^1, H^2, $\ldots$ forms a complete invariant for g.

Milnor determines a standard form for the restriction of g to H^e by first choosing an orthogonal basis (v_1), (v_2), $\ldots$, (v_r) for H^e and observing that the vectors $v_\ell g^i s(g)^j$ for $0 \le i < 2d$ and $0 \le j < e$ form a basis for the cyclic submodule generated by v_ℓ.

Furthermore he chooses the representatives v_ℓ such that $\beta(v_\ell g^i s(g)^j, v_\ell g^{i'} s(g)^{j'}) = 0$ whenever $|i - i'| < d$ and $j + j' \neq e$. The remaining values of $\beta(v_\ell g^i s(g)^j, v_\ell g^{i'} s(g)^{j'})$ are then uniquely determined. In particular, the restriction of β to each cyclic summand is non-degenerate and H^e is the orthogonal sum of these cyclic submodules.

Type 1 companion matrices

Suppose that V is a cyclic component of type 1. Then $V \simeq k[t]/(h(t))$, where $h(t) = f(t)^i$ and $f(t)$ is an irreducible $*$-symmetric polynomial. If the degree of h is $2d$, then $h(t)$ can be written as

$$h(t) = 1 + a_1 t + a_2 t^2 + \cdots + a_{d-1} t^{d-1} + t^d (a_d + a_{d-1} t + a_{d-2} t^2 + \cdots + a_1 t^{d-1} + t^d).$$

Thus, if v is a generator of V, the matrix of g with respect to the basis $v, vg, \dots, vg^{2d-1}$ is the 'standard' companion matrix

$$C_h = \left(\begin{array}{cccc|ccccc}
0 & 1 & & & & & & & \\
 & 0 & \ddots & & & & & & \\
 & & \ddots & 1 & & & & & \\
 & & & 0 & 1 & & & & \\
\hline
 & & & & 0 & 1 & & & \\
 & & & & & 0 & 1 & & \\
 & & & & & & \ddots & \ddots & \\
 & & & & & & & 0 & 1 \\
-1 & -a_1 & \cdots & -a_{d-1} & -a_d & -a_{d-1} & \cdots & -a_2 & -a_1
\end{array}\right).$$

Now set $J' = \begin{pmatrix} 0 & -P^{\mathrm{tr}} \\ P & 0 \end{pmatrix}$ where P is the $d \times d$ upper triangular matrix

$$\begin{pmatrix}
1 & a_1 & a_2 & \cdots & a_{d-1} \\
 & 1 & a_1 & \cdots & a_{d-2} \\
 & & \ddots & \ddots & \vdots \\
 & & & 1 & a_1 \\
 & & & & 1
\end{pmatrix}.$$

A direct calculation shows that $C_h^{\mathrm{tr}} J' C_h = J'$ and so g preserves the alternating form whose matrix is J'^{-1}. Furthermore $J' = Q J_{2d} Q^{\mathrm{tr}}$, where

$$Q = \begin{pmatrix} I & \\ & -P\Lambda_d \end{pmatrix} = Q^{\mathrm{tr}} \quad \text{and} \quad J_{2d} = \begin{pmatrix} & \Lambda_d \\ -\Lambda_d & \end{pmatrix}.$$

Therefore $S_h = Q C_h Q^{-1}$ satisfies $S_h J_{2d} S_h^{\mathrm{tr}} = J_{2d}$. Consequently S_h is the matrix of g with respect to the basis $u_1, u_2, \dots, u_{2d}$ where $Q = (q_{ij})$ and $u_i = \sum_{j=1}^{2d} q_{ij} v g^{j-1}$. Setting $v_i = u_{2d-i+1}$ for $1 \le i \le d$ the pairs (u_i, v_i) are mutually orthogonal hyperbolic pairs and (with $a_0 = 1$) we have

$$u_i = vg^{i-1} \quad \text{and} \quad v_i = -\sum_{j=1}^{i} a_{i-j} v g^{d+j-1} \quad 1 \le i \le d.$$

We call S_h the *symplectic companion matrix* of $h(t)$ and writing S_h with respect to the basis $u_1, u_2, \ldots, u_d, v_d, v_{d-1}, \ldots, v_1$ we have

$$S_h = \left(\begin{array}{cccc|ccccc}
0 & 1 & & & & & & & \\
 & 0 & \ddots & & & & & & \\
 & & \ddots & 1 & & & & & \\
 & & & 0 & & & & & -1 \\
\hline
1 & a_1 & \cdots & a_{d-1} & 0 & 0 & \cdots & 0 & -a_d \\
 & & & & 1 & 0 & \cdots & 0 & -a_{d-1} \\
 & & & & & \ddots & \ddots & & \vdots \\
 & & & & & & 1 & 0 & -a_2 \\
 & & & & & & & 1 & -a_1
\end{array}\right).$$

By construction $\det(tI - S_h) = h(t)$ and then a matrix representing the restriction of g to $V^i = m_i \bullet k[t]/(f)^i$ is

$$\left.\begin{pmatrix} S_h & & & \\ & S_h & & \\ & & \ddots & \\ & & & S_h \end{pmatrix}\right\} m_i \text{ blocks}$$

This matrix preserves the form

$$\left.\begin{pmatrix} J_{2d} & & & \\ & J_{2d} & & \\ & & \ddots & \\ & & & J_{2d} \end{pmatrix}\right\} m_i \text{ blocks}$$

and later we shall transform this to a matrix preserving the standard alternating form J_{2dm_i}.

Remark 4.10. This construction of a symplectic normal form for a symplectic transformation whose characteristic polynomial is $h(t)$ is independent of the characteristic of k; it requires only that $h(t)$ is a power of an irreducible $*$-symmetric polynomial and that its degree is even.

```
type1Companion := function( f )
  error if f ne DualPolynomial(f), "polynomial must be *-symmetric";
  e := Degree( f );
  error if IsOdd(e), "degree must be even";
  d := e div 2;
  a := Coefficients( f )[2..d+1];
  C := ZeroMatrix( BaseRing(f), e, e );
  for i := 1 to d-1 do
    C[i,i+1] := 1;
    C[d+1,i+1] := a[i];
    C[d+i+1,d+i] := 1;
    C[e-i+1,e] := -a[i];
  end for;
```

```
    C[d, e] := −1;
    C[d+1, 1] := 1;
    C[d+1, e] := −a[d];
    return C;
end function;
```

The endomorphism ring of a homocyclic component

This section connects Milnor's approach with that of Britnell [1, Chapter 5] and Wall [16, §2].

We begin with the cyclic g-module $W = k[t]/(f(t)^i)$ where $f(t)$ is irreducible, $*$-symmetric and g is multiplication by t.

The endomorphism ring $\mathcal{C} = \mathrm{End}_{k[t]}(W)$ of W is the centralizer of g in the algebra of all linear transformations of W. Suppose that v generates W. If the degree of $f(t)$ is d, the vectors v, vg, $vg^2, \dots, vg^{di-1}$ form a basis for W. Thus for $A \in \mathcal{C}$ we have $vA = vr(g)$ for some polynomial $r(t)$ of degree less than di and then $vg^jA = vg^jr(g)$. Therefore $A = r(g)$ and consequently $\mathcal{C} \simeq k[t]/(f(t)^i)$ as k-algebras. The radical of $\mathcal{C}$ is the ideal generated by $f(g)$.

If $A = r(g)$, then $A^* = r(g^{-1})$ and the adjoint map $A \mapsto A^*$ is an automorphism of $\mathcal{C}$. The induced map of $E = k[t]/(f(t))$ is the field automorphism $e \mapsto \bar{e}$ considered in section 3. It is the identity if and only if $f(t) = t \pm 1$.

Let $V = W_1 \perp W_2 \perp \cdots \perp W_m$ be the orthogonal sum of m copies of W and let $\mathcal{C}_m$ denote the endomorphism ring of V. The action of $A \in \mathcal{C}_m$ on V is given by the $m \times m$ matrix (α_{ij}), where α_{ij} is an endomorphism of W regarded as a map from W_i to W_j. Thus $\mathcal{C}_m$ is the matrix algebra $\mathrm{Mat}(m, \mathcal{C})$.

The spaces W_i are orthogonal and therefore, for all $v_i \in W_i$ and all $v_j \in W_j$ we have

$$\beta(v_i, v_jA^*) = \beta(v_iA, v_j) = \beta(v_i\alpha_{ij}, v_j) = \beta(v_i, v_j\alpha_{ij}^*)$$

and so the matrix representing A^* is the transpose of (α_{ij}^*). In this case the adjoint map $A \mapsto A^*$ is an antiautomorphism.

The endomorphism ring $\widehat{\mathcal{C}}_m$ of $H = V/Vf(g)$ is $\mathcal{C}_m/\operatorname{rad}\mathcal{C}_m \simeq \mathrm{Mat}(m, E)$ and if $B = \widehat{A}$ represents the action of $A \in \mathcal{C}_m$ on H, the action of A^* on H is represented by $\overline{B}^{\mathrm{tr}}$.

Theorem 4.11 (Britnell [1, Theorem 5.6], Wall [16, Theorem 2.2.1])**.**

(i) *Suppose that $\alpha \in \widehat{\mathcal{C}}_m$ and $\alpha^* = \varepsilon\alpha$, where $\varepsilon = \pm 1$. Then there exists $A \in \mathcal{C}_m$ such that $\widehat{A} = \alpha$ and $A^* = \varepsilon A$. If α is non-singular, so is A.*

(ii) *Suppose that $S, T \in \mathcal{C}_m$ are invertible, $S^* = \varepsilon S$, $T^* = \varepsilon T$ and $\alpha\widehat{S}\alpha^* = \widehat{T}$ for some $\alpha \in \widehat{\mathcal{C}}_m$. Then there exists $A \in \mathcal{C}_m$ such that $\widehat{A} = \alpha$ and $ASA^* = T$.*

Proof. (i) Choose $A_0 \in \mathcal{C}_m$ such that $\alpha = \widehat{A}_0$ and put $A = \frac{1}{2}(A_0 + \varepsilon A_0^*)$. Then $\widehat{A} = \alpha$ and $A^* = \varepsilon A$. If α is invertible, there exists $B \in \mathcal{C}_m$ such that $AB = I - N$, for some $N \in \operatorname{rad}\mathcal{C}_m$. But then N is nilpotent, hence $I - N$ is invertible. Therefore A is invertible.

(ii) Choose A_0 such that $\widehat{A}_0 = \alpha$. Then A_0 is non-singular and $N_0 = T - A_0SA_0^* \in \operatorname{rad}\mathcal{C}_m$. Now suppose that we have $A_i \in \mathcal{C}_m$ such that $\widehat{A}_i = \alpha$ and $N_i = T - A_iSA_i^* \in (\operatorname{rad}\mathcal{C}_m)^{2^i}$. Put

$A_{i+1} = A_i + \frac{1}{2} N_i A_i^{*-1} S^{-1}$. Then $\widehat{A}_{i+1} = \alpha$. Furthermore, $N_i^* = \varepsilon N_i$ and therefore

$$\begin{aligned} T - A_{i+1} S A_{i+1}^* &= T - (A_i + \tfrac{1}{2} N_i A_i^{*-1} S^{-1}) S (A_i^* + \tfrac{1}{2} S^{-1} A_i^{-1} N_i) \\ &= T - A_i S A_i^* - \tfrac{1}{2} N_i - \tfrac{1}{2} N_i - \tfrac{1}{4} N_i A_i^{*-1} S^{-1} A_i^{-1} N_i \\ &= -\tfrac{1}{4} N_i A_i^{*-1} S^{-1} A_i^{-1} N_i \in (\operatorname{rad} \mathcal{C}_m)^{2^{i+1}}. \end{aligned}$$

For sufficiently large i we have $(\operatorname{rad} \mathcal{C}_m)^i = \{0\}$ and thus there exists $A \in \mathcal{C}_m$ such that $\widehat{A} = \alpha$ and $ASA^* = T$. ◻

Lemma 4.12. *Let E be a finite field of odd characteristic and let $\sigma : x \mapsto \bar{x}$ be an automorphism of E such that $\sigma^2 = 1$. Acting on each matrix entry extends σ to an automorphism $A \mapsto \overline{A}$ of $M(n, E)$. Suppose that $B \in M(n, E)$ satisfies $B = \overline{B}^{\mathrm{tr}}$. If $\sigma = 1$, suppose in addition that* $\det B$ *is a square. Then $B = A\overline{A}^{\mathrm{tr}}$ for some $A \in M(n, E)$.*

Proof. For unitary spaces over finite fields this is a consequence of the fact that up to isometry there is just one unitary space in each dimension.

More specifically, let V be the vector space of row vectors of length n over E and furnish V with the hermitian form $(u, v) \mapsto uB\bar{v}^{\mathrm{tr}}$. Choose an orthogonal basis $v_1, v_2, \ldots, v_n$ with respect to this form and put $P = (v_1, v_2, \ldots, v_n)^{\mathrm{tr}}$. Then $PB\overline{P}^{\mathrm{tr}} = D = \operatorname{diag}(\delta_1, \delta_2, \ldots, \delta_n)$. We have $\bar{\delta}_i = \delta_i$ for all i.

If $\sigma \neq 1$, the norm map from E to the fixed field of σ is onto and therefore, for all i there exists α_i such that $\delta_i = \alpha_i \bar{\alpha}_i$. Let $A = \operatorname{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, so that $D = A\overline{A}$. Then $B = (P^{-1}A)\overline{(P^{-1}A)}^{\mathrm{tr}}$.

Suppose that $\sigma = 1$. If a is a non-square in E, there exist $x, y \in E$ such that $a = x^2 + y^2$. Then for all $b \in E$ we have

$$\begin{pmatrix} x & y \\ -by & bx \end{pmatrix} \begin{pmatrix} x & -by \\ y & bx \end{pmatrix} = \begin{pmatrix} x^2 + y^2 & 0 \\ 0 & (x^2 + y^2)b^2 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & ab^2 \end{pmatrix}.$$

By assumption $\det B$ is a square and so the number of non-squares amongst the δ_i is even. It follows that $D = AA^{\mathrm{tr}}$ for some A and we have $B = (P^{-1}A)(P^{-1}A)^{\mathrm{tr}}$. ◻

Theorem 4.13. *Suppose that V is a the orthogonal sum of m copies of the cyclic g-module $W = k[t]/(f(t)^i)$, where $f(t)$ is irreducible and $*$-symmetric. If β and γ are non-degenerate alternating forms on V preserved by g, there exists $A \in \mathcal{C}$ such that $\gamma(u, v) = \beta(uA, vA)$ for all $u, v \in V$.*

Proof. If J is the matrix of β, then the matrix of γ has the form BJ. Since g preserves both β and γ it follows from Proposition 1.2 that $B \in \mathcal{C}$ and $B = B^*$, where B^* is the adjoint with respect to β. Thus the image b of B in $\widehat{\mathcal{C}}_m$ satisfies $b = \bar{b}^{\mathrm{tr}}$. From the previous lemma $b = \alpha\bar{\alpha}^{\mathrm{tr}}$ for some $\alpha \in \widehat{\mathcal{C}}_m$. It follows from the Approximation Theorem 4.11 that $B = AA^*$ for some $A \in \mathcal{C}_m$. Thus $\gamma(u, v) = \beta(uA, vA)$ for all $u, v \in V$. ◻

Corollary 4.14. *Suppose that g and g' are elements of* $\mathrm{Sp}(2n, q)$ *such that $V = k^{2n}$ is a primary component of type 1 for g and g' with the same minimal polynomial and the same partition. Then g and g' are conjugate in* $\mathrm{Sp}(2n, q)$.

Proof. We may suppose that V is homocyclic and that g and g' have the same minimal polynomial $f(t)^i$. Furthermore we may suppose that the matrix of g is a diagonal join of symplectic companion matrices, as constructed above. That is, V is an orthogonal sum of cyclic modules $k[t]/(f(t)^i)$.

There exists $\rho \in \mathrm{GL}(2n, q)$ such that $g = \rho g' \rho^{-1}$ and the bilinear form $\gamma(u, v) = \beta(u\rho, v\rho)$ is non-degenerate and alternating. Moreover,

$$\gamma(ug, vg) = \beta(ug\rho, vg\rho) = \beta(u\rho g', v\rho g') = \beta(u\rho, v\rho) = \gamma(u, v)$$

and therefore, by the previous theorem, there exists $\theta \in \mathrm{GL}(2n, q)$ such that $g\theta = \theta g$ and $\gamma(u, v) = \beta(u\theta, v\theta)$ for all u and v. Let $\alpha = \rho^{-1}\theta$. Then

$$\beta(u\alpha, v\alpha) = \beta(u\rho^{-1}\theta, v\rho^{-1}\theta) = \gamma(u\rho^{-1}, v\rho^{-1}) = \beta(u, v)$$

and $\alpha^{-1}g'\alpha = \theta^{-1}\rho g' \rho^{-1}\theta = g$. Thus α is an element of $\mathrm{Sp}(2n, q)$ that conjugates g' to g. □

This is another version of Theorem 3.3 of Milnor [10]; namely that the sequence of skew-hermitian spaces $H^1, H^2, \ldots$ of Theorem 4.9 determines the conjugacy class of g.

4.3 Primary components of type 2, odd characteristic

Assume that the characteristic of k is odd. Suppose that $f(t) = t \pm 1$ and let $V^1 \perp \cdots \perp V^r$ be an orthogonal decomposition of $V_{(f)}$ as in Lemma 4.5. The corresponding partition is the sequence of pairs $\langle i, m_i \rangle$, where $V^i = m_i \bullet k[t]/(f)^i$. Note that we may have $m_i = 0$ for some i.

Lemma 4.15. *If $\Delta = g - g^{-1}$, then $\beta(u\Delta, v) = -\beta(u, v\Delta)$.* □

Define $H^i = V^i / V^i f(g)$. Then $\dim H^i = m_i$. For $v \in V^i$, let (v) denote its image in H^i and for $(u), (v) \in H^i$ define

$$(u) \circ (v) = \beta(u\Delta^{i-1}, v). \tag{4.2}$$

Theorem 4.16 (Milnor [10])**.** *The bilinear form $(u) \circ (v)$ is well-defined and non-degenerate. If i is even it is symmetric, whereas if i is odd it is alternating and hence m_i is even. Furthermore, the sequence consisting of the isomorphism classes of these quadratic and symplectic spaces H^i forms a complete invariant for the restriction of g to $V_{(f)}$.*

Type 2, symplectic type

If i is odd, a matrix representing the action of g on V^i can be obtained by repeated application of *type3Companion*. Alternatively we may use the following code.

The 'standard' Jordan block of size n for the scalar a is the $n \times n$ matrix with a along the diagonal, 1s on the upper diagonal and 0 elsewhere. Its primary invariant is $(t - a)^n$.

```
stdJordanBlock := function(n, a)
  D := ScalarMatrix(n, a);
  for i := 1 to n−1 do D[i,i+1] := 1; end for;
  return D;
end function;
```

Here is the code to produce a symplectic companion matrix for < $t + a_0$, [<i ,2>] >, where i is odd and $a_0 = \pm 1$. This is a variant of *type3Companion* because in this case $\Lambda B^{-\mathrm{tr}}\Lambda = B^{-1}$.

```
type2CompanionS := func< a0, i | DiagonalJoin(B, B^-1) where
    B is stdJordanBlock(i, -a0) >;
```

Type 2, orthogonal type

If i is even, H^i is a quadratic space of dimension m_i. We may take the quadratic form to be $Q((v)) = \frac{1}{2}(v) \circ (v)$ and write H^i as an orthogonal sum of 1-dimensional subspaces.

Definition 4.17.

(i) A pair of vectors u, v in a quadratic space with quadratic form Q and polar form $(u, v) \mapsto u \circ v = Q(u + v) - Q(u) - Q(v)$ is a *hyperbolic pair* if $Q(u) = Q(v) = 0$ and $u \circ v = 1$. The subspace spanned by u and v is called a *hyperbolic plane*.

(ii) The *discriminant* dV of a quadratic space V is the determinant (modulo squares) of a matrix representing the symmetric form.

(iii) A quadratic space is a *metabolic* space if it is the orthogonal sum of hyperbolic planes. The discriminant of a hyperbolic plane is -1 and therefore the discriminant of a metabolic space that is the sum of m hyperbolic planes is $(-1)^m$.

Because we assume that q is odd, we regard a quadratic space as a pair (V, β) and use the notation $V = \langle a_1, a_2, \ldots, a_m \rangle$ to mean that V has an orthogonal basis $v_1, v_2, \ldots\ v_m$ such that $\beta(v_i, v_i) = a_i$ for all i. In particular, $\langle 0 \rangle$ is the unique quadratic space of dimension 0.

Lemma 4.18. *If a and b are non-zero elements of k, then for all $c \in k$ there exist $x, y \in k$ such that $c = ax^2 + by^2$.*

Corollary 4.19. *We have $V = \langle 1, 1, \ldots, 1, a \rangle$, where a is either 1 or a non-square in k. In this case $dV = a$. In particular, H^i has an orthogonal basis $(v_1), (v_2), \ldots, (v_{m_e})$ such that $(v_j) \circ (v_j) = 1$ for $1 < j \leq m_i$ and $(v_1) \circ (v_1)$ is either 1 or a non-square in k.* □

Corollary 4.20. *If V is a quadratic space of dimension at least 3, then V contains a singular vector.* □

Corollary 4.21. *The quadratic space V can be written in the form $V = M \perp V_0$, where M is a metabolic space,* $\dim V_0 \leq 2$ *and there are no singular vectors in V_0.* □

The space V_0 is called the *anisotropic kernel* of V. It is uniquely determined by V up to isometry. The *Witt index* of V is $\frac{1}{2} \dim M$. The Witt index is said to be *maximal* if $V_0 = 0$. For the finite field $k = \mathrm{GF}(q)$ there are four possibilities for the anisotropic kernel: $\langle 0 \rangle$, $\langle 1 \rangle$, $\langle \delta \rangle$ or $\langle 1, -\delta \rangle$, where δ is a non-square in k.

Two quadratic spaces are *equivalent* if they have the same anisotropic kernel. The equivalence classes of the spaces $\langle 1, 1, \ldots, 1 \rangle$ and $\langle 1, \ldots, 1, \delta \rangle$, both of dimension m, depend on the congruences of m and q modulo 4.

If $q \equiv 1 \pmod 4$, then

$$\langle 1, 1, \ldots, 1 \rangle \equiv \begin{cases} \langle 0 \rangle & m \equiv 0 \pmod 2 \\ \langle 1 \rangle & m \equiv 1 \pmod 2 \end{cases}$$

$$\langle 1, \ldots, 1, \delta \rangle \equiv \begin{cases} \langle 1, -\delta \rangle & m \equiv 0 \pmod 2 \\ \langle \delta \rangle & m \equiv 1 \pmod 2 \end{cases}$$

If $q \equiv 3 \pmod 4$, then

$$\langle 1, 1, \ldots, 1 \rangle \equiv \begin{cases} \langle 0 \rangle & m \equiv 0 \pmod 4 \\ \langle 1 \rangle & m \equiv 1 \pmod 4 \\ \langle 1, -\delta \rangle & m \equiv 2 \pmod 4 \\ \langle \delta \rangle & m \equiv 3 \pmod 4 \end{cases}$$

$$\langle 1, \ldots, 1, \delta \rangle \equiv \begin{cases} \langle 1, -\delta \rangle & m \equiv 0 \pmod 4 \\ \langle \delta \rangle & m \equiv 1 \pmod 4 \\ \langle 0 \rangle & m \equiv 2 \pmod 4 \\ \langle 1 \rangle & m \equiv 3 \pmod 4 \end{cases}$$

If i is even, there are two conjugacy classes of elements in $\mathrm{Sp}(im_i, q)$ with the same minimal polynomial $(t + a_0)^i$ and multiplicity m_i. In order to distinguish between these classes we attach a sign to the pair $\langle i, m_i \rangle$, when i is even.

Definition 4.22. The *sign* of a non-degenerate quadratic space V is $+$ if its anisotropic kernel is $\langle 0 \rangle$ or $\langle 1 \rangle$; otherwise the sign is $-$. Thus, if the dimension of V is even, its sign is $+$ if and only if its Witt index is maximal.

We shall apply this definition to the quadratic space H^i in order to attach a sign to $\langle i, m_i \rangle$. As can be seen from the calculation above the sign is determined by the discriminant, the dimension modulo 4 and the size of the field modulo 4.

Suppose that the discriminant of H^i is a square in $k = \mathrm{GF}(q)$. If its dimension m_i is congruent to 2 or 3 modulo 4 and if $q \equiv 3 \pmod 4$, the sign is $-$; otherwise it is $+$. On the other hand, if the discriminant is a non-square, $m_i \equiv 2, 3 \pmod 4$ and $q \equiv 3 \pmod 4$, the sign is $+$; otherwise it is $-$.

For an even integer e and $a_0 = \pm 1$, the following code constructs a representative for $< t + a_0,\ [\ <e\ ,1>\ ]\ >$. The return value is $g = \begin{pmatrix} -a_0 B & aS \\ 0 & -a_0 B^{-1} \end{pmatrix}$, where B is a standard $c \times c$ Jordan block all of whose non-zero entries are 1. All entries in S are 0 except for its last row, which alternates between 1 and -1. If $|e| = 2c$, one checks directly that $B\Lambda_c B^{-\mathrm{tr}} = \Lambda_c$ and that $S\Lambda B^{\mathrm{tr}}$ is symmetric, whence $g \in \mathrm{Sp}(2c, q)$.

```
type2CompanionO := function(a0, e)
  assert IsEven(e);
  c := Abs(e) div 2;
  F := Parent( a0 );
```

```
    B := stdJordanBlock(c, F ! 1);
    X := −a0∗DiagonalJoin(B, B^−1);
    a := IsEven(c) select F ! 2 else −F ! 2;
    if (e lt 0) then a ∗:= Nonsquare(F); end if;
    for i := 1 to c do X[c, c+i] := IsOdd(i) select a else −a; end for;
    return X;
  end function;
```

The quadratic space of Theorem 4.16 for g is one-dimensional and it follows from (4.2) that its discriminant is $-z$, where z is the last entry in the first row of Δ^{2c-1}. In this case $\Delta = g - g^{-1} = \begin{pmatrix} -a_0 R & aU \\ 0 & a_0 R \end{pmatrix}$, $R = B - B^{-1}$ and $U = S + B^{-1}SB$.

The matrix R^{c-1} is zero everywhere except for the last entry in the top row, which is 2^{c-1} and therefore $\Delta^{2c-1} = \begin{pmatrix} 0 & (-1)^{c-1} a R^{c-1} U R^{c-1} \\ 0 & 0 \end{pmatrix}$.

The code for *type2CompanionO* sets $a = (-1)^c 2b$, where b is 1 if $e > 0$ and a non-square if $e < 0$. Thus every entry in Δ^{2c-1} is 0 except for the last entry in the top row, which is $-2^{2c}b$. If $u = (1, 0, \ldots, 0)$, the discriminant of the quadratic space is $\beta(u\Delta^{2c-1}, u) \equiv b \pmod{k^2}$. This means that the function returns an element of $+$ type if $e > 0$ and an element of $-$ type if $e < 0$.

Let g^+ denote the element g with $b = 1$ and let g^- denote g when b is a non-square. Let $g^+_{[m]}$ be the direct sum of m copies of g^+ and let $g^-_{[m]}$ be the direct sum of $m-1$ copies of g^+ and a single copy of g^-. The quadratic space of $g^+_{[m]}$ is $\langle 1, 1, \ldots, 1, 1 \rangle$ and its discriminant is 1, whereas the quadratic space of $g^-_{[m]}$ is $\langle 1, 1, \ldots, 1, b \rangle$ and its discriminant is $b \pmod{k^2}$.

The type of $g^+_{[m]}$ is $-$ if and only if $m \equiv 2$ or $3 \pmod 4$ and $q \equiv 3 \pmod 4$. On the other hand, the type of $g^-_{[m]}$ is $+$ if and only if $m \equiv 2$ or $3 \pmod 4$ and $q \equiv 3 \pmod 4$.

5 Conjugacy classes in symplectic groups (q odd)

In order to preserve the standard alternating form when forming a direct sum of matrices we replace the 'diagonal join' of matrices with their 'central join'.

Symplectic direct sums

If $A \in \mathrm{Sp}(2m, q)$ and $B \in \mathrm{Sp}(2n, q)$ we may write A as the block matrix

$$A = \begin{pmatrix} P & Q \\ R & S \end{pmatrix}.$$

and then the 'central join'

$$A \circ B = \begin{pmatrix} P & 0 & Q \\ 0 & B & 0 \\ R & 0 & S \end{pmatrix}$$

belongs to $\mathrm{Sp}(2m + 2n, q)$.

```
  centralJoin := function( A, B )
    d := NRows(A);
    if d eq 0 then return B; end if;
```

```
    e := NRows(B);
    if e eq 0 then return A; end if;
    assert IsEven(d);
    m := d div 2;
    X := ZeroMatrix(BaseRing(A), d+e, d+e);
    InsertBlock(~X, Submatrix(A, 1,1, m,m), 1,1);
    InsertBlock(~X, Submatrix(A, 1,m+1, m,m), 1,m+e+1);
    InsertBlock(~X, Submatrix(A, m+1,1, m,m), m+e+1,1);
    InsertBlock(~X, Submatrix(A, m+1,m+1, m,m), m+e+1,m+e+1);
    InsertBlock(~X, B, m+1,m+1);
    return X;
end function;

type3Matrix := function(f, plist)
    factors := Factorisation(f);
    h := factors[1][1];
    assert f eq h*factors[2][1];
    X := ZeroMatrix( BaseRing(f), 0, 0 );
    for μ in plist do
        e, m := Explode(μ);
        for i := 1 to m do X := centralJoin(X, type3Companion(h^e)); end for;
    end for;
    return X;
end function;

type1Matrix := function(f, plist)
    X := ZeroMatrix( BaseRing(f), 0, 0 );
    for μ in plist do
        e, m := Explode(μ);
        for i := 1 to m do X := centralJoin(X, type1Companion( f^e )); end for;
    end for;
    return X;
end function;

isSignedPartition := func< π |
    forall{ μ : μ in π |IsEven(μ[1]) or (IsEven(μ[2]) and μ[1] gt 0)} >;

type2Matrix := function(f, plist)
    assert Degree(f) eq 1;
    error if not isSignedPartition( plist ), "not a signed partition";
    a0 := Coefficient(f,0);
    F := BaseRing(f);
    q := #F;
    X := ZeroMatrix( F, 0, 0 );
    for μ in plist do
        e, m := Explode(μ);
        if IsOdd( e ) then
            for i := 1 to (m div 2) do
```

```
        X := centralJoin( X, type2CompanionS( a_0, e ) );
      end for;
    else
      X := ((q mod 4 eq 1) or (m mod 4 in {0,1}))
        select centralJoin(X, type2CompanionO(a_0, e))
        else centralJoin(X, type2CompanionO(a_0, -e));
      for i := 2 to m do
        X := centralJoin(X, type2CompanionO( a_0, Abs(e)));
      end for;
    end if;
  end for;
  return X;
end function;
```

Class invariants and representatives

```
intrinsic InternalRepMatrixSp( inv :: SetIndx[Tup] ) -> GrpMatElt
{A representative of the symplectic conjugacy class with
 invariant inv}
 F := BaseRing(Parent(inv[1][1]));
 X := ZeroMatrix( F, 0, 0 );
 for polpart in inv do
   f, plist := Explode(polpart);
   if (Degree(f) eq 1) then
     X := centralJoin(X, type2Matrix(f, plist));
   elif IsIrreducible(f) then
     X := centralJoin(X, type1Matrix(f, plist));
   else
     X := centralJoin(X, type3Matrix(f, plist));
   end if;
 end for;
 return SymplecticGroup(Nrows(X), F) ! X;
end intrinsic;
```

The class invariants can be constructed in several steps. Firstly, choose a partition $\nu = [n_1, n_2, \ldots, n_k]$ of d where the parts n_i are restricted to the set of degrees of the $*$-irreducible polynomials, namely $\{1, 2, 4, \ldots\}$. If ν has m parts of size n, choose m polynomials of degree n (with repetition) represented as a list ξ of pairs, where $\langle f, r \rangle$ indicates that the polynomial f of degree n has been chosen r times.

Secondly, refine ξ by replacing each pair $\langle f, r \rangle$ by $\langle f, \lambda \rangle$, where λ is a partition of r. Moreover, if the degree of f is 1, ξ must be replaced by a sequence of pairs $\langle f, \mu \rangle$, where μ runs through all signed partitions obtained by adding signs to λ. This refinement step is carried out by the following function.

```
refine := function(ξ, addsign)
  Λ := [{@ @}];
  for η in ξ do
    Γ := [];
```

```
      f, r := Explode(η);
      for λ in Partitions(r) do
        for π in Λ do
          β := convert(λ);
          if addsign then
            if forall{ b : b in β | IsEven(b[1]) or IsEven(b[2]) } then
              evens := { i : i in [1..#β] | IsEven(β[i][1]) };
              for T in Subsets(evens) do
                μ := β;
                for i in T do
                  e, m := Explode(β[i]);
                  μ[i] := < −e, m >;
                end for;
                Append(~Γ, Include(π, <f, μ>));
              end for;
            end if;
          else
            Append(~Γ, Include(π, <f, β> ));
          end if;
        end for;
      end for;
      Λ := Γ;
    end for;
    return Λ;
  end function;

  signedPartitions := func< d | addSignsSp([convert(π) : π in Partitions(d)]) >;
```

The invariants for the unipotent conjugacy classes in the symplectic group $\mathrm{Sp}(d, q)$. If Subset is `Semisimple` (rep. `Unipotent`), only the invariants for the semisimple (resp. unipotent) classes are returned.

```
  intrinsic InternalClassInvariantsSp( d :: RngIntElt, q :: RngIntElt : Subset := "All")
      → SeqEnum
  { The conjugacy class invariants for the symplectic group Sp(d,q) }
    require IsEven(d): "d must be even";
    require IsOdd(q) or Subset eq "Semisimple": "q must be odd";
    if Subset eq "Unipotent" then
      t := PolynomialRing(GF(q)).1;
      return [ {@ <t − 1, part> @} : part in signedPartitions(d) ];
    end if;
    deg := [1] cat [2. . d by 2];
    pols := [];
    polsz := [];
    for k in deg do
      pols[k] := StarIrreduciblePolynomials(GF(q), k);
      polsz[k] := { 1..#pols[k] };
    end for;
```

```
    degptns := RestrictedPartitions(d, Set(deg));
    degptnz := [convert(λ) : λ in degptns];
    inv := [];
    for δ in degptnz do
      prev := [{@ @}];
      for term in δ do
        ss := [];
        n, m := Explode(term);
        pp := pols[n];
        for S in Multisets(polsz[n], m) do
          if Subset eq "Semisimple" then
            Ξ := [{@ @}];
            for i -> r in S do
              Ξ := [ Include(π, <pp[i], [<1, r>]>) : π in Ξ | n ne 1 or IsEven(r) ];
            end for;
          else
            ξ := [ < pp[i], r > : i -> r in S ];
            Ξ := refine(ξ, n eq 1);
          end if;
          for stub in prev do
            for π in Ξ do Append(~ss, stub join π); end for;
          end for;
        end for;
        prev := ss;
      end for;
      inv cat:= ss;
    end for;
    return inv;
  end intrinsic;
```

Centraliser orders

The centraliser orders of elements of the symplectic group can be computed using Wall's functions $A(\varphi^{\mu})$ and $B(\varphi)$ from [16]. Here f is a polynomial and $\langle e, m\rangle$ is a term from the partition list.

```
  A_fn := function(f, e, m, q)
    d := Degree(f);
    if IsIrreducible(f) then
      if d eq 1 then
        if IsOdd(e) then
          val := OrderSp(m, q);
        else
          if IsOdd(m) then
            val := OrderGO(m, q);
          elif (e lt 0) then
            val := OrderGOMinus(m, q);
          else
```

```
          val := OrderGOPlus(m, q);
        end if;
      end if;
    else
      val := OrderGU(m, q^(d div 2));
    end if;
  else
    val := OrderGL(m, q^(d div 2));
  end if;
  return val;
end function;

κ := function(plist, d)
  val := 0;
  for μ in plist do
    e, m := Explode(μ);
    val +:= (Abs(e)−1)∗m^2;
    if d eq 1 and IsEven(e) then val +:= m; end if;
  end for;
  for i := 1 to #plist−1 do
    e := Abs(plist[i][1]);
    m := plist[i][2];
    for j := i+1 to #plist do val +:= 2∗e∗m∗plist[j][2]; end for;
  end for;
  val ∗:= d;
  assert IsEven(val);
  return val div 2;
end function;
```

Here *pol_part* has the form $\langle f, [\ \dots\ , \langle e, m \rangle, \ \dots\ ] \rangle$.

```
B_fn := function(pol_part)
  f, plist := Explode(pol_part);
  q := #BaseRing(f);
  d := Degree(f);
  return q^κ(plist, d) ∗ &∗[A_fn(f, μ[1], μ[2], q) : μ in plist];
end function;

centraliserOrderSp := func< inv | &∗[ B_fn(pol_part) : pol_part in inv ] >;
```

The conjugacy classes of $\mathrm{Sp}(d, q)$, q odd

As well as returning the conjugacy classes we return the labels.

```
classesSp := function(d, q)
  ord := OrderSp(d, q);
  L := InternalClassInvariantsSp(d, q);
  cc := [car<Integers(), Integers(), Sp(d, q)>|
    < Order(M), ord div centraliserOrderSp(μ), M > : μ in L | true
```

```
            where M is InternalRepMatrixSp(μ) ];
    ParallelSort(~cc, ~L);
    return cc, L;
end function;
```

6 The conjugacy class invariant of a symplectic matrix

In the previous section we provided code to construct a representative of a conjugacy class invariant. The code in this section does the converse and computes the conjugacy class invariant of a symplectic matrix.

Guided by Lemma 4.5 we shall define a function *homocyclicSplit* designed to be applied to a matrix g acting on a primary component $V_{(f)}$. But first we need a function that returns the row indices for the homocyclic components of the rational canonical form of the matrix g. (We use this only when the polynomial is $t \pm 1$.)

```
getSubIndices := function(pFact)
    f := pFact[1][1];
    error if exists{ p : p in pFact | p[1] ne f },
      "the component is not homocyclic";
    d := Degree(f);
    ndx := 0;
    base := [];
    last := 0;
    rng := [];
    for j := 1 to #pFact do
      if j gt 1 and pFact[j][2] ne last then
        Append(~base, rng);
        rng := [];
      end if;
      last := pFact[j][2];
      n := last*d;
      rng cat:= [ndx+i : i in [1..n]];
      ndx +:= n;
    end for;
    Append(~base, rng);
    return base;
end function;
```

We also need the restriction of a linear transformation (defined by a matrix M) to an invariant subspace; S is either the basis matrix for the subspace or a sequence of basis vectors. (There is no check that the subspace is invariant.)

```
restriction := func< M, S | Solution(T, T*M) where T is Matrix(S) >;
```

In the following function W represents a primary component of g.

```
homocyclicSplit := function(g, W)
    U := Universe([ W, sub<W|> ]);
    _, T, pFact := PrimaryRationalForm(g);
```

```
    baseNdx := getSubIndices(pFact);
    W_0 := sub< W | [T[i] : i in baseNdx[#baseNdx]] >;
    D := [U| W_0 ];
    while W ne W_0 do
      W0p := OrthogonalComplement(W, W_0);
      gp := restriction(g, BasisMatrix(W0p));
      _, T, pFact := PrimaryRationalForm(gp);
      baseNdx := getSubIndices(pFact);
      W_1 := sub< W | [T[i]*BasisMatrix(W0p) : i in baseNdx[#baseNdx]] >;
      Append(~D, W_1);
      W_0 := sub< W | W_0, W_1 >;
    end while;
    return Reverse(D);
  end function;
```

In the following function D is the subspace V^e obtained from *homocyclicSplit*, g is the matrix acting on the generic space of D, f is the polynomial $t+1$ or $t-1$ and μ is the pair $\langle e, m \rangle$.

The matrix B represents the symmetric form $(u) \circ (v)$ defined on $H^e = V^e / V^e f(g)$ as in Theorem 4.9.

```
  attachSign := function(D, g, f, μ)
    F := BaseRing(g);
    a_0 := Evaluate(f, 0);
    e, m := Explode(μ);
    A := g + ScalarMatrix(F, Nrows(g), a_0);
    D_0 := sub< D | [v*A : v in Basis(D)] >;
    E := [v : v in ExtendBasis(D_0, D) | v notin D_0];
    assert #E eq m;
    δ := (g - g^-1)^(e-1);
    B := Matrix(F, m, m, [DotProduct(D ! (u*δ), v) : u, v in E ]);
    d := Determinant(B);
    assert d ne 0;
    sq, _ := IsSquare(d);
```

If the determinant of B is a square, $m \equiv 2$ or $m \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$, the sign is $-$. On the other hand, if the determinant of B is a non-square, $m \equiv 2$ or $m \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$, the sign is $+$.

```
    flag := (m mod 4 in {2,3}) and (#F mod 4 eq 3);
    return (sq and not flag) or (not sq and flag) select μ else < -e, m>;
  end function;
```

Given a symplectic matrix g, we find the invariant of its conjugacy class, following Wall [16] and Milnor [10]. First obtain the generalised Jordan decomposition and then treat the components whose minimal polynomials are powers of $t-1$ or $t+1$ specially.

```
  intrinsic InternalConjugacyInvariantSp( g :: GrpMatElt ) -> SetIndx[Tup]
  { The conjugacy class invariant of the symplectic matrix g }
    F := BaseRing(g);
    J := StandardAlternatingForm(Nrows(g), F);
    if g*J*Transpose(g) ne J then
```

```
      _, alt := InvariantBilinearForms(Parent(g));
      error if IsEmpty(alt), "the parent of g is not a symplectic group";
      J := alt[1];
    end if;
    _, T, pFact := PrimaryRationalForm(g);
    V := SymplecticSpace(J);
    pols, parts, bases := primaryParts(pFact);
    inv := {@ @};
    for i := 1 to #pols do
      f := pols[i];
      plist := convert(parts[i]);
      if Degree(f) eq 1 then
        base := bases[i];
```

Extract the f-primary component W as a symplectic space with the g-action given by *gg*.

```
        gg := restriction(g, [T[j] : j in base]);
        d := #base;
        B := Matrix(F, d, d, [DotProduct(V ! T[r], V ! T[s]) : r, s in base]);
        W := SymplecticSpace(B);
        D := homocyclicSplit(gg, W);
        for j := 1 to #plist do
          if IsEven(plist[j][1]) then
            plist[j] := attachSign(D[j], gg, f, plist[j]);
          end if;
        end for;
      end if;
      Include(~inv, <f, plist> );
    end for;
    return inv;
  end intrinsic;
```

The following intrinsic is a variant of the old ClassRepresentativesSp.

```
  intrinsic InternalSymplecticClasses(G :: GrpMat : Subset := "All")
     -> SeqEnum, SetIndx
  {Conjugacy class representatives and labels for the standard
   symplectic group. The parameter Subset is either "Unipotent",
   "Semisimple" or "All" (the default)}
    require Subset in {"Unipotent", "Semisimple", "All"}:
      "invalid Subset";
    F := BaseRing(G);
    d := Dimension(G);
    q := #F;
    M := StandardAlternatingForm(d, F);
    require forall{ g : g in Generators(G) | g*M*Transpose(g) eq M }:
      "G is not a standard symplectic group";
    if IsOdd(q) or Subset eq "Semisimple" then
      L := InternalClassInvariantsSp(d, q : Subset := Subset);
```

```
    ord := OrderSp(d, q);
    cc := [car<Integers(), Integers(), Sp(d, q)>|
      < Order(M), ord div centraliserOrderSp(μ), M > : μ in L | true
        where M is InternalRepMatrixSp(μ) ];
    ParallelSort(~cc, ~L);
    L := [ tagToNameSp(μ) : μ in L ];
  else
    fn := case <Subset |
      "Unipotent" : UnipotentClasses,
       default : ClassicalConjugacyClasses >;
    cc, L := fn("Sp", d, q);
  end if;
  return cc, {@ x : x in L @};
end intrinsic;
```

7 The number of conjugacy classes in $\mathrm{Sp}(2n, q)$

7.1 q odd

It has been shown by Wall [16] that when the prime power q is odd, the number of conjugacy classes in $\mathrm{Sp}(2n, q)$ is the coefficient of $2n$ in the formal power series

$$\prod_{k=1}^{\infty} \frac{(1+t^{2k})^4}{1-qt^{2k}} .$$

Using a calculation similar to that for $\mathrm{GL}(n, q)$ this formal power series becomes (see Macdonald [8])

$$\prod_{k=1}^{\infty}(1+t^{2k})^4 \sum_{r=0}^{\infty} q^r t^{2r} \prod_{k=1}^{r}(1-t^{2k})^{-1}.$$

```
TruncatedEulerProduct := function(t, s, m)
  P := Parent(t);
  f := P ! 1;
  if m eq 0 then return f; end if;
  for j := 1 to Min(m, s) do
    f *:= &+[P| t^(j*i) : i in [0..(m div j)]];
  end for;
  c := Rank(P) eq 1 select Coefficients(f) else Coefficients(f, t);
  return &+[c[i+1]*t^i : i in [0..Min(#c-1, m)]];
end function;

intrinsic NClassesSpOdd(n :: RngIntElt) → RngUPolElt
{The number of conjugacy classes of Sp(n,q), q odd, as a
 polynomial in q}
  require IsEven(n) : "n must be even";
  d := n div 2;
```

```
  P<t,qq> := PolynomialRing(Integers(), 2);
  gf := P ! 0;
  for r := 0 to d do
    gf +:= qq^r * t^(2*r) * Evaluate(TruncatedEulerProduct(t, r, n-2*r), [t^2, 1]);
  end for;
  gf *:= &*[ (1+t^(2*k))^4 : k in [1..d]];
  _<q> := PolynomialRing(Integers());
  return Evaluate(Coefficient(gf, t, n), [1, q]);
end intrinsic;
```

7.2 q even

Wall [16] has shown that when q is a power of 2, the number of conjugacy classes in $\mathrm{Sp}(2n, q)$ is the coefficient of t^{2n} in the formal power series

$$\chi(t^2) \prod_{k=1}^{\infty} (1 - qt^{2k})^{-1} .$$

where $\chi(t)$ is defined as follows. First define a sequence of polynomials $\chi_{-1}(t)$, $\chi_0(t)$, $\chi_1(t)$, ..., where

$$\begin{aligned}
\chi_{-1}(t) &= 0, \\
\chi_0(t) &= 1, \\
\chi_{2k+1}(t) - \chi_{2k}(t) &= t^{2k+1}\chi_{2k-1}(t), \\
\chi_{2k+2}(t) - \chi_{2k+1}(t) &= t^{k+1}(1 + t^{k+1})(\chi_{2k+1}(t) + (1 - t^{2k+1})\chi_{2k-1}(t)),
\end{aligned}$$

then let $\chi(t)$ be the formal power series such that

$$\chi(t) \equiv \chi_{2k}(t) \pmod{t^k} \quad \text{for } r = 0, 1, 2, \ldots$$

The following MAGMA function returns $\chi_\nu(t)$.

```
χ := function(ν)
  P<x> := PolynomialRing(Integers());
  val := P ! 0;
  if ν eq -1 then
    val := P ! 0;
  elif ν eq 0 then
    val := P ! 1;
  elif IsEven(ν) then
    μ := ν div 2;
    ψ := $$(ν-1);
    val := ψ + x^μ*(1+x^μ)*(ψ+(1-x^(ν-1))*$$(ν-3));
  else    // if IsOdd(nu) then
    val := $$(ν-1) + x^ν * $$(ν-2);
```

```
  end if;
  return val;
end function;

intrinsic NClassesSpEven(n :: RngIntElt) → RngUPolElt
{The number of conjugacy classes of Sp(n,q), q a power of 2,
 as a polynomial in q}
  require IsEven(n) : "n must be even";
  d := n div 2;
  P<t,qq> := PolynomialRing(Integers(),2);
  gf := P ! 0;
  for r := 0 to d do
    gf +:= qq^r * t^(2*r) * Evaluate(TruncatedEulerProduct(t,r,n-2*r),[t^2,1]);
  end for;
  g := χ(n+2);
  cf := Coefficients(g)[1..d+1];
  gf *:= &+[ cf[i]*t^(2*(i-1)) : i in [1..d+1]];
  _<q> := PolynomialRing(Integers());
  return Evaluate(Coefficient(gf,t,n),[1,q]);
end intrinsic;
```

8 Test code

```
testDual := procedure()
  print "Test DualPolynomial";
  for q in [11,25] do
    F := GF(q);
    P<t> := PolynomialRing(F);
    for i := 1 to 5 do
      lst :=[ Random(F) : i in [1..6]];
      if lst[1] ne 0 and lst[6] ne 0 then
        assert Dual(P ! lst) eq DualPolynomial(P ! lst);
      end if;
    end for;
  end for;
  print "Passed\n";
end procedure;

testDual();

test0sp := procedure(n,q)
  print "Test 0: compare with Classes(G)";
  G := SymplecticGroup(n,q);
  reps := Classes(G);
  delete G;
  G := SymplecticGroup(n,q);
```

```
    cc := Classes(G : Al := "Random");
    ndx := [];
    for X in reps do
      assert exists(i){ i : i in [1..#cc] | IsConjugate(G, X[3], cc[i][3]) };
      Append(~ndx, i);
    end for;
    assert #reps eq #SequenceToSet(ndx);
    print "Passed\n";
  end procedure;

  test0sp(4, 3);

  test1sp := procedure(n, r)
    printf "Test 1: class sizes for Sp(%o,%o)\n", n, r;
    f := NclassesSpOdd(n);
    #ClassInvariantsSp(n, r) eq Evaluate(f, r);
  end procedure;

  test1sp(6, 5);

  test2sp := procedure(n, r)
    printf "Test 2: conjugacy invariants for Sp(%o,%o)\n", n, r;
    for μ in ClassInvariantsSp(n, r) do
      g := InternalRepMatrixSp(μ);
      c := InternalConjugacyInvariantSp(g);
      assert μ eq c;
    end for;
    print "Passed\n";
  end procedure;

  test2sp(4, 3);
  test2sp(6, 5);

  test3sp := procedure(n, r)
    printf "Test 3: centraliser orders for Sp(%o,%o)\n", n, r;
    S := Sp(n, r);
    for μ in ClassInvariantsSp(n, r) do
      g := InternalRepMatrixSp(μ);
      assert #Centraliser(S, g) eq CentraliserOrderSp(μ);
    end for;
    print "Passed\n";
  end procedure;

  test3sp(4, 3);
```

Conjugacy invariants (randomised)

```
  test4sp := procedure(n, r)
    printf "Randomised conjugacy invariants for Sp(%o,%o)\n", n, r;
    G := Sp(n, r);
```

```
    for μ in ClassInvariantsSp(n, r) do
      g := InternalRepMatrixSp(μ);
      h := Random(G);
      c := InternalConjugacyInvariantSp(g^h);
      assert μ eq c;
    end for;
    print "Passed\n";
  end procedure;

  test4sp(4, 5);
  test4sp(8, 5);
```

References

[1] J. R. Britnell. *Cycle index methods for matrix groups over finite fields*. DPhil Thesis, University of Oxford, 2003.

[2] S. Haller and S. H. Murray. Computing conjugacy in finite classical groups 1: similarity in unitary groups. preprint, January 2009.

[3] W. H. Hesselink. Nilpotency in classical groups over a field of characteristic 2. *Math. Z.*, 166(2):165–181, 1979.

[4] J. E. Humphreys. *Conjugacy classes in semisimple algebraic groups*, volume 43 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1995.

[5] B. Huppert. Isometrien von Vektorräumen. I. *Arch. Math. (Basel)*, 35(1-2):164–176, 1980.

[6] B. Huppert. Isometrien von Vektorräumen. II. *Math. Z.*, 175(1):5–20, 1980.

[7] M. W. Liebeck and G. M. Seitz. *Unipotent and nilpotent classes in simple algebraic groups and Lie algebras*, volume 180 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2012.

[8] I. G. Macdonald. Numbers of conjugacy classes in some finite classical groups. *Bull. Austral. Math. Soc.*, 23(1):23–48, 1981.

[9] I. G. Macdonald. *Symmetric functions and Hall polynomials*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1995. With contributions by A. Zelevinsky, Oxford Science Publications.

[10] J. Milnor. On isometries of inner product spaces. *Invent. Math.*, 8:83–97, 1969.

[11] S. H. Murray. Computing conjugacy in finite classical groups 2: similarity in symplectic and orthogonal groups. preprint, July 2007.

[12] C. Riehm. The equivalence of bilinear forms. *J. Algebra*, 31:45–66, 1974.

[13] K. Shinoda. The characters of Weil representations associated to finite fields. *J. Algebra*, 66(1):251–280, 1980.

[14] T. A. Springer. *Over Symplectische Transformaties*. Thesis. University of Leiden, 1951.

[15] T. A. Springer and R. Steinberg. Conjugacy classes. In *Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69)*, Lecture Notes in Mathematics, Vol. 131, pages 167–266. Springer, Berlin, 1970.

[16] G. E. Wall. On the conjugacy classes in the unitary, symplectic and orthogonal groups. *J. Aust. Math. Soc.*, 3:1–62, 1963.

[17] J. Williamson. On the normal forms of linear canonical transformations in dynamics. *Amer. J. Math.*, 59(3):599–617, 1937.

[18] J. Williamson. Normal matrices over an arbitrary field of characteristic zero. *Amer. J. Math.*, 61(2):335–356, 1939.

[19] T. Xue. Nilpotent orbits in classical Lie algebras over finite fields of characteristic 2 and the Springer correspondence. *Represent. Theory*, 13:371–390, 2009.

Revision history

2016-05-12 Installed in the MAGMA package tree.

2018-01-19 Changed to Milnor's order of types.

2020-09-07 Faster version of *convert*.

2020-09-12 New algorithm to compute conjugacy invariants.

2020-09-17 Removed the restriction to standard symplectic groups.

2020-10-27 Revised the labels for conjugacy invariants.

2021-03-20 Added LABELS_A and LABELS_S attributes to GRPMAT.

2021-03-21 The intrinsics SEMISIMPLEINVARIANTSSP and UNIPOTENTINVARIANTSSP have changed to functions. New intrinsic INTERNALSYMPLECTICCLASSES allows subsets.

2021-04-28 Changed the intrinsic CLASSINVARIANTSSP to INTERNALCLASSINVARIANTSSP and also changed CENTRALISERORDERSP to a function *centraliserOrderSp*. The two functions SEMISIMPLEINVARIANTSSP and UNIPOTENTINVARIANTSSP have been incorporated into the intrinsic INTERNALCLASSINVARIANTSSP.

2021-05-02 Removed CLASSREPRESENTATIVESSP.

2021-05-06 Changed CONJUGACYINVARIANTSP to INTERNALCONJUGACYINVARIANTSP.