Conjugacy Classes in Finite Conformal Symplectic Groups

D. E. Taylor

Version of 6 May, 2021
TEXed: 21 August, 2021

This treatment of the conformal symplectic groups is modelled on the report 'Conjugacy Classes in Finite Symplectic Groups'. It is a revision of the C code of Sergei Haller (in `classes_classical.c`) and the package code of Scott Murray (in `symplectic.m`).

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 There are some remarks about the conformal symplectic groups in the unpublished draft [5]. A more extended account is in Chapter 5 of Britnell's thesis [1] and a description of the invariants, based on the work of Wall [8], Springer and Steinberg [7] and Milnor [4] can be found in the Shinoda's paper [6].

1 Conformal symplectic groups

The 'standard' alternating form $J = J_n$ 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 conformal symplectic group $\mathrm{CSp}(2n, q)$ considered here is the set of $2n \times 2n$ matrices A over the field $k = \mathrm{GF}(q)$ such that for each A there is a non-zero element $\phi = \phi(A)$ in k such that $AJA^{\mathrm{tr}} = \phi(A)J$, where A^{tr} is the transpose of A. We say that A preserves the alternating form $\beta(u, v) = uJv^{\mathrm{tr}}$ *with multiplier* ϕ.

It is immediate that $\phi : \mathrm{CSp}(2n, q) \to k^\times$ is a homomorphism. If Q is the subgroup $\left\{ \begin{pmatrix} aI & 0 \\ 0 & I \end{pmatrix} \,\middle|\, a \in k^\times \right\}$, then $Q \cap \mathrm{Sp}(2n, q) = 1$ and $\mathrm{CSp}(2n, q) = \mathrm{Sp}(2n, q)Q$. It follows that ϕ is surjective and its kernel is $\mathrm{Sp}(2n, q)$. That is, $g_1, g_2 \in \mathrm{CSp}(2n, q)$ are in the same coset of $\mathrm{Sp}(2n, q)$ if and only if $\phi(g_1) = \phi(g_2)$. The centre Z of $\mathrm{CSp}(2n, q)$ is the group of $q - 1$ non-zero scalar matrices and $|\,\mathrm{CSp}(2n, q) : Z \circ \mathrm{Sp}(2n, q)|$ is 2 if q is odd and 1 if q is a power of 2. Let $\mathrm{CSp}_\phi(2n, q)$ denote the coset of elements of $\mathrm{CSp}(2n, q)$ with multiplier ϕ.

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

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 $f \in k[t]$.

As shown in Macdonald [3, 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 $\mu(f) = (\mu_1(f), \mu_2(f), \ldots,)$ is a partition such that

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

If $g \in \mathrm{CSp}(2n, q)$ there are restrictions on the polynomials and partitions that can occur in this decomposition. The elements $g, h \in \mathrm{CSp}(2n, q)$ are conjugate in $\mathrm{CSp}(2n, q)$ if and only if there is an isomorphism of $k[t]$-modules $T : V_g \to V_h$ such that $T \in \mathrm{CSp}(2n, q)$.

The functions listed in the following **import** statement were defined in `SpConjugacy.tex` and written to the file `common.m`. The code is included in this file (coloured red) but not written to the MAGMA file `CSpConjugacy.m`.

```
import "common.m" : convert, allPartitions, signedPartitionsSp, stdJordanBlock,
    centralJoin, getSubIndices, restriction, homocyclicSplit;
import "SpConjugacy.m" : classesSp, centraliserOrderSp;
```

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

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

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

A conjugacy calculation

Let g_1 and g_2 be elements of $\mathrm{CSp}_\phi(V)$ and suppose that g_1 and g_2 are conjugate in $\mathrm{GL}(V)$. Then there are linear transformations ρ_1, ρ_2 and $\kappa \in \mathrm{GL}(V)$ such that

$$\rho_1 g_1 \rho_1^{-1} = \kappa = \rho_2 g_2 \rho_2^{-1}.$$

For $i = 1, 2$ define $\gamma_i(u, v) = \beta(u\rho_i, v\rho_i)$ and observe, as in Williamson [9], that

$$\gamma_i(u\kappa, v\kappa) = \phi\gamma_i(u, v).$$

Lemma 1.2. *Using the notation just established, $g_1 = \alpha^{-1} g_2 \alpha$ for some $\alpha \in \mathrm{Sp}(V)$ if and only if there exists $\theta \in \mathrm{GL}(V)$ such that $\theta\kappa = \kappa\theta$ and $\gamma_2(u, v) = \gamma_1(u\theta, v\theta)$.*

Proof. Suppose that $\theta\kappa = \kappa\theta$ and $\gamma_2(u, v) = \gamma_1(u\theta, v\theta)$. Let $\alpha = \rho_2^{-1}\theta\rho_1$. Then

$$\alpha^{-1} g_2 \alpha = \rho_1^{-1}\theta\rho_2 g_2 \rho_2^{-1}\theta\rho_1 = \rho_1^{-1}\theta\kappa\theta\rho_1 = \rho_1^{-1}\kappa\rho_1 = g_1$$

and

$$\beta(u\alpha, v\alpha) = \beta(u\rho_2^{-1}\theta\rho_1, v\rho_2^{-1}\theta\rho_1) = \gamma_1(u\rho_2^{-1}\theta, v\rho_2^{-1}\theta)$$
$$= \gamma_2(u\rho_2^{-1}, v\rho_2^{-1}) = \beta(u, v).$$

Conversely, suppose that $g_1 = \alpha^{-1}g_2\alpha$ for some $\alpha \in \mathrm{Sp}(V)$ and let $\theta = \rho_2\alpha\rho_1^{-1}$. Then $\theta\kappa = \kappa\theta$ and $\gamma_2(u, v) = \gamma_1(u\theta, v\theta)$. □

The following corollary is used implicitly in several places in Chapter 5 of [1].

Corollary 1.3. *Suppose that $g \in \mathrm{CSp}_\phi(V)$ and that for all non-degenerate alternating forms γ preserved by g with multiplier ϕ there exists $\theta \in \mathrm{GL}(V)$ which commutes with g and satisfies $\gamma(u, v) = \beta(u\theta, v\theta)$. Then for all $h \in \mathrm{CSp}_\phi(V)$, if h is conjugate to g in $\mathrm{GL}(V)$, there exists an element of $\mathrm{Sp}(V)$ which conjugates h to g.*

Polynomials

Definition 1.4.

(i) Given $\phi \in k^\times$ and a polynomial $f(t)$ of degree d such that $f(0) \neq 0$, the *ϕ-dual* of $f(t)$ is
$$f^{[\phi]}(t) = f(0)^{-1}t^d f(\phi t^{-1}).$$
The polynomial $f(t)$ is *ϕ-symmetric* if $f^{[\phi]}(t) = f(t)$. Thus $f(t)$ is ϕ-symmetric if and only if $t^d f(\phi t^{-1}) = f(0)f(t)$. For example $t^2 - \phi$ and $t^2 + \phi$ are ϕ-symmetric and if $\phi = \lambda^2$, then $t - \lambda$ and $t + \lambda$ are ϕ-symmetric.

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

If $f(t)$ is a monic polynomial such that $f(0) \neq 0$, then $f^{[\phi][\phi]}(t) = f(t)$. Furthermore, the monic polynomial $f(t) = a_0 + a_1t + \cdots + a_{d-1}t^{d-1} + t^d$ is ϕ-symmetric if and only if

$$a_0^2 = \phi^d \quad \text{and} \quad \phi^{d-i}a_{d-i} = a_0a_i \quad \text{for } 0 < i < d. \tag{1.2}$$

Thus an element a in an extension field of k is a root of $f(t)$ if and only if ϕa^{-1} is also a root.

Remark 1.5.

(i) An irreducible polynomial may have the same ϕ-dual for more than one value of ϕ. For example, if $k = \mathbb{F}_5$ and $f(t) = t^4 + 2$, then $f(t)$ is irreducible and $f^{[2]}(t) = f^{[4]}(t) = t^4 + 3$.

(ii) It is possible for a polynomial to be ϕ-symmetric for several values of ϕ. For example, if ζ is a primitive element of $k = \mathbb{F}_{25}$ and $f(t) = t^6 + \zeta t^3 + 3$, then $f(t) = f^{[2]}(t) = f^{[1+\zeta]}(t) = f^{[2-\zeta]}(t) = (t^3 + 1 + 2\zeta)(t^3 - 1 - \zeta)$.

```
intrinsic PhiDual(f :: RngUPolElt, ϕ :: FldFinElt) → RngUPolElt
{The phi-dual of the polynomial f}
  eseq := Coefficients(f);
  require eseq[1] ne 0 : "Polynomial must have non-zero constant term";
```

```
    dseq := [ eseq[i]*phi^(i-1) : i in [1..#eseq] ];
    return dseq[1]^-1 * Parent(f) ! Reverse(dseq);
end intrinsic;
```

Lemma 1.6. *If $\beta(ug, vg) = \phi\beta(u, v)$ for all $u, v \in V$, then for all $f(t) \in k[t]$ we have $f(g)^* = f(\phi g^{-1})$; that is,*

$$\beta(uf(g), v) = \beta(u, vf(\phi g^{-1})). \tag{1.3}$$

Corollary 1.7. *If $m(t)$ is the minimal polynomial of g, then $m(t)$ is ϕ-symmetric.*

Proof. It follows from the lemma that $vm(\phi g^{-1}) = 0$ for all $v \in V$ and so $g^e m(\phi g^{-1}) = 0$, where e is the degree of $m(t)$. Thus $m(t)$ divides $t^e m(\phi t^{-1})$ and hence $m(t)$ is ϕ-symmetric. □

Lemma 1.8. *Let $f(t)$ be a monic ϕ-irreducible polynomial.*

(i) *If $f(t)$ is reducible, there exists an irreducible polynomial $h(t)$ such that $f(t) = h(t)h^{[\phi]}(t)$ and $h(t) \neq h^{[\phi]}(t)$.*

(ii) *If the degree of $f(t)$ is $2d$, then $f(0) = \phi^d$ or ϕ is not a square and $f(t) = t^2 - \phi$.*

(iii) *If $f(t)$ is irreducible and of odd degree, then $\phi = \lambda^2$ for some $\lambda \in k$ and $f(t)$ is either $t - \lambda$ or $t + \lambda$.*

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

Proof. (i) Suppose that $h(t)$ is an irreducible factor of $f(t)$. Then $h^{[\phi]}(t)$ divides $f^{[\phi]}(t) = f(t)$ and since $f(t)$ is ϕ-irreducible $f(t) = h(t)h^{[\phi]}(t)$ or $f(t) = h(t)$.

(ii) Suppose that the degree of $f(t)$ is $2d$. Then $a_0^2 = \phi^{2d}$ and hence $a_0 = \pm\phi^d$. Thus we may suppose that the characteristic of the field is not 2. If $a_0 = -\phi^d$ then (1.2) becomes $a_i = -\phi^{d-i}a_{2d-i}$ and hence $a_d = 0$. Then for $0 \le i \le d$ we have $a_{d-2i}t^{2d-i} + a_i t^i = a_{d-2i}t^i(t^{2(d-i)} - \phi^{d-i})$ and consequently the ϕ-symmetric polynomial $t^2 - \phi$ divides $f(t)$ whence $f(t) = t^2 - \phi$. Since $f(t)$ is ϕ-irreducible ϕ cannot be a square in this case.

(iii) Suppose that $f(t)$ is irreducible and that its degree e is odd. We have $a_0^2 = \phi^e$ and hence $\phi = \lambda^2$ for some $\lambda \in k$. Thus $a_0 = \pm\lambda^e$ and (1.2) becomes $\lambda^{e-2i}a_{e-i} = \pm a_i$. It follows that either $f(\lambda) = 0$ or $f(-\lambda) = 0$. Thus $f(t)$ is either $t - \lambda$ or $t + \lambda$, proving (iii).

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

```
intrinsic PhiIrreduciblePolynomials(F :: FldFin, d :: RngIntElt) -> SeqEnum[Tup]
{All pairs <phi,pols> where pols is the sequence of all monic
 polynomials of degree d with no proper phi-symmetric factor}

  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 $h(t)$ of degree d, define $\hat{h}(t) = t^d h(t + \phi t^{-1})$.

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

multGrp := [ φ : φ in F | φ ne 0 ];
m := #multGrp;
polseq := [];
if d eq 1 then
  for i := 1 to m do
    φ := multGrp[i];
    flag, λ := IsSquare(φ);
```

It is essential (for conjugacy testing) that the polynomials of degree 1 occur in the order used by PrimaryInvariantFactors and friends.

```
    polseq[i] := flag select <φ, Sort([t + λ, t − λ])> else <φ, [] >;
  end for;
elif IsEven(d) then
  allhalf := monicIrreducibles(d div 2 );
  for i := 1 to m do
    φ := multGrp[i];
    pols := {@ @};
    if d eq 2 then
      if not IsSquare(φ) then Include(~pols, t^2 − φ); end if;
      if not IsSquare(−φ) then Include(~pols, t^2 + φ); end if;
    end if;
    pols join:= {@ f : g in allhalf | IsIrreducible(f) where f is hatPoly(g,φ) @}
        join {@ g*gphi : g in allhalf | g ne gphi where gphi is PhiDual(g, φ) @};
    polseq[i] := < φ, IndexedSetToSequence(pols) >;
  end for;
end if;
return polseq;
end intrinsic;
```

Partitions

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) ]) >;

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

Definition 1.9. 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.

The justification for the assignment of signs is given at the end of section 3.

```
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;
```

Thus a signed partition π is a list of pairs $\lambda = \langle e, m \rangle$. If e is odd, λ is of *symplectic* type; if e is even, λ is of *orthogonal* type. The absolute value of e will be the exponent of an associated irreducible polynomial.

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

Each conjugacy class of $\mathrm{CSp}(2n, q)$ will be represented by a pair $\langle \phi, \Xi \rangle$, where $\phi \in k^\times$ and Ξ is an indexed set of pairs $\langle f, \mu \rangle$, where f is a ϕ-irreducible polynomial and μ is either a partition or, in the case that f divides $t^2 - \phi$, a signed partition. That is, a conjugacy class invariant has the form $\langle \phi, \{@ \langle f_1, \mu_1 \rangle, \langle f_2, \mu_2 \rangle, \cdots @\} \rangle$.

2 A skew-hermitian form

Throughout this section g is an element of $\mathrm{CSp}(2n, q)$ whose minimal polynomial $m(t)$ is irreducible of degree d. We set $\phi = \phi(g)$ and we follow the exposition in Milnor [4, §1], modified for conformal symplectic groups.

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

By Corollary 1.7 $m(t)$ is ϕ-symmetric and so $m(\phi\tau^{-1}) = 0$. It follows that there is an automorphism $e \mapsto \bar{e}$ of E such that $\bar{\tau} = \phi\tau^{-1}$. The automorphism is the identity if and only if $\tau^2 = \phi$. If $m(t)$ does not divide $t^2 - \phi$ then by Lemma 1.8 the degree of $m(t)$ is even and the automorphism $e \mapsto \bar{e}$ has order 2. In general (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

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

Theorem 2.1. *$u \circ v$ is the unique skew-hermitian inner product on V such that*

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

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

Proof. By definition

$$\operatorname{trace}_{E/k}(e(u \circ v)) = \beta(ue, v) \tag{2.1}$$

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

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

whence

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

Furthermore,

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

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 (2.1) 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 2.2. Suppose that $m(t) \in k[t]$ is an irreducible ϕ-symmetric polynomial and let H be a vector space over the field $E = k[t]/(m(t))$.

If $m(t)$ does not divide $t^2 - \phi$ let $u \circ v$ be a non-degenerate skew-symmetric hermitian form on H whereas, if $m(t)$ divides $t^2 - \phi$, let $u \circ v$ be a non-degenerate alternating 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 $m(\phi\tau^{-1}) = 0$ and $\tau \mapsto \phi\tau^{-1}$ extends to an automorphism of E. Then multiplication by τ satisfies $\beta(u\tau, v\tau) = \phi\beta(u, v)$ and hence belongs to the conformal symplectic group.

3 Orthogonal decompositions

We return to a general element $g \in \mathrm{CSp}(2n, q)$ and set $\phi = \phi(g)$.

3.1 Primary components

Definition 3.1. For each irreducible polynomial $f(t)$, the *f-primary component* of V_g is

$$V_{(f)} = \bigoplus_i k[t]/(f)^{\mu_i(f)} = \{\, v \mid vf(g)^i = 0 \text{ for sufficiently large } i \,\}.$$

Lemma 3.2. *$V_{(f)}$ is orthogonal to $V_{(h)}$ unless $h(t) = f^{[\phi]}(t)$.*

Proof. (cf. Milnor [4]) If $u \in V_{(f)}$ and $v \in V$, then for sufficiently large i

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

and hence $V_{(f)}$ is orthogonal to $Vf^{[\phi]}(g)^i$.

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

$$V_{(h)} \to V_{(h)} : v \mapsto vf(\phi g^{-1})$$

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

Corollary 3.3. *$V = \perp_f \widetilde{V}_{(f)}$, where f ranges over all ϕ-irreducible polynomials and where*

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

Lemma 3.4. *If $f(t)$ is not ϕ-symmetric, then $V_{(f)}$ and $V_{(f^{[\phi]})}$ are totally isotropic and $V_{(f)} \oplus V_{(f^{[\phi]})}$ is non-degenerate.*

Proof. Let $U = V_{(f)}$ and write $V = U \oplus W$, where W is the sum of the h-primary components with $h \neq f$. Then $U^* = W^\perp$ is a $k[t]$-submodule and $\dim U^* = \dim U$.

For all $u \in U$, $v \in U^*$ and $i \geq 1$ we have

$$\beta(uf(g)^i, v) = 0 \quad \text{if and only if} \quad \beta(u, vf^{[\phi]}(g)^i) = 0$$

and therefore $f(g)^i$ vanishes on U if and only if $f^{[\phi]}(g)^i$ vanishes on U^*. (This is a consequence of the equalities $W = W^{\perp\perp}$, $U^\perp \cap W^\perp = 0$ and $U \cap W = 0$.) It follows that $U^* = V_{(f^{[\phi]})}$. But $V_{(f^{[\phi]})} \subseteq W$ and hence U^* is totally isotropic. Reversing the rôles of U and U^* we see that U is also isotropic. It is now clear that $U \oplus U^*$ is non-degenerate. □

The PrimaryRationalForm(X) intrinsic returns the rational form C of X, a transformation matrix T 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 *primaryPhiParts* returns

- the sequence *pols* of ϕ-irreducible polynomials,
- the corresponding sequence *parts* of partitions, and
- a sequence *rows* of row indices giving the location of each primary component.

Then the subspace $V_{(f)}$ can be found using the matrix T. Suppose, for example, 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 $V_{(f)}$.

```
primaryPhiParts := function(φ, 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 PhiDual(f,φ) 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 := PhiDual(f,φ);
      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 := PhiDual(f,φ);
      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 [4] we divide the primary components $\widetilde{V}_{(f)}$, where $f(t)$ is ϕ-irreducible, into three types.

Type 1. $f(t) = f^{[\phi]}(t)$ is irreducible, $f(t) \neq t^2 - \phi$, and the degree of $f(t)$ is even.

Type 2. $f(t) = f^{[\phi]}(t)$ is irreducible and $f(t)$ divides $t^2 - \phi$.

Type 3. $f(t) = h(t)h^{[\phi]}(t)$ and $h(t) \neq h^{[\phi]}(t)$.

Type 3 companion matrices

For $\widetilde{V}_{(f)}$ of type 3, if we choose a basis $v_1, v_2, \ldots, v_r$ for $V_{(h)}$ and the basis $w_1, w_2, \ldots, w_r$ for $V_{(h^{[\phi]})}$ such that $\beta(v_i, w_{r-j+1}) = \delta_{ij}$, the matrices of β and g restricted to $\widetilde{V}_{(f)}$ are

$$\begin{pmatrix} 0 & \Lambda \\ -\Lambda & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} A & 0 \\ 0 & \phi\Lambda A^{-\mathrm{tr}}\Lambda \end{pmatrix}. \tag{3.1}$$

The minimal polynomial of A is $h(t)^s$ for some s and the minimal polynomial of $\phi\Lambda A^{-\mathrm{tr}}\Lambda$ is $h^{[\phi]}(t)^s$.

Theorem 3.5. *Suppose that g and g' are elements of* $\mathrm{CSp}(2n, q)$ *such that $V = k^{2n}$ is a primary component of type 3 for g and g' with the same multiplier ϕ, the same minimal polynomial and the same partition. Then g and g' are conjugate via an element of* $\mathrm{Sp}(2n, q)$. *Therefore* $\mathrm{CSp}(V) = \mathrm{Sp}(V)C_{\mathrm{CSp}(V)}(g)$.

Proof. As shown above it is enough to prove that if γ is a non-degenerate alternating form such that $\gamma(ug, vg) = \phi\gamma(u, v)$ for all $u, v \in V$, there is a matrix K, which commutes with g, such that $\gamma(u, v) = \beta(uK, vK)$ for all $u, v \in V$.

Let L be the matrix such that $\gamma(u, v) = \beta(uL, v)$. Then $LJ = JL^{\mathrm{tr}}$ and $Lg = gL$ and so L fixes the primary components $V_{(h)}$ and $V_{(h^{[\phi]})}$ of g. Hence there is a matrix M such that

$$L = \begin{pmatrix} M & 0 \\ 0 & \Lambda M^{\mathrm{tr}}\Lambda \end{pmatrix}.$$

Therefore $\gamma(u, v) = \beta(uK, vK)$ and $gK = Kg$, where

$$K = \begin{pmatrix} M & 0 \\ 0 & I \end{pmatrix}. \qquad \square$$

As a consequence of this theorem the conjugacy class of $g\,|_{\widetilde{V}_{(f)}}$ is completely determined by the triple $\langle \phi, f, \mu(h) \rangle$, where $f(t) = h(t)h^{[\phi]}(t)$ and every such triple represents a conjugacy class in $\mathrm{CSp}(\widetilde{V}_{(f)})$.

Definition 3.6. Define A to be a *ϕ-symplectic companion matrix* of a polynomial $f(t)$ if $f(t) = \det(tI - A)$ and $AJA^{\mathrm{tr}} = \phi J$.

Given $\phi \in k$ and the companion matrix A of a polynomial $h(t)$ the matrix $\begin{pmatrix} A & 0 \\ 0 & \phi\Lambda A^{-\mathrm{tr}}\Lambda \end{pmatrix}$ is a ϕ-symplectic companion matrix of $h(t)h^{[\phi]}(t)$.

```
type3Companion := function(φ, 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, φ∗Λ∗Transpose(A^−1)∗Λ);
end function;
```

If $h(t)$ is ϕ-symmetric, this code returns a matrix with characteristic polynomial $h(t)^2$ and minimal polynomial $h(t)$. In this case its conjugacy invariant is $< \phi,\ \{ < h,\ [<d, 2>] > \} >$.

An example

Let $k = \mathbb{F}_3$ and consider the matrices

$$h_1 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \quad h_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad h_3 = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix},$$

All three matrices belong to $\mathrm{Sp}(2,3)$ and $(t-1)^2$ is the only primary invariant factor of both h_1 and h_2. The matrices h_1 and h_2 are conjugate in $\mathrm{CSp}(2,3)$ but not in $\mathrm{Sp}(2,3)$. Furthermore, if g_1 is the orthogonal sum of h_1 and h_3 and if g_2 is the orthogonal sum of h_2 and h_3, then g_1 is *not* conjugate to g_2 in $\mathrm{CSp}(4,3)$. Since $V_{g_1} = V_{g_2} = V_{((t-1)^2)} \perp V_{((t+1)^2)}$, this example shows that conjugacy in $\mathrm{CSp}(2n,q)$ cannot be decided by considering the primary components in isolation.

Orthogonal splitting of a primary component

Suppose that $V_{(f)}$ is a primary component of type 1 or 2. In this case $V_{(f)}$ is an orthogonal summand of V_g.

Theorem 3.7. *The space $V_{(f)}$ 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 $k[t]/(f(t)^i)$.*

Proof. (Milnor [4]) From the Jordan decomposition we have $V_{(f)} = W_1 \oplus W_2 \oplus \cdots \oplus W_r$ 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

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

because $f(t) = f^{[\phi]}(t)$ and $i < r$. Thus $u \in V^{\perp} = \{0\}$ contradicting the assumption that β is non-degenerate. Therefore $V_{(f)} = W_r^{\perp} \perp W_r$ and the theorem follows by induction on r. □

Definition 3.8. The $k[t]$-modules V^i are the *homocyclic* components of $V_{(f)}$.

3.2 Primary components of type 1

Lemma 3.9. *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 $s(g)$ is self-adjoint; that is, 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), Lemma 1.8 (ii) and the assumption that $f(t)$ is ϕ-symmetric that

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

□

Corollary 3.10. *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 $vs(g)^i$, $vs(g)^i g$, …, $vs(g)^i g^{2di-1}$ are linearly independent. Thus $\dim V^{2i}s(g)^i = \frac{1}{2}\dim V^{2i}$, as claimed. □

Theorem 3.11 (Milnor [4]). *If $V_{(f)} = V^1 \perp V^2 \perp \cdots \perp V^r$ 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 $V^i/V^i f(g) \cong V(i)/(V(i-1) + V(i+1)f(g))$ 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, the results of section 2 apply to H^i.

From the previous lemma and the comment following Definition 1.1, 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 2.1. □

3.3 The endomorphism ring of a homocyclic component

This section connects Milnor's approach with that of Britnell [1, Chapter 5] and Wall [8, §2].

Suppose at first that W is a cyclic g-module and that the minimal polynomial of g is $f(t)^i$, where $f(t)$ is irreducible and ϕ-symmetric. Thus $W \simeq k[t]/(f(t)^i)$.

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, …, 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 $A^* = r^{[\phi]}(g)$ 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 2. It is the identity if and only if $f(t)$ divides $t^2 - \phi$.

Let $V = V_1 \perp \cdots \perp V_m$ where $V_i = W$ for $1 \le i \le m$ and extend the action of g to V in the obvious way. If $\mathcal{C}_m$ is 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 V_i to V_j. Thus $\mathcal{C}_m$ is the matrix algebra $\mathrm{Mat}(m, \mathcal{C})$.

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

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

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 $\widehat{V} = V/Vf(g)$ is $\mathrm{Mat}(n, E)$ and if $B = \widehat{A}$ represents the action of $A \in \mathcal{C}_m$ on $\widehat{V}$, then the action of A^* on $\widehat{V}$ is represented by $\overline{B}^{\mathrm{tr}}$.

Theorem 3.12 (Britnell [1, Theorem 5.6], Wall [8, 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_1 such that $\widehat{A}_0 = \alpha$. Then A_1 is non-singular and $N_1 = T - A_1SA_1^* \in \operatorname{rad}\mathcal{C}_m$. Now suppose that we have $A_i \in \mathcal{C}_m$ such that $\widehat{A}_i = \alpha$ and $N_i = T - A_iSA_i^* \in (\operatorname{rad}\mathcal{C}_m)^i$. Put $A_{i+1} = A_i + \frac{1}{2}S^{-1}A_i^{*-1}N_i$. Then $\widehat{A}_{i+1} = \alpha$. Furthermore, $N_i^* = \varepsilon N_i$ and therefore

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

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 $ASA^* = T$. $\square$

Theorem 3.13. *Suppose that W is a cyclic g-module such that the minimal polynomial of g is $f(t)^i$, where $f(t)$ is irreducible, ϕ-symmetric and does not divide $t^2 - \phi$. If β and γ are non-degenerate alternating forms on W preserved by g with the same multiplier ϕ, then there exists $A \in \mathcal{C}$ such that $\gamma(u, v) = \beta(uA, vA)$ for all $u, v \in W$.*

Proof. If J is the matrix of β, then the matrix of γ has the form BJ and since g preserves both β and γ (with the same multiplier ϕ) we have $B \in \mathcal{C}$. Furthermore $B = B^*$, where B^* is the adjoint with respect to β. Thus the image b of B in $E = k[t]/f(t)$ is fixed by the field automorphism. For a finite field the norm homomorphism is onto and therefore $b = \alpha\alpha^*$ for some $\alpha \in E$. It follows from the previous theorem that $B = AA^*$ for some $A \in \mathcal{C}$. Thus $\gamma(u, v) = \beta(uA, vA)$ for all $u, v \in W$. $\square$

Corollary 3.14. *Suppose that g and g' are elements of $\mathrm{CSp}(2n, q)$ such that $V = k^{2n}$ is a primary component of type 1 for g and g' with the same multiplier ϕ, the same minimal polynomial and the same partition. Then g and g' are conjugate via an element of $\mathrm{Sp}(2n, q)$ and therefore $\mathrm{CSp}(V) = \mathrm{Sp}(V)C_{\mathrm{CSp}(V)}(g)$.*

This is another version of Theorem 3.3 of Milnor [4]; namely that the sequence of skew-hermitian spaces H^1, H^2, ... of Theorem 3.11 determines the conjugacy class of $g \mid V_{(f)}$. Milnor determines a standard form for the restriction of g to H^m by first choosing an orthonormal basis (v_1), (v_2), ..., (v_r) for H^m and observing that the vectors $v_\ell g^i s(g)^j$ for $0 \leq i < 2d$ and $0 \leq j < m$ 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 $j + j' \neq m$. 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^m is the orthogonal sum of these cyclic submodules.

Type 1 companion matrices

Another normal form for the restriction of g to a cyclic submodule is the following ϕ-symplectic companion matrix.

Suppose that $h(t) = f(t)^i$ where $f(t)$ is an irreducible ϕ-symmetric polynomial. In addition, if $f(t)$ divides $t^2 - \phi$ suppose that i is even. Therefore, if the degree of $h(t)$ is $2d$, then $h(0) = \phi^d$ and $h(t)$ has the form

$$\begin{aligned} h(t) = \phi^d &+ a_1 t + a_2 t^2 + \cdots + a_{d-1} t^{d-1} \\ &+ t^d (a_d + \phi^{-1} a_{d-1} t + \phi^{-2} a_{d-2} t^2 + \cdots + \phi^{1-d} a_1 t^{d-1} + t^d) \end{aligned}$$

and its ϕ-symplectic companion matrix is

$$C_{\phi,h} = \left(\begin{array}{cccc|cccc} 0 & 1 & & & & & & \\ & 0 & \ddots & & & & & \\ & & \ddots & 1 & & & & \\ & & & 0 & & & & -\phi^{-d} \\ \hline \phi^{d+1} & \phi a_1 & \cdots & \phi a_{d-1} & 0 & \cdots & 0 & -\phi^{1-d} a_d \\ & & & & \phi & \ddots & & \vdots \\ & & & & & \ddots & 0 & -\phi^{1-d} a_2 \\ & & & & & & \phi & -\phi^{1-d} a_1 \end{array}\right).$$

That is, $C_{\phi,h} \in \mathrm{CSp}(2d, q)$, $h(t) = \det(tI - C_{\phi,h})$ and $C_{\phi,h} J C_{\phi,h}^{\mathrm{tr}} = \phi J$.

Note that when $d = 1$ we have $C_{\phi,h} = \begin{pmatrix} 0 & -\phi^{-1} \\ \phi^2 & -a_1 \end{pmatrix}$.

```
type1Companion := function(φ, f, i)
   error if f ne PhiDual(f, φ), "polynomial must be phi-symmetric";
   error if not IsIrreducible(f), "polynomial must be irreducible";
   t := Parent(f).1;
   error if IsDivisibleBy(t^2 − φ, f) and IsOdd(i), "power must be even";
   h := f^i;
   e := Degree(h);
   d := e div 2;
   a := Coefficients(h)[2 . . d+1];
   C := ZeroMatrix( BaseRing(h), e, e );
   ψ := φ^(1−d);
   for i in [1 . . d−1] do
      C[i, i+1] := 1;
      C[d+1, i+1] := φ∗a[i];
```

```
    C[d+i+1, d+i] := φ;
    C[e−i+1, e] := −ψ∗a[i];
  end for;
  C[d, e] := −φ^(−d);
  C[d+1, 1] := φ^(d+1);
  C[d+1, e] := −ψ∗a[d];
  return C;
end function;
```

3.4 Primary components of type 2

Suppose that V is a homocyclic component of type 2. That is, V is the sum of m copies of a cyclic g-module W, where g has multiplier ϕ. Then the minimal polynomial of g is $f(t)^i$ and either $\phi = \lambda^2$ and $f(t)$ is $t - \lambda$ or $t + \lambda$ or else ϕ is not a square and $f(t) = t^2 - \phi$.

Lemma 3.15. *If $\Delta = g - \phi g^{-1}$, then $\beta(u\Delta, v) = -\beta(u, v\Delta)$.*

Let $E = k[t]/(f(t))$. If ϕ is not a square, E is a quadratic extension of k, otherwise $E = k$.

Theorem 3.16. *In the vector space $\widehat{V} = V/Vf(g)$ over the field E let (v) denote the image of $v \in V$ in $\widehat{V}$. Then $\widehat{V}$ has a non-degenerate well-defined inner product $(u) \circ (v)$ such that*

$$\beta(u\Delta^{i-1}, v) = \operatorname{trace}_{E/k}((u) \circ (v)). \tag{3.2}$$

If i is odd, the inner product is alternating and therefore m is even. If i is even, the inner product is symmetric.

Type 2, symplectic type

If i is odd, a matrix representing the action of g on V 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 code to produce a ϕ-symplectic companion matrix for $\langle \phi, \{@ \langle f, [\langle i, 2\rangle] @\}\rangle$ where i is odd, m is even and $f(t)$ is irreducible of type 2. The difference between this code and *type3Companion* is the use of *stdJordanBlock* when the degree of $f(t)$ is 1.

```
type3CompanionS := function(φ, f, i)
  a0 := Coefficient(f, 0);
  C := (Degree(f) eq 1) select stdJordanBlock(i, −a0) else CompanionMatrix(f^i);
  d := Nrows(C);
  Λ := ZeroMatrix(BaseRing(f), d, d);
  for i := 1 to d do Λ[i, d−i+1] := 1; end for;
```

```
    return DiagonalJoin(C, φ*Λ*Transpose(C^-1)*Λ);
  end function;
```

If g is the matrix returned by this function and if W is the space on which it acts, then as in the case of primary components of type 3, we have $\mathrm{CSp}(V) = \mathrm{Sp}(V)C_{\mathrm{CSp}(V)}(g)$.

Lemma 3.17. *Suppose that g and g' are elements of $\mathrm{CSp}_\phi(W)$ such that as both a g-module and a g'-module W is a direct sum of an even number of $k[t]/(f(t)^i)$-modules where $f(t)$ divides $t^2 - \phi$ and i is odd. Then g and g' are conjugate via an element of $\mathrm{Sp}(W)$.*

Type 2, orthogonal type

Assume that the characteristic of k is odd. If the minimal polynomials of g is $f(t)^i$ where $f(t)$ divides $t^2 - \phi$ and i is even, then $\widehat{V} = V/Vf(g)$ is a quadratic space over the field $E = k[t]/(f(t))$. We may take the quadratic form to be $Q((v)) = \frac{1}{2}(v) \circ (v)$ and write $\widehat{V}$ as an orthogonal sum of 1-dimensional subspaces.

For completeness we record some well-known facts about finite fields.

Lemma 3.18. *Suppose that q is an odd prime power.*

(i) *If a and b are non-zero elements of $\mathrm{GF}(q)$, then for all $c \in \mathrm{GF}(q)$ there exist $x, y \in \mathrm{GF}(q)$ such that $c = ax^2 + by^2$.*

(ii) -1 *is a square in* $\mathrm{GF}(q)$ *if and only if* $q \equiv 1 \pmod 4$.

(iii) 2 *is a square in* $\mathrm{GF}(q)$ *if and only if* $q \equiv \pm 1 \pmod 8$.

(iv) *If ϕ is not a square in $\mathrm{GF}(q)$ and if $\tau \in \mathrm{GF}(q^2)$ satisfies $\tau^2 = \phi$, then τ is a square in $\mathrm{GF}(q^2)$ if and only if $q \equiv 3 \pmod 4$.*

The following corollary is a consequence of part (i) of this lemma.

Corollary 3.19. *In the notation of Theorem 3.16, $\widehat{V}$ has an orthogonal basis (v_1), (v_2), $\ldots$, (v_m) such that $(v_j) \circ (v_j) = 1$ for $1 < j \leq m$ and $(v_1) \circ (v_1) = a$, where a is either 1 or a non-square in E.*

Thus if i is even there are at most two conjugacy classes of elements in $\mathrm{CSp}(\widehat{V})$ with the same minimal polynomial $f(t)^i$ and multiplicity m. In order to distinguish between these classes we attach a sign to the pair $\langle i, m \rangle$ as follows.

Definition 3.20.

(i) If m is even and $\widehat{V}$ has maximal Witt index the *sign* of $\langle i, m \rangle$ is $+1$ whereas if the Witt index is not maximal the *sign* is -1.

(ii) If m is odd, there are two isomorphism classes of quadratic spaces $\widehat{V}$, which have the same group of isometries but are distinguished by the discriminant of the symmetric form $(u) \circ (v)$. If the discriminant is a square, the *sign* is $+1$ and -1 otherwise.

The discriminant of a hyperbolic plane is $-1 \pmod{k^2}$ and the discriminant of a 2-dimensional quadratic space with no isotropic vectors is $-a \pmod{k^2}$, where a is a non-square in k.

Consequently, if m is even and $\widehat{V}$ has maximal Witt index, the discriminant is $(-1)^{m/2} \pmod{k^2}$ whereas if the Witt index is not maximal, the discriminant is $(-1)^{m/2}a \pmod{k^2}$.

The function *type1Companion* returns a ϕ-symplectic companion matrix for $f(t)^i$ that preserves β with multiplier ϕ. However when $f(t) = t - \lambda$ it is important to know the sign of the conjugacy invariant and the following code is easier to analyse. The return value is a $2c \times 2c$ matrix $g = \begin{pmatrix} \lambda B & aS \\ 0 & \lambda B^{-1} \end{pmatrix}$ with the single primary invariant $(t-\lambda)^{2c}$. The matrix B is the standard Jordan block all of whose non-zero entries are 1. All entries in S are 0 except for the last row which alternates between 1 and -1.

The parameter *flag* is a boolean. It is related to, but not necessarily equal to, the sign of the invariant.

```
type3CompanionO := function(λ, c, flag)
  F := Parent(λ);
  B := stdJordanBlock(c, F ! 1);
  g := λ*DiagonalJoin(B, B^-1);
  a := IsEven(c) select -F ! 2 else F ! 2;
  if (not flag) then a *:= Nonsquare(F); end if;
  for i := 1 to c do g[c, c+i] := IsOdd(i) select a else -a; end for;
  return g;
end function;
```

In this case $\Delta = g - \phi g^{-1} = \begin{pmatrix} \lambda R & aU \\ 0 & -\lambda R \end{pmatrix}$ and $R = B - B^{-1}$. The matrix R^{c-1} is zero everywhere except for the last entry in the top row, which is 2^{c-1}.

Since $\Delta^{2c-1} = \begin{pmatrix} 0 & (-1)^{c-1}\lambda^{2c-2}aR^{c-1}UR^{c-1} \\ 0 & 0 \end{pmatrix}$ every entry in Δ^{2c-1} is 0 except for the last entry in the top row, which is $(-1)^{c-1}\phi^{c-1}2^{2c-1}a$. We have $a = (-1)^{c-1}2b$ where b is 1 if the sign is positive and a non-square otherwise and therefore the only non-zero entry in Δ^{2c-1} is $2^{2c}\phi^{c-1}b$, which is a square if and only if b is a square.

Let g^+ (resp. g^-) be the matrix returned by *type3CompanionO* when *flag* is true (resp. false). Then $A^{-1}g^+A = g^-$, where $A = \begin{pmatrix} I & 0 \\ 0 & bI \end{pmatrix}$. If J is the standard alternating form, $AJA^{\mathrm{tr}} = bJ$ and therefore $A \in \mathrm{CSp}(2n, q)$.

Let $g^+_{[m]}$ denote the direct sum of m copies of g^+ and let $g^-_{[m]}$ denote the direct sum of $m-1$ copies of g^+ and a single copy of g^-. Then the discriminant of $g^+_{[m]}$ is $(-1)^m \pmod{k^2}$ and the discriminant of $g^-_{[m]}$ is $(-1)^m b \pmod{k^2}$, where b is a non-square.

If $m \equiv 0 \pmod 4$ or $q \equiv 1 \pmod 4$, $g^+_{[m]}$ is an element of $+$ type and $g^-_{[m]}$ is an element of $-$ type, whereas if $m \equiv 2 \pmod 4$ and $q \equiv 3 \pmod 4$, $g^+_{[m]}$ is an element $-$ type and $g^-_{[m]}$ is an element of $+$ type.

If $f(t) = t^2 - \phi$ and ϕ is not a square we essentially repeat the code for *type3CompanionO* in the quadratic extension $E = k[t]/(t^2 - \phi)$ of k. However, in this case there is no element of $\mathrm{CSp}(2n, q)$ that conjugates g^+ to g^-.

```
type3CompanionOext := function(φ, c, flag)
  F := Parent(φ);
  C := Matrix(F,2,2,[0,1,φ,0]);    // companion matrix for t^2 − φ
  B := stdJordanBlock(c,F ! 1);
  X11 := KroneckerProduct(B,C);
  X22 := KroneckerProduct(B^-1,C);
  if flag then
    M := IdentityMatrix(F,2);
  else
    t := PolynomialRing(F).1;
    E<τ> := ext< F | t^2 − φ >;
    α := Nonsquare(E);
    M := Matrix(F,2,2,[Eltseq(α,F),Eltseq(α*τ,F)]);
  end if;
  S := ZeroMatrix(F,c,c);
  for i := 1 to c do S[c,i] := IsOdd(i) select 1 else −1; end for;
  X12 := KroneckerProduct(S,M);
  return BlockMatrix(2,2,[[X11,X12],[ZeroMatrix(F,2*c,2*c),X22]]);
end function;
```

The return value of this function is a $4c \times 4c$ matrix $g = \begin{pmatrix} X_{11} & X_{12} \\ 0 & X_{22} \end{pmatrix}$, where $X_{22} = \phi X_{11}^{-1}$ because $C = \phi C^{-1}$. The matrix g preserves the form with multiplier ϕ if and only if $X_{11}\Lambda X_{22}^{\mathrm{tr}} = \phi\Lambda$ and $X_{11}\Lambda X_{12}^{\mathrm{tr}}$ is symmetric. A direct calculation shows that $X_{11}\Lambda X_{22}^{\mathrm{tr}} = \phi\Lambda$ and that the only non-zero entry in $X_{11}\Lambda X_{12}^{\mathrm{tr}}$ is the 2×2 block $\pm C\Lambda_2 M^{\mathrm{tr}}$ at the left end of the last row. Thus in order to preserve the form, $C\Lambda_2 M^{\mathrm{tr}}$ must be symmetric.

If τ is the image of t in E, then C is the matrix representing multiplication by τ with respect to the k-space basis 1, τ of E. If $\alpha = r + s\tau$ where $a, b \in k$ and if M represents multiplication by α, then $C\Lambda_2 M^{\mathrm{tr}} = \begin{pmatrix} r & s\phi \\ s\phi & r\phi \end{pmatrix}$, which is symmetric, as required.

Thus we may write $g = \begin{pmatrix} \tau B & \alpha S \\ 0 & \tau B^{-1} \end{pmatrix}$ and then $\Delta = g - \phi g^{-1} = \tau \begin{pmatrix} R & \alpha\tau^{-1}U \\ 0 & -R \end{pmatrix}$, where $R = B - B^{-1}$ and $U = S + B^{-1}SB$. A calculation similar to one above shows that $R^c = 0$ and every entry in Δ^{2c-1} is 0 except for the last entry in the top row, which is $(-1)^{c-1}\tau^{2c-2}2^{2c-1}\alpha$. Since -1 and 2 are both squares in $E = \mathrm{GF}(q^2)$ this top row value is a square if and only if α is a square.

We have $f(g) = \tau^2 \begin{pmatrix} B^2 - I & \tau^{-1}\alpha(BS + SB^{-1}) \\ 0 & B^{-2} - I \end{pmatrix}$ and consequently, in the notation of Theorem 3.16, the space $\widehat{V} = V/Vf(g)$ has a basis (v_1), (v_2), where $v_1, v_2, \dots$ is the standard basis for $V = k^{2c}$ and (v) denotes the image of v in $\widehat{V}$. We have $\dim_E \widehat{V} = 1$ and from (3.2)

$$\mathrm{trace}_{E/k}((v_1) \circ (v_1)) = \beta(v_1\Delta^{2c-1}, v_1).$$

Writing $(v_1) \circ (v_1) = a_1 + a_2\tau$ with $a_1, a_2 \in k$ and using the fact that $\mathrm{trace}_{E/k}(\tau) = 0$ we have

$$2a_1 = \beta(v_1\Delta^{2c-1}, v_1) \quad \text{and} \quad 2a_2\phi = \beta(v_1\Delta^{2c-1}, v_1 g)$$

and consequently

$$(v_1) \circ (v_1) = (-1)^c 2^{2c-2}\phi^{c-2}\alpha\tau.$$

This is a square in E if and only if $\alpha\tau$ is a square. Furthermore, τ is a square if and only if $q \equiv 3 \pmod 4$.

Let g^+ (resp. g^-) be the matrix returned by *type3CompanionOext* when *flag* is true (resp. false), let $g^+_{[m]}$ denote the direct sum of m copies of g^+ and let $g^-_{[m]}$ denote the direct sum of $m-1$ copies of g^+ and a single copy of g^-.

For $g^+_{[m]}$ the discriminant of the induced inner product on $\widehat{V}$ is $\tau^m \pmod{k^2}$ and for $g^-_{[m]}$ it is $\alpha\tau^m \pmod{k^2}$. Therefore, if m is even, $g^+_{[m]}$ is an element of $+$ type and $g^-_{[m]}$ is an element of $-$ type. On the other hand, if m is odd, $g^+_{[m]}$ is an element of $+$ type if and only if $q \equiv 3 \pmod 4$.

Lemma 3.21 (Britnell [1, Lemma 5.8])**.** *If A is a non-singular symmetric matrix over a finite field of odd characteristic, then $A = BB^{\mathrm{tr}}$ for some matrix B if and only* $\det A$ *is a square.*

Proof. The existence of an orthogonal basis for the symmetric form with matrix A is equivalent to the existence of a matrix P such that PAP^{tr} is diagonal. We may suppose that the diagonal entries are $d_1, d_2, \dots, d_n$, where $d_1, d_2, \dots, d_m$ are non-squares and the remaining entries are squares. If $\det A$ is a square, then m is even.

If $m > 0$, choose r, s and t in the field such that $r^2 + s^2 = d_1$ and $t^2 = d_2/d_1$. Then

$$\begin{pmatrix} r & -s \\ st & rt \end{pmatrix} \begin{pmatrix} r & -s \\ st & rt \end{pmatrix}^{\mathrm{tr}} = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}.$$

Thus it is clear that there exists B such that $A = BB^{\mathrm{tr}}$. The converse is obvious. $\square$

Let $\mathcal{C}$ be the centralizer of g in $\mathrm{End}_k(W)$ and let $\mathcal{C}_m$ be the centralizer of g in $\mathrm{End}_k(V)$. The adjoint map on $\mathcal{C}$ induces the identity automorphism of E and hence if $\widehat{A}$ is the matrix of $A \in \mathcal{C}_m$ acting on $\widehat{V}$, the matrix of its adjoint is $\widehat{A}^{\mathrm{tr}}$.

For $A \in \mathrm{GL}(V)$, the form $\beta(uA, v)$ is alternating if and only if $A = A^*$ and in addition it is preserved by g if and only if $A \in \mathcal{C}_m$. Therefore, if g preserves and alternating form $\beta(uA, v)$, then $\widehat{A}$ is symmetric. It follows from the lemma just proved that $\widehat{A} = \alpha\alpha^{\mathrm{tr}}$ for some matrix α if and only if $\det \widehat{A}$ is a square in E. From Theorem 3.12 this is the case if and only if there exists $K \in \mathcal{C}_m$ such that $A = KK^*$ if and only if $\beta(uA, v) = \beta(uK, vK)$.

The map $\mathcal{C} \to E$ is onto and thus there is a matrix $Z \in \mathcal{C}$ such that its image in E is a non-square. We may assume that the matrix of β restricted to W is the standard alternating form J.

4 Class representatives in conformal 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 $A \in \mathrm{CSp}(2m, q)$, $B \in \mathrm{CSp}(2n, q)$ and $\phi(A) = \phi(B)$ we may write A as the block matrix

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

and then the 'central sum'

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

belongs to $\mathrm{CSp}(2m+2n, q)$ because

$$X^{-1} \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} X = A \circ B$$

where

$$X = \begin{pmatrix} I_m & 0 & 0 \\ 0 & 0 & I_m \\ 0 & I_{2n} & 0 \end{pmatrix} \text{ so that } X^{-1} = X^{\mathrm{tr}} \text{ and } X^{\mathrm{tr}} \begin{pmatrix} J_m & 0 \\ 0 & J_n \end{pmatrix} X = J_{m+n}.$$

```
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;
```

Conjugacy class invariants

If g and g' are elements of $\mathrm{CSp}_\phi(V)$, which are conjugate in $\mathrm{GL}(V)$, it follows from Theorem 3.5, Corollary 3.14, Lemma 3.17 and Corollary 3.19 that there is an element of $\mathrm{Sp}(V)$ which conjugates g to g' if and only if for each primary component of type 2 for g and g' with the same polynomial f, of degree 1, the signed partitions of f for g and g' are the same.

The conjugacy class of g in $\mathrm{CSp}(V)$ does not split in $\mathrm{Sp}(V)$ if and only if g is centralized by some $a \in \mathrm{CSp}_\phi(V)$, where ϕ is a non-square. It follows from the previous results that the centralizer of g does not cover $\mathrm{CSp}(V)/\mathrm{Sp}(V)$ if and only if g has a component of type 2 with an associated quadratic space $\widehat{V}$, as in Theorem 3.16, corresponding to a term $\langle e, m\rangle$ where e is even, m is odd and the degree of the polynomial is 1.

Such a pair $\langle e, m\rangle$ will be said to be of *otype*. Furthermore, if $\langle \phi, \xi\rangle$ is an invariant in which ξ contains a pair $\langle f, \mu\rangle$ where the degree of f is 1 and the partition μ has a term of *otype*, then $\langle \phi, \xi\rangle$ is also said to be of *otype*. If the first occurrence of an *otype* term $\langle e, m\rangle$ in ξ has $e > 0$, it is of *positive otype*

An element of $\mathrm{CSp}(V)$ whose invariant contains a pair $\langle \phi, \xi \rangle$ of *otype* is conjugate to the element corresponding to the invariant obtained by reversing the signs of the *otype* pairs $\langle e, m \rangle$ in ξ. Therefore we retain only those pairs of *positive otype*.

```
intrinsic InternalClassInvariantsCSp(d :: RngIntElt, q :: RngIntElt) → SeqEnum
{The conjugacy class invariants for the conformal symplectic
  group CSp(d,q), q odd}
  require IsOdd(q) : "q must be odd";
  F := GF(q);
  t := PolynomialRing(F).1;
  polseq := [];
  mgrp := [ x[1] : x in PhiIrreduciblePolynomials(F, 1) ];
  X := [PhiIrreduciblePolynomials(F, i) : i in [1] cat [2. . d by 2] ];
  for i := 1 to q−1 do polseq[i] := &cat[x[i][2] : x in X]; end for;
  parts := allPartitions(d);
  sparts := signedPartitionsSp(d);
  inv := [];
```

A function to check whether μ is of *otype* and if so whether the first occurrence of $\langle e, m \rangle$ in μ with e even and m odd has $e > 0$.

```
  isOtype := function(μ)
    for λ in μ do
      e, m := Explode(λ);
      if IsEven(e) and IsOdd(m) then return true, (e gt 0); end if;
    end for;
    return false, _;
  end function;

  for i := 1 to q − 1 do
    φ := mgrp[i];
    fseq := polseq[i];
```

The nth term of the sequence Ξ contains the indexed sets $\{@ \ \cdots, \langle f_i, \mu_i \rangle, \cdots \ @\}$ such that $\sum_i \deg(f_i)|\mu_i| = n$ and *tags*$[n]$ is a parallel sequence of boolean values indicating which pairs $\langle f_i, \mu_i \rangle$ are of positive *otype*.

```
    Ξ := [ [] : n in [1. . d] ];
    prevXi := Ξ;
    prevTags := Ξ;
    tags := Ξ;
    for f in fseq do
      fparts := IsDivisibleBy(t^2 − φ, f) select sparts else parts;
      deg := Degree(f);
      for n := 0 to d−1 do
        dimleft := d−n;
        if deg le dimleft then
          for i := 1 to dimleft div deg do
            pol_parts := ((n ne 0) select prevXi[n] else [ {@ @}]);
            taglist := ((n ne 0) select prevTags[n] else [ false ]);
```

```
          for j := 1 to #pol_parts do
            pol_part := pol_parts[j];
            tagged := taglist[j];
            for μ in fparts[i] do

              accept := true;
              newtag := false;
              if deg eq 1 then
                if tagged then
                  newtag := true;
                else
                  otype, tag := isOtype(μ);
                  if otype then
                    if tag then newtag := true; else accept := false; end if;
                  end if;
                end if;
              end if;

              if accept then
                Append(~Ξ[n+deg*i], Include(pol_part, <f, μ>));
                Append(~tags[n+deg*i], newtag);
              end if;

            end for;
          end for;
        end for;
      end if;
    end for;
    prevXi := Ξ;
    prevTags := tags;
  end for;
  inv cat:= [ <φ,ξ> : ξ in Ξ[d] ];
end for;
return inv;
end intrinsic;
```

Conjugacy class representatives

Return a matrix in the conformal symplectic group with a given conjugacy class invariant *inv*, where *inv* is a pair $<\phi,\ \Xi>$, where ϕ is a non-zero field element and Ξ is an indexed set of pairs $<f,\ \pi>$, and where f is a polynomial and π is a partition.

```
intrinsic InternalRepMatrixCSp(inv :: Tup) → GrpMatElt
{A representative of the conjugacy class with invariant inv
 in the conformal symplectic group}
  φ, Ξ := Explode(inv);
  F := Parent(φ);
  q := #F;
```

```
t := PolynomialRing(F).1 ;
X := ZeroMatrix(F, 0, 0) ;
for polpart in Ξ do
  f, plist := Explode(polpart) ;
```

First deal with the type 2 invariants.

```
    if IsDivisibleBy(t^2 − φ, f) then
      for term in plist do
        e, m := Explode(term) ;
```

If e is odd, the term is of symplectic type.

```
          if IsOdd(e) then
            assert IsEven(m) ;
            for i := 1 to m div 2 do
              X := centralJoin(X, type3CompanionS(φ, f, e)) ;
            end for ;
```

If e is even, the term is of orthogonal type.

```
          else
           flag := Sign(e) gt 0 ;
           c := Abs(e) div 2 ;
           if Degree(f) eq 1 then
             λ := − Coefficient(f, 0) ;
             X := ((q mod 4 eq 1) or (m mod 4 eq 0))
               select centralJoin(X, type3CompanionO(λ, c, flag))
                 else centralJoin(X, type3CompanionO(λ, c, not flag)) ;
             for i := 2 to m do
               X := centralJoin(X, type3CompanionO(λ, c, true)) ;
             end for ;
           else
             X := (IsOdd(m) and (q mod 4 eq 1))
               select centralJoin(X, type3CompanionOext(φ, c, not flag))
                 else centralJoin(X, type3CompanionOext(φ, c, flag)) ;
             for i := 2 to m do
               X := centralJoin(X, type3CompanionOext(φ, c, true)) ;
             end for ;
           end if ;
         end if ;
      end for ;
```

Next we have the type 1 invariants.

```
  elif IsIrreducible(f) then
    for μ in plist do
      e, m := Explode(μ) ;
      for i := 1 to m do X := centralJoin(X, type1Companion(φ, f, e)) ; end for ;
    end for ;
```

And finally, the type 3 invariants.

```
    else
      h := Factorisation(f)[1][1];
      assert f eq h*Factorisation(f)[2][1];
      for μ in plist do
        e, m := Explode(μ);
        for i := 1 to m do X := centralJoin(X, type3Companion(ϕ, h^e)); end for;
      end for;
    end if;
  end for;
  return ConformalSymplecticGroup(Nrows(X), F) ! X;
end intrinsic;
```

Centralizer orders

The centralizer orders of elements of the conformal symplectic group can be computed using a modification of Wall's functions $A(\varphi^{\mu})$ and $B(\varphi)$ from [8].

```
A_fn := function(ϕ, f, d, m)
  q := #BaseRing(f);
  deg := Degree(f);
  t := Parent(f).1;
  if IsIrreducible(f) then
    if IsDivisibleBy(t^2 − ϕ, f) then
      if IsOdd(d) then val := OrderSp(m, q^deg);
      else
        if IsOdd(m) then val := OrderGO(m, q^deg);
        elif (d lt 0) then val := OrderGOMinus(m, q^deg);
        else val := OrderGOPlus(m, q^deg); end if;
      end if;
    else val := OrderGU(m, q^(deg div 2)); end if;
  else val := OrderGL(m, q^(deg div 2)); end if;
  return val;
end function;

κ := function(ϕ, plist, f)
  t := Parent(f).1;
  val := 0;
  for μ in plist do
    d, m := Explode(μ);
    val +:= (Abs(d)−1)*m^2;
    if IsDivisibleBy(t^2−ϕ, f) and IsEven(d) then val +:= m; end if;
  end for;
  r := #plist;
  for i := 1 to r−1 do
    d := Abs(plist[i][1]);
    m := plist[i][2];
    for j := i+1 to r do val +:= 2*d*m*plist[j][2]; end for;
  end for;
```

```
    val *:= Degree(f);
    assert IsEven(val);
    return val div 2;
  end function;

  otype := function(inv)
    φ, ξ := Explode(inv);
    F := Parent(φ);
    t := PolynomialRing(F).1;
    q := #F;
    tp := false;
    for pol_part in ξ do
      f, μ := Explode(pol_part);
      if IsDivisibleBy(t^2 − φ, f) and Degree(f) eq 1 then
        for λ in μ do
          e, m := Explode(λ);
          tp or:= IsEven(e) and IsOdd(m);
        end for;
      end if;
    end for;
    return tp select (q − 1) div 2 else q − 1;
  end function;
```

Here *pol_part* has the form $\langle f,\ [\cdots, \langle \mu, m_\mu \rangle, \cdots]\rangle$.

```
  B_fn := function(φ, pol_part)
    f, partn := Explode(pol_part);
    q := #BaseRing(f);
    return q^κ(φ, partn, f) * &*[A_fn(φ, f, μ[1], μ[2]) : μ in partn];
  end function;
```

The order of the centralizer of any element in the symplectic group whose conjugacy invariant is *inv*.

```
  centraliserOrderCSp := function(inv)
    φ, ξ := Explode(inv);
    return otype(inv) * &*[ B_fn(φ, pol_part) : pol_part in ξ ];
  end function;
```

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

Return the sequence of labels as well as the conjugacy classes.

```
  classesCSp := function(d, q)
    ord := OrderCSp(d, q);
    L := InternalClassInvariantsCSp(d, q);
    cc := [car<Integers(), Integers(), CSp(d, q)>|
      < Order(M), ord div centraliserOrderCSp(μ), M > : μ in L | true
          where M is InternalRepMatrixCSp(μ) ];
    ParallelSort(~cc, ~L);
```

```
    return cc, L;
end function;
```

5 The class invariant of a conformal symplectic matrix

Guided by Theorem 3.7 we shall define a function *homocyclicSplit* designed to be applied to a matrix g acting on a primary component $V_{(f)}$, where $f(t)$ is irreducible and ϕ-symmetric. But first we need a function that returns the row indices for the homocyclic components of the rational canonical form of the matrix g restricted to $V_{(f)}$.

```
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 shall 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. The return value is the sequence of mutually orthogonal homocyclic components of W.

```
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 D_i obtained from *homocyclicSplit*, g is the matrix acting on the generic space of D, f is the polynomial $t+1$ or $t-1$ and λ is the pair $\langle d_i, m_i \rangle$.

The matrix B represents the symmetric form $(u) \cdot (v)$ on $\overline{D}_i$. There are two versions of the function that attaches a sign to a partition list term $\mu = \langle e, m \rangle$. The first one is used for polynomials of degree 1, the second is used for polynomials of degree 2.

```
  attachSign_1 := function(D, g, f, e, m)
    F := BaseRing(g);
    λ := Evaluate(f, 0);
    A := g + ScalarMatrix(F, Nrows(g), λ);
    D_0 := sub< D | [v*A : v in Basis(D)] >;
    E := [v : v in ExtendBasis(D_0, D) | v notin D_0];
    δ := (g − λ^2*g^(−1))^(e−1);
    B := Matrix(F, #E, #E, [DotProduct(D ! (u*δ), v) : u, v in E ]);
    assert Determinant(B) ne 0;
    sq, _ := IsSquare(Determinant(B));
```

If $m \equiv 0 \pmod 4$ or $q \equiv 1 \pmod 4$, the quadratic space defined by B has maximal Witt index if and only if the determinant of B is a square. Conversely if $m \equiv 2 \pmod 4$ and $q \equiv 3 \pmod 4$, the Witt index is maximal if and only if the determinant of B is not a square.

```
    if (#F mod 4 eq 3) and (m mod 4 eq 2) then sq := not sq; end if;
    return sq select e else −e;
  end function;

  attachSign_2 := function(D, g, f, e, m)
    F := BaseRing(g);
    φ := −Evaluate(f, 0);
    A := g*g − ScalarMatrix(F, Nrows(g), φ);
    D_0 := sub< D | [v*A : v in Basis(D)] >;
    L := [v : v in ExtendBasis(D_0, D) | v notin D_0];
    L_2 := [L[i] : i in [1..#L by 2]];
    δ := (g − φ*g^(−1))^(e−1);
    E<τ> := ext< F | f >;
```

At this point E is the field $k[t]/(f(t))$ where $f = t^2 - \phi$ and if $\tau = t + (f(t))$, then $\tau^q + \tau = 0$. Therefore, if $y = a + b\tau$, $\mathrm{trace}_{E/k}(y) = 2a$ and $\mathrm{trace}_{E/k}(y\tau) = 2b\phi$ for all $a, b \in k$. The induced inner product $(u) \circ (v)$ on D/D_0 satisfies

$$\operatorname{trace}_{E/k}((u) \circ (v)) = \beta(u\Delta^{e-1}, v)$$

where $\Delta = g - \phi g^{-1}$. Therefore we have $(u) \circ (v) = a + b\tau$ where $a = \frac{1}{2}\beta(u\Delta^{e-1}, v)$ and $b = \frac{1}{2}\phi^{-1}\beta(u\Delta^{e-1}, vg)$ because $\beta(ug, v) = \beta(u, vg)$ for all $u, v \in D$. Since 2 is always a square in GF(q^2) we may ignore the factors of $\frac{1}{2}$.

```
dotprod := function(u, v)
  w := D ! (u*δ);
  a := DotProduct(w, v);
  b := φ^-1 *DotProduct(w, D ! (v*g));
  return E ! [a, b];
end function;

  B := Matrix(E, #L2, #L2, [dotprod(u, v) : u, v in L2 ]);
  assert Determinant(B) ne 0;
  sq, _ := IsSquare(Determinant(B));
```

Since it is always the case that $q^2 \equiv 1 \pmod 4$, the quadratic space defined by B, when m is even, has maximal Witt index if and only if the determinant of B is a square.

```
  return sq select e else -e;
end function;
```

If the class of g does not split in $\mathrm{Sp}(V)$, then g has a component of type 2 with an associated quadratic space $\widehat{V}$ corresponding to a term $\langle e, m \rangle$ where e is even, m is odd and the degree of the polynomial is 1. Our convention is to use only those class invariants for polynomials of degree 1 for which the first signed term of the form $\langle e, m \rangle$ with e even and m odd has $e > 0$.

```
intrinsic InternalConjugacyInvariantCSp(g :: GrpMatElt) → Tup
{The conjugacy class invariant of the conformal symplectic
 matrix g}
  F := BaseRing(g);
  t := PolynomialRing(F).1;
  n := Nrows(g);
  std := StandardAlternatingForm(n, F);
  stdg := g*std*Transpose(g);
  φ := stdg[1, n];
  require stdg eq φ*std :
    "matrix is not in the standard conformal symplectic group";
  _, T, pFact := PrimaryRationalForm(g);
  V := SymplecticSpace(std);
  pols, parts, bases := primaryPhiParts(φ, pFact);
  inv := {@ @};
```

While *scanning* is true we look for the first instance of a term $\langle e, m \rangle$ with e even and m odd for a polynomial of degree 1. If $e < 0$ we switch *invert* to true.

```
  scanning := true;
  invert := false;
```

```
    for i := 1 to #pols do
      plist := convert(parts[i]);
      f := pols[i];
      if IsDivisibleBy(t^2 − φ, f) 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);
```

Run through the homocyclic components looking for quadratic spaces.

```
        for j := 1 to #plist do
          e, m := Explode(plist[j]);
          if IsEven(e) then
            if Degree(f) eq 1 then
              e := attachSign_1(D[j], gg, f, e, m);
```

If we encounter a class that does not split in $\mathrm{Sp}(V)$ we may need to replace the invariant by an equivalent one with signs inverted.

```
              if IsOdd(m) then
                if scanning then scanning := false; invert := e lt 0; end if;
                if invert then e := −e; end if;
              end if;
            else
              e := attachSign_2(D[j], gg, f, e, m);
            end if;
            plist[j] := <e, m>;
          end if;
        end for;
      end if;
      Include(~inv, <f, plist>);
    end for;
    return <φ, inv>;
  end intrinsic;
```

6 Extended symplectic groups

A group G such that $\mathrm{Sp}(n,q) \subseteq G \subseteq \mathrm{CSp}(n,q)$ will be designated an *extended* symplectic group of index m, where $m = |G : \mathrm{Sp}(n,q)|$.

```
  intrinsic ExtendedSp(n :: RngIntElt, q :: RngIntElt, m :: RngIntElt)
      → GrpMat
  {The subgroup of CSp(n,q) that contains Sp(n,q) as a subgroup
   of index m}
    require IsEven(n) : "invalid dimension---should be even";
```

```
    require m gt 0 : "the index should be positive";
    divides, r := IsDivisibleBy(q − 1, m);
    require divides : "the index should divide q - 1";
    if m eq 1 then G := Sp(n, q);
    elif m eq q − 1 then G := CSp(n, q);
    else
      F := GF(q);
      ξ := PrimitiveElement(F)^r;
      A := IdentityMatrix(F, n);
      for i := 1 to n div 2 do A[i, i] := ξ; end for;
      G := sub< CSp(n, q) | Sp(n, q), A >;
      G`Order := OrderSp(n, q) ∗ m;
    end if;
    return G;
  end intrinsic;

  intrinsic IndexOfSp(G :: GrpMat) → RngIntElt
  {The index of the symplectic group in G}
    F := BaseRing(G);
    require ISA(Type(F), FldFin) : "the base field should be finite";
    msg := "G should contain the symplectic
    group and be a subgroup of the conformal symplectic group";
    count := 0;
    repeat    // at most 4 times
      flag := RecognizeClassical(G);
      count +:= 1;
    until flag or count gt 3;
    require flag and ClassicalType(G) eq "symplectic" : msg;
    n := Dimension(G);
    std := StandardAlternatingForm(n, F);
    ndx := [];
    for g in Generators(G) do
      stdg := g∗std∗Transpose(g);
      φ := stdg[1, n];
      require stdg eq φ∗std : msg;
      Append(~ndx, Order(φ));
    end for;
    return LCM(ndx);
  end intrinsic;
```

Given an extended symplectic group G of index m over $\mathrm{GF}(q)$ there are two cases to consider when constructing conjugacy class representatives.

On the one hand, if $(q-1)/m$ is even and $2ms = q-1$, we have $G = \mathrm{Sp}(n,q)D$, where $D = \{\zeta I \mid \zeta^s = 1\}$. In this case representatives of the conjugacy classes of G can be constructed from the conjugacy classes of $\mathrm{Sp}(n,q)$ by multiplying by scalar matrices. In particular, if $g \in \mathrm{Sp}(n,q)$ and $z \in D$, then $C_G(zg) = C_{\mathrm{Sp}(n,q)}(g)D$. Thus, if the index of $\mathrm{ExtSp}(n,q,m)$ in $\mathrm{CSp}(n,q)$ is even there are elements $g, h \in \mathrm{ExtSp}(n,q,m)$ that are not conjugate in $\mathrm{ExtSp}(n,q,m)$ but are conjugate in $\mathrm{CSp}(n,q)$.

On the other hand, if $(q-1)/m$ is odd, elements of G are conjugate in G if and only of they are conjugate in $\mathrm{CSp}(n,q)$.

To deal with the first case we need a function that transforms an invariant for $g \in \mathrm{Sp}(n,q)$ to an invariant for ζg, where $\zeta \in \mathrm{GF}(q)$.

Lemma 6.1. *Given a polynomial $f(t)$ of degree d and a non-zero element $\zeta \in k$, let $\tilde{f}(t) = \zeta^d f(\zeta^{-1}t)$. If $f(t)$ is ϕ-symmetric, then $\tilde{f}(t)$ is $\zeta^2\phi$-symmetric.*

Proof. Suppose that $f^{[\phi]}(t) = f(t)$. Then

$$\begin{aligned}\tilde{f}^{[\zeta^2\phi]} &= \tilde{f}(0)^{-1}t^d\,\tilde{f}(\zeta^2\phi t^{-1}) = f(0)^{-1}t^d f(\zeta\phi t^{-1})\\ &= \zeta^d f^{[\phi]}(\zeta^{-1}t) = \zeta^d f(\zeta^{-1}t)\\ &= \tilde{f}(t).\end{aligned}$$

□

In the notation of this lemma, the following function replaces every polynomial $f(t)$ in *inv* by $\tilde{f}(t)$.

```
extendByScalar := function(inv, ζ)
  F := Parent(ζ);
  P<t> := PolynomialRing(F);
  if ζ eq F ! 1 then return < F ! 1, inv >; end if;
  newinv := {@ @};
  for polpart in inv do
    f, μ := Explode(polpart);
    ff := ζ^Degree(f) * Evaluate(f, ζ^-1 * t);
    Include(~newinv, <ff, μ>);
  end for;
  return newinv;
end function;

intrinsic InternalClassInvariantsExtSp(d :: RngIntElt, q :: RngIntElt,
    m :: RngIntElt) -> SeqEnum
{The conjugacy class invariants for the extended symplectic
  group ExtendedSp(d,q,m) of index m, q odd}
  if m eq q - 1 then return InternalClassInvariantsCSp(d, q); end if;
  if m eq 1 then return InternalClassInvariantsSp(d, q); end if;
  require IsOdd(q) : "q must be odd";
  require m gt 0 : "the index should be positive";
  divides, r := IsDivisibleBy(q - 1, m);
  require divides : "the index should divide q - 1";

  F := GF(q);
  ξ := PrimitiveElement(F);
  if IsEven(r) then
    s := r div 2;
    X := InternalClassInvariantsSp(d, q);
    invList := [];
    for i := 1 to m do
```

```
      ζ := ξ^(s*i);
      for inv in X do
        Append(~invList, < ζ^2, extendByScalar(inv,ζ)>);
      end for;
    end for;
  else
    mgrp := { ξ^(r*i) : i in [1..m] };
    invList := [ ν : ν in InternalClassInvariantsCSp(d,q) | ν[1] in mgrp ];
  end if;
  return invList;
end intrinsic;
```

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

The conjugacy classes of ExtendedSp(d,q,m).

```
classesExtSp := function(d, q, m)
  if m eq q - 1 then return classesCSp(d,q); end if;
  if m eq 1 then return classesSp(d,q); end if;
  divides, r := IsDivisibleBy(q - 1, m);
  assert divides;

  ξ := PrimitiveElement(GF(q));
  cc := [car<Integers(), Integers(), ExtendedSp(d,q,m)>| ];
  L := [];
  if IsEven(r) then
    α := ξ^(r div 2);
    X := InternalClassInvariantsSp(d,q);
    ord := OrderSp(d,q);
    invList := [];
    for i := 1 to m do
      ζ := α^i;
      for inv in X do
        μ := extendByScalar(inv,ζ);
        tag := <ζ^2,μ>;
        g := InternalRepMatrixCSp(tag);
        Append(~cc, < Order(g), ord div centraliserOrderSp(inv), g >);
        Append(~L, tag);
      end for;
    end for;
  else
    ord := OrderCSp(d,q);
    mgrp := { ξ^(r*i) : i in [1..m] };
    X := InternalClassInvariantsCSp(d,q);
    for inv in X do
      if inv[1] in mgrp then
        g := InternalRepMatrixCSp(inv);
```

```
        Append(~cc, < Order(g), ord div centraliserOrderCSp(inv), g >);
        Append(~L, inv);
      end if;
    end for;
  end if;
  ParallelSort(~cc, ~L);
  return cc, L;
end function;
```

The following intrinsic is called by InternalClassesClassical which itself is called by the C code `matg/access.c/matg_ensure_classes`.

```
intrinsic InternalClassesExtendedSp(G :: GrpMat) → BoolElt
{Internal function: attempt to assign the conjugacy classes
 of the extended symplectic group. Return true if successful}
 /*
    It is assumed that this function is called only when it is known
    that G is a finite symplectic group.
 */
  F := BaseRing(G);
  n := Dimension(G);
  M := StandardAlternatingForm(n, F);
  if forall{ g : g in Generators(G) | g*M*Transpose(g) eq M } then
    m := 1;
    std := true;
  else
    forms := SemiInvariantBilinearForms(G);
    if not exists(alt){ t : t in forms | not IsEmpty(t[3]) } then
      vprint Classes: "no (semi-)invariant alternating form";
      return false;
    end if;
    J := alt[3][1];
    X := TransformForm(J, "symplectic"); assert Type(X) ne BoolElt;
    m := LCM([ Order(g) : g in alt[1] ]);
    std := J eq M;
  end if;
  vprint Classes: "Standard copy:", std;
  L := [ ];
  q := #F;
  if IsEven(q) then
    if m eq 1 then
      cc, L := ClassicalConjugacyClasses("Sp", n, q);
      G`Labels_A := L;
    else
      vprint Classes: "extended symplectic group in characteristic 2";
      return false;
    end if;
```

```
  else
    cc, L := classesExtSp(n, q, m);
    G`LABELS_S := {@ x : x in L @};
  end if;
  if m eq 1 then
    G`CLASSICALTYPE := "Sp";
  elif m eq q-1 then
    G`CLASSICALTYPE := "CSp";
  else
    G`CLASSICALTYPE := "ExtSp";
  end if;
  if not std then
    cc := [ < t[1], t[2], X*t[3]*X^-1 > : t in cc ];
  end if;
  vprint CLASSES: "assigning symplectic classes";
  G`CLASSES := cc;
  return true;
end intrinsic;
```

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] 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.

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

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

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

[7] 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.

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

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