Notes on root systems

Markus Rost

Fakultät für Mathematik, Universität Bielefeld, Postfach 100131, D-33501 Bielefeld, Germany

Email address: `rost` *at* `math.uni-bielefeld.de`

URL: `www.math.uni-bielefeld.de/~rost`

preliminary version

October 27, 2024

(with minor changes from November 27, 2024)

Contents

Preface 5
Plans 5
Overview 5

Chapter I. Main 7

§1. $\mathcal{C}$-matrices 7
1.0.1. Infinite $\mathcal{C}$-matrices 9
§2. Root systems 11
2.1. Definition of root systems 11
2.1.1. Comments 11
2.1.2. References 12
2.2. Duals and the trace 12
2.3. Reflections 12
2.3.1. Comment 13
2.3.2. Remark 13
2.4. First properties of coroots 14
2.4.1. Comment 15
2.5. Traces of elements of finite order in $\mathrm{SL}_2(\mathbf{Z})$ 16
2.5.1. Prelude 16
2.6. Two roots 16
2.6.1. Comment 17
2.6.2. Comment 17
2.6.3. An abstract lattice 17
2.6.4. The case rank $L_{a,b} = 1$ 18
2.6.5. Comment 18
2.6.6. The case rank $L_{a,b} = 2$ 19
2.6.7. Summary 19
2.6.8. Interlude 20
2.6.9. Comment 20
2.6.10. Comment 20
2.6.11. Prospect 21
2.7. The $\mathcal{C}$-matrix of a root system 22
§3. The root system of a finite $\mathcal{C}$-matrix 22

Chapter II. Further sections 23

§4. Preliminaries (notations for sets) 23
4.1. Subset notations 23
4.2. Fix-point free involutions 24
4.3. The groups $\overline{\mathbf{Z}}[M]$ 24

4.3.1. Duals 25

Chapter III. Appendices 27
§5. Traces of rotations of finite order 27
5.0.1. Comment 1 27
5.0.2. Comment 2 28
5.0.3. Comment 3 28
5.0.4. Comment 4 28
5.0.5. Comment 5 (dynamical systems) 29
5.0.6. Comment 6 (Ω again) 30
§6. General reflections and rotations 31
6.1. Reflections 31
6.2. Rotations 32

Chapter IV. Unordered snippets 33

Bibliography 35

Preface

You are looking at Notes on root systems [pdf].

Here is a prelude: [13] (Notes on root systems (two roots), [pdf]).

Currently this is a draft of a part of projected notes on root systems.

There is more to come, hopefully.

Still collecting material...

Plans

- Recover a root system R from the set $\overline{R} = R/\{\pm 1\}$ and the set of triples in $\overline{R}$ consisting of "three roots with sum zero". Here the topic of "four roots with sum zero" plays an important role. This is motivated in parts by Tits 1966 ("Sur les constantes...") [20].
- Get a better understanding of "folding" (any root system is obtained from a simply laced one by taking invariants). Actually, this part will be hopefully about "unfolding".
- Present a construction of the Chevalley Lie algebra of a root system. Basically as in Tits 1966 ("Sur les constantes...") [20], but hopefully simpler.
- Along the way, a lot of special things showed up. Ever noticed the linear bijection $A_3 \to G_2$?

Overview

The program is very far from complete. Even the goals are not really clear. Currently the purpose of these notes is to pin down some considerations. The notion of a "$\mathcal{C}$-matrix" appeared as a first step.

Chapter I "Main" contains the current version of the notes, so to speak.

Section 1 "$\mathcal{C}$-matrices" contains a new (tentative) definition, which see.
Section 2 "Root systems" derives the properties of root systems needed for $\mathcal{C}$-matrices. The arguments are slightly non-standard.
Section 3 "The root system of a finite $\mathcal{C}$-matrix" is a stub. Expanding it is the next task.

Chapter II "Further sections" contains sections to be merged later.

Section 4 "Preliminaries" will be used in Section 3.

Chapter III "Appendices" contains what its title says.

Chapter IV "Unordered snippets" contains what its title says.

CHAPTER I

Main

§1. $\mathcal{C}$-matrices

The notion of a $\mathcal{C}$-matrix comprises properties of the family of integers

$$n(a,b) = a^*(b)$$

in a root system.

(1.1) Definition. A *$\mathcal{C}$-matrix* is a triple (R, τ, N) where R is a set,

$$\tau\colon R \to R$$

is a fix-point free involution on R and

$$N\colon R \times R \to \mathbf{Z}$$

is a function such that the following conditions (C1)–(C6) hold for a, $b \in R$:

(C1) $$N(\tau(a), b) = N(a, \tau(b)) = -N(a,b)$$

(C2) $$N(a,a) = 2$$

(C3) $$N(a,b) = N(b,a) = 2 \quad \Rightarrow \quad a = b$$

(C4) $$N(a,b) = 0 \quad \Leftrightarrow \quad N(b,a) = 0$$

(C5) $$N(a,b)N(b,a) \in \{0,1,2,3,4\}$$

(C6) There exists $s(a,b) \in R$ with

(C6s) $$N(d, s(a,b)) = N(d,b) - N(a,b)N(d,a) \qquad (d \in R)$$

(C6t) $$N(s(a,b), e) = N(b,e) - N(b,a)N(a,e) \qquad (e \in R)$$

The *transpose* of a $\mathcal{C}$-matrix (R, τ, N) is the $\mathcal{C}$-matrix (R, τ, N^t), where

$$N^t\colon R \times R \to \mathbf{Z}$$

$$N^t(a,b) = N(b,a)$$

A $\mathcal{C}$-matrix (R, τ, N) is called *symmetric* if $N^t = N$.
A $\mathcal{C}$-matrix (R, τ, N) is called *finite* if R is finite.

(1.2) Remark. The triple (R, τ, N^t) is indeed a $\mathcal{C}$-matrix as well. For instance, (C6t) is (C6s) with N replaced by N^t.

We derive some properties of a $\mathcal{C}$-matrix (R, τ, N).

(1.3) Lemma. *Let a, $b \in R$ with*

$$N(d,a) = N(d,b) \qquad (d \in R)$$

or with

$$N(a,e) = N(b,e) \qquad (e \in R)$$

Then $a = b$.

Proof: In the first condition, taking $d = a, b$ yields $N(a,a) = N(a,b)$, $N(b,a) = N(b,b)$, respectively. From (C2) one gets $N(a,b) = 2 = N(b,a)$, thus $a = b$ by (C3). Similarly for the second condition. □

(1.4) Corollary. *The element* $s(a,b)$ *in* (C6) *is unique.*
One has

$$s(\tau(a), b) = s(a,b)$$
$$s(a, \tau(b)) = \tau(s(a,b))$$

Moreover

$$s(a,a) = \tau(a)$$

and, if $N(a,b)N(b,a) = 0$,

$$s(a,b) = b$$

Proof: The first claim is immediate from Lemma (1.3). Then the τ-variances follow from (C1) and the remaining claims from (C2) resp. (C4). □

In particular, a $\mathcal{C}$-matrix comes along with the map

$$s\colon R \times R \to R$$
$$(a,b) \mapsto s(a,b)$$

Let a, $b \in R$ and write

$$m = M(a,b) = N(a,b)N(b,a) \in \{0,1,2,3,4\}$$

for the integer appearing in (C5). Since m takes only non-negative values, it follows that $N(a,b)$, $N(b,a)$ are both ≥ 0 or ≤ 0. After possibly replacing a by $\tau(a)$ (see (C1)) and interchanging a, b, one can arrange

$$0 \leq N(a,b) \leq N(b,a)$$

Under this assumption, exactly one of the following conditions holds (by looking at the factorizations of m and using (C4)):

(N0) $m = 0, \quad N(a,b) = N(b,a) = 0$

(N1) $m = 1,2,3,4, \quad N(a,b) = 1, \quad N(b,a) = m$

(N2) $m = 4, \quad N(a,b) = N(b,a) = 2, \quad a = b$

(1.5) Lemma. *The map* s *is completely determined by its restriction to pairs* a, b *with*

$$N(a,b) = 1 \quad \textit{or} \quad N(b,a) = 1$$

and also by its restriction to pairs a, b *with*

$$N(a,b) = -1 \quad \textit{or} \quad N(b,a) = -1$$

Proof: In the cases (N0), (N2), the element $s(a,b)$ is known anyway, cf. Corollary (1.4). The remaining case (N1) has to be considered up to a permutation of a, b. By the sign rule (C1) and Corollary (1.4) there remain the cases $N(a,b) = \pm 1$, $N(b,a) = \pm 1$ where the signs can be chosen arbitrarily (with two alternatives formulated in the Lemma). □

1.0.1. Infinite $\mathcal{C}$-matrices. I have no special interest in specific infinite $\mathcal{C}$-matrices. However it might be clarifying to see which definitions and arguments work smoothly in the infinite case as well.

For an infinite $\mathcal{C}$-matrix (R, τ, N) I expect that every finite subset of R is contained in a finite $\mathcal{C}$-"submatrix" (a notion we haven't defined yet, same for irreducibility).

An irreducible infinite $\mathcal{C}$-matrix should be a $\mathcal{C}$-submatrix of one of the two $\mathcal{C}$-matrices given as limit via

$$\bigcup_{n \geq 0} D_n, \qquad \bigcup_{n \geq 0} BC_n$$

The maximal irreducible $\mathcal{C}$-matrices should be these two together with G_2, F_4, E_8.

(1.6) Remark. The axioms (C1)–(C6) for $\mathcal{C}$-matrices have some redundancies.

For now Definition (1.1) serves as a convenient list of properties of root systems. After the main constructions have been worked out, one may relax one or the other axiom.

In the finite case (which we are mainly interested in anyway) one may probably drop (C4), (C5). This will become clearer (I hope) after Section 3 has been completed (constructing a root system out of a finite $\mathcal{C}$-matrix). Namely, (C4), (C5) correspond to basic properties of root systems (usually proved using the finiteness of the Weyl group).

However, we are more interested in relaxing condition (C6), see Remark (1.7).

(1.7) Remark. (This discussion is preliminary.)

Let
$$X = N^{-1}(-1) = \{\, (a,b) \mid N(a,b) = -1 \,\}$$
Consider the functions
$$u_1, u_2, v_1, v_2 \colon X \to R$$
$$u_2(a,b) = v_1(a,b) = s(a,b)$$
$$u_1(a,b) = v_2(a,b) = s(b,a)$$
As we have just noticed, each of the pairs u_1, u_2 and v_1, v_2 determine the map s.

Condition (C6) yields

(1.8) $$N(d, u_2(a,b)) = N(d,b) + N(d,a) \qquad (d \in R)$$

(1.9) $$N(u_1(a,b), e) = N(a,e) + N(b,e) \qquad (e \in R)$$

and

(1.10) $$N(d, v_2(a,b)) = N(d,a) - N(b,a)N(d,a) \qquad (d \in R)$$

(1.11) $$N(v_1(a,b), e) = N(b,e) - N(b,a)N(a,e) \qquad (e \in R)$$

Conditions (1.8), (1.9) are particularly appealing as they have no factor $N(b,a)$.

If I am not mistaken, under presence of (C1)–(C5) the existence of functions
$$u_1, u_2 \colon X \to R$$
with (1.8), (1.9) imply (C6) with s defined by
$$s(a,b) = u_2(a,b), \quad s(b,a) = u_1(a,b) \qquad \big((a,b) \in X\big)$$
The proof I have in mind at the moment is pretty long (and hasn't been fully worked out).

Further (again: if I am not mistaken), under presence of (C1)–(C5) the existence of functions
$$v_1, v_2 \colon X \to R$$
with (1.10), (1.11) also imply (C6) with s defined by
$$s(a,b) = v_1(a,b), \quad s(b,a) = v_2(a,b) \qquad \big((a,b) \in X\big)$$
Interestingly, the proof I have in mind is for the v_1, v_2-case considerably simpler than for the u_1, u_2-case.

For the v_1, v_2-case I have no application in mind, except for a better understanding of the various possibilities to ensure condition (C6) for a $\mathcal{C}$-matrix.

§2. Root systems

In this section we define root systems and establish some (well known) properties. The goal is to show in the end that a root system defines a $\mathcal{C}$-matrix (Proposition (2.24)).

Along the way we do not shy away from further comments and discussions.

Our general reference for root systems is Serre 2001 (1966) [15, Chapter V. Root systems, p. 24]. (I don't have the French original.)

Another major reference: Bourbaki 1968 [3, Chapitre VI. Systèmes des racines, p. 142], English translation: Bourbaki 2002 (1968) [4, Chapter VI. Root Systems, p. 155].

2.1. Definition of root systems.

(2.1) Definition. A *root system* is a pair (V, R) where V is an $\mathbf{R}$-vector space and

$$R \subset V \setminus \{0\}$$

is a subset of nonzero vectors in V such that the following conditions hold:

(R0.1) R is finite.

(R0.2) R generates V as $\mathbf{R}$-vector space.

(R1) For each $a \in R$ there exists an $\mathbf{R}$-linear map

$$a^*\colon V \to \mathbf{R}$$

with

(R1.1) $$a^*(R) \subset \mathbf{Z}$$

(R1.2) $$a^*(a) = 2$$

(R1.3) $$b - a^*(b)a \in R \qquad (b \in R)$$

An element $a \in R$ is called a *root* of the root system.

A linear form a^* as in (R1) is called a *coroot of* a.

The dimension

$$n = \dim_{\mathbf{R}} V$$

of V is called the *rank* of the root system.

One also speaks of R as a *root system in* V.

(2.2) Remark. Coroots are uniquely determined, see the subsequent Lemma (2.7). Hence one may speak of *the* coroot a^* of a.

The rank is finite by (R0.1), (R0.2).

One has

$$R = -R$$

(take $b = a$ in (R1.3) and use (R1.2)).

2.1.1. Comments. Definition (2.1) adopts the definition in Bourbaki [3] for the case of the ground field $\mathbf{R}$. It is equivalent to the definition in Serre [15].

However it is formulated entirely in terms of coroots. This comes arguably close to the definition of a $\mathcal{C}$-matrix (Definition (1.1)). A side effect is that there is no need for a preceding discussion of symmetries or reflections (to be considered next).

2.1.2. References. There are of course many places where root systems are defined. Here is a list of related articles and books, most of which I haven't digested or looked at a long time ago (so this is rather a to-do list for myself).

Bourbaki [3], Serre [15] (see above).

Tits 1966 ("Sur les constantes…") [20, 3. Systèmes des racines, p. 37 (541)] has almost the same wording as Definition (2.1) but assumes additionally that the root system is reduced, that is $\mathbf{Q}a \cap R = \{\pm a\}$.

Tits 1966 ("Normalisateurs de tores") [19, 4.1. Systèmes des racines, p. 111] starts with a free abelian group V, generated over $\mathbf{Q}$ by R and the intersection of the hyperplanes $\ker a^*$. R is reduced.

The notion of "root data" starts with a dual pair of root lattices, see SGA3 [6, Exposé XXI, Donnés radicielles, M. Demazure, p. 85], Springer 1979 [16], Springer 2009 (1981) [17, 7. Weyl group, Roots, Root Datum, 7.4. Root data, p. 124]

Some books: (Springer, Humphreys, Humphreys, Fulton-Harris, Borel) [17, 9, 10, 7, 2].

Comments and further suggestions are welcome.

2.2. Duals and the trace. In the following, V can be a finitely generated locally free module over some ring k. We are mainly interested in the cases $k = \mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$. In the case of fields, V is a finite-dimensional vector space. When $k = \mathbf{Z}$, V is a finitely generated free abelian group. In any of these cases, V has a k-basis ($V \simeq k^n$).

The dual space of V is denoted by

$$V^\vee = \operatorname{Hom}(V, k)$$

For a k-module W we identify

$$V^\vee \otimes W = \operatorname{Hom}(V, W)$$

via the natural isomorphism

$$\varphi \otimes w \mapsto (v \mapsto \varphi(v)w)$$

In particular

$$V^\vee \otimes V = \operatorname{End}(V)$$

This way the trace map

$$\operatorname{trace}\colon \operatorname{End}(V) \to k$$

reads as evaluation:

$$\operatorname{trace}(\varphi \otimes v) = \varphi(v)$$

2.3. Reflections. References:

Serre [15, Chapter V. Root systems, 1. Symmetries, p. 24–25],

Bourbaki 1968 [3, Chapitre V. Groupes engendrés par des réflexions, §2 Réflexions, p. 66], Bourbaki 2002 [4, Chapter V. Groups generated by reflections, §2 Reflections, p. 70].

In the following, the ground field is $\mathbf{R}$ (or any field with $\operatorname{char} \neq 2$, resp. $\operatorname{char} = 0$ starting from Lemma (2.6)).

(2.3) Definition. A *reflection in V* is an endomorphism s of V which leaves a hyperplane $H \subset V$ pointwise fixed and such that the induced endomorphism on the line V/H is multiplication by -1.

If $v \in V \setminus \{0\}$, a *symmetry with vector v* is a reflection in V with $s(v) = -v$.

(The latter wording is very convenient. It has been taken from Serre [15].)

A decomposition

$$V = V_{-1} \oplus V_{+1}, \qquad \operatorname{rank} V_{-1} = 1$$

yields a reflection with matrix

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

and any reflection is of this form with $V_{\pm 1}$ as eigenspaces (by Definition (2.3), the eigenvalues are ± 1 and the subspace of $+1$-eigenvectors has codimension 1). In particular, a reflection s is of order 2:

$$s^2 = 1$$

Other descriptions of reflections are

(2.4) Lemma. *An endomorphism s is a reflection if and only if it is in*

$$\operatorname{End}(V) = V^\vee \otimes V$$

of the form

$$s = 1 - \varphi \otimes v$$

with $\varphi \in V^\vee$, $v \in V$ such that

$$\varphi(v) = 2$$

(In this case s is a symmetry with vector v and $V_{+1} = \ker \varphi$.) □

(2.5) Lemma. *An endomorphism s is a reflection if and only if $t = 1 - s$ has the properties*

$$\operatorname{rank} t = 1$$
$$\operatorname{trace} t = 2$$

(In this case $V_{-1} = \operatorname{im} t$ and $V_{+1} = \ker t$.) □

2.3.1. Comment. Lemma (2.5) yields a quick description/definition of reflections in terms of the map

$$t = 1 - s \colon V/V_{+1} \to V_{-1}$$

of rank 1. The "residual space" $(1-s)(V) \subset V$ appears also in other contexts, for instance for s in an orthogonal group (in particular in characteristic 2).

2.3.2. Remark. Consider the integral 2×2-matrices

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z})$$

When considered in $\mathrm{GL}_2(\mathbf{R})$, both of A and B are reflections. However, when passing to $\mathrm{GL}_2(\mathbf{F}_2)$, A becomes the identity, while the B becomes a non-trivial transvection.

Over the base ring $\mathbf{Z}$, the matrix B is not diagonalizable: the eigenvectors

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

span a subgroup of $\mathbf{Z}^2$ of index 2.

On the other hand, B is conjugated in $\mathrm{GL}_2(\mathbf{Z})$ to the permutation matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Hence $\mathbf{Z}^2$ is a free module over the group $\{1, B\}$ $(B^2 = 1)$.

It is not difficult to see that any $s \in \mathrm{GL}_2(\mathbf{Z})$ which over $\mathbf{R}$ is a reflection is conjugated in $\mathrm{GL}_2(\mathbf{Z})$ to A or B.

For root systems, the following remark is important.

(2.6) Lemma. *In a finite group of automorphisms of V, every element is diagonalizable and there is at most one reflection for a given -1-eigenspace.*

Proof: Since $\operatorname{char} \mathbf{R} = 0$, Jordan blocks of size > 1 and with non-zero eigenvalue have infinite order. Let s, s' be two reflections with same -1-eigenspace and let

$$V = V_{-1} \oplus V_{+1}$$

be the eigenspace decomposition for s. The induced endomorphisms on V/V_{-1} are the identity. Thus s, s', ss' have the form

$$s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad s' = \begin{pmatrix} -1 & f \\ 0 & 1 \end{pmatrix}, \qquad ss' = \begin{pmatrix} 1 & -f \\ 0 & 1 \end{pmatrix}$$

Hence $f = 0$ and so $s' = s$. □

Given a root system (V, R), let

$$\mathrm{Aut}(V, R) \subset \mathrm{GL}(V)$$

be the subgroup of automorphisms leaving R invariant. Since R generates V, the natural map $\mathrm{Aut}(V, R) \to \Sigma_R$ to the permutation group of R is injective. Since R is finite, it follows that $\mathrm{Aut}(V, R)$ is finite.

2.4. First properties of coroots. Let (V, R) be a root system.

Fix a family of coroots a^* $(a \in R)$ as in (R1).

For a root a, let

$$s_a : V \to V$$
$$s_a = 1 - a^* \otimes a$$
$$s_a(v) = v - a^*(v)a$$

Since $a^*(a) = 2$ by (R1.2), the endomorphism s_a is a reflection and a symmetry with vector a. Its eigenspace decomposition is

$$V = a\mathbf{R} \oplus H_a$$

with $+1$-eigenspace the hyperplane

$$H_a = \ker a^* \subset V$$

Condition (R1.3) means that s_a leaves R invariant,

$$s_a(R) \subset R$$

that is, $s_a \in \mathrm{Aut}(V, R)$.

We are ready to prove uniqueness of the coroots.

(2.7) Lemma. *Let*

$$a^*, a^{*\prime}\colon V \to \mathbf{R}$$

be two coroots of a. *Then* $a^{*\prime} = a^*$.

Proof: The reflection s_a and the reflection

$$s'_a = 1 - a^{*\prime} \otimes a$$

corresponding to $a^{*\prime}$ are both symmetries with vector a and in the finite group $\mathrm{Aut}(V, R)$. Hence $s'_a = s_a$ by Lemma (2.6) and the claim follows. □

Here comes an important coroot computation.

(2.8) Lemma. *Let* a, $b \in R$ *and let* $c = s_a(b)$. *Then*

$$s_c = s_a s_b s_a \tag{2.9}$$

$$c^* = b^* \circ s_a \tag{2.10}$$

$$c^* = b^* - b^*(a)a^* \tag{2.11}$$

Proof: The first claim follows from Lemma (2.6), since both of s_c and $s_a s_b s_a^{-1}$ are symmetries with vector c and are in the finite group $\mathrm{Aut}(V, R)$.

The second claim follows then from an inspection of

$$\begin{aligned} s_b &= 1 - b^* \otimes b \\ s_a s_b s_a &= 1 - (b^* \circ s_a) \otimes s_a(b) \\ s_c &= 1 - c^* \otimes c \end{aligned}$$

Making it explicit yields the third claim:

$$c^*(v) = \big(b^* \circ s_a\big)(v) = b^*\big(v - a^*(v)a\big) = \big(b^* - b^*(a)a^*\big)(v)$$

□

2.4.1. Comment. Let q be a definite Weyl invariant quadratic form on V and let

$$\langle v, w\rangle = q(v + w) - q(v) - q(w)$$

be the associated symmetric bilinear form (so that $\langle v, v\rangle = 2q(v)$). Then

$$a^*(v) = \frac{\langle a, v\rangle}{q(a)} \qquad (a \in R)$$

The computation (2.11) follows also like this

$$c^*(v) = \frac{\langle c, v\rangle}{q(c)} = \frac{\langle b - a^*(b)a, v\rangle}{q(b)} = b^*(v) - \frac{\langle b^*(a)a, v\rangle}{q(a)} = b^*(v) - b^*(a)a^*(v)$$

using, of course,

$$\frac{a^*(b)}{q(b)} = \frac{\langle a, b\rangle}{q(a)q(b)} = \frac{b^*(a)}{q(a)} \tag{2.12}$$

Strangely, I don't know an explicit reference for (2.11). On the other hand, (2.10) is part of establishing the inverse root system (not yet included in this text). Comments and suggestions are welcome.

References for Weyl invariant quadratic forms:

Serre [15, Chapter V. Root systems, 5. Invariant quadratic forms, pp. 27],

Bourbaki 1968 [3, Chapitre VI. Systèmes des racines, pp. 143], Bourbaki 2002 (1968) [4, Chapter VI. Root Systems, pp. 156].

2.5. Traces of elements of finite order in $\mathrm{SL}_2(\mathbf{Z})$.

2.5.1. Prelude.

$m = 2 + \mathrm{Trace}(f)$	Trace	Order	Example	$s_a s_b = f$
0	-2	2	$\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right) = \left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)$
1	-1	3	$\left(\begin{smallmatrix}0 & -1\\ 1 & -1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}-1 & 1\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 1 & -1\end{smallmatrix}\right) = \left(\begin{smallmatrix}0 & -1\\ 1 & -1\end{smallmatrix}\right)$
2	0	4	$\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}-1 & 1\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 2 & -1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1 & -1\\ 2 & -1\end{smallmatrix}\right)$
3	1	6	$\left(\begin{smallmatrix}0 & -1\\ 1 & 1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}-1 & 1\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 3 & -1\end{smallmatrix}\right) = \left(\begin{smallmatrix}2 & -1\\ 3 & -1\end{smallmatrix}\right)$
4	2	1	$\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$	-

The table will be explained soon. By the way, filling the empty spot yields elements of order ∞:

$$m = 1 \cdot 4: \qquad \begin{pmatrix}-1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 4 & -1\end{pmatrix} = \begin{pmatrix}3 & -1\\ 4 & -1\end{pmatrix} = 1 + \begin{pmatrix}1\\ 2\end{pmatrix}\begin{pmatrix}2 & -1\end{pmatrix}$$

$$m = 2 \cdot 2: \qquad \begin{pmatrix}-1 & 2\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 2 & -1\end{pmatrix} = \begin{pmatrix}3 & -2\\ 2 & -1\end{pmatrix} = 1 + 2\begin{pmatrix}1\\ 1\end{pmatrix}\begin{pmatrix}1 & -1\end{pmatrix}$$

Sometimes we write $T(f) = \mathrm{trace}(f)$ for the trace of an endomorphism f.

(2.13) Lemma. *Let $f \in \mathrm{SL}_2(\mathbf{Z})$ have finite order n. The possible traces of f are*

$$T(f) = -2, -1, 0, 1, 2$$

If $T(f) = -2$, then $f = -1$. If $T(f) = 2$, then $f = 1$.

The corresponding orders are

$$n = 2, 3, 4, 6, 1$$

Proof: Each eigenvalue of f is an n-th root of unity. Since $\det(f) = 1$, the two eigenvalues are reciprocal, hence of the form $\cos\varphi \pm i\sin\varphi$ for some φ. Moreover,

$$2\cos\varphi = T(f) \in \mathbf{Z}$$

is integral and $|\cos\varphi| \leq 1$ yields the lists of possible traces.

If $T(f) = \pm 2$, there is only one eigenvalue ± 1. By Lemma (2.6), f is diagonalizable, hence conjugated over $\mathbf{R}$ to ± 1. Since ± 1 is central, this means $f = \pm 1$.

The corresponding orders are the orders of the eigenvalues. □

2.6. Two roots.

Let (V, R) be a root system.

For two roots a, b define the integer

$$m = m(a, b) = a^*(b) b^*(a) \in \mathbf{Z}$$

(2.14) Lemma. *One has*

$$m(a, b) \in \{0, 1, 2, 3, 4\} \tag{2.15}$$

and

$$m(a, b) = 0 \quad \Rightarrow \quad a^*(b) = b^*(a) = 0 \tag{2.16}$$

$$a^*(b) = b^*(a) = 2 \quad \Rightarrow \quad a = b \tag{2.17}$$

Moreover

$$m(a, b) = 4 - \mathrm{trace}(1 - s_a s_b) \tag{2.18}$$

2.6.1. Comment. The trace description (2.18) of $m(a, b)$ is currently not used. However it is appealing, because it doesn't explicitly refer to coroots, but rather to generators of the Weyl (or Coxeter) group.

We give the 5-element set a prominent notation:

$$\Omega = \{0, 1, 2, 3, 4\}$$

This is all about Ω!

We are going to prove Lemma (2.14).

For two roots a, $b \in R$ let

$$L_{a,b} = a\mathbf{Z} + b\mathbf{Z} \subset V$$

be the subgroup generated by them. This is a free abelian group of rank 1 or 2. By (R1.1) one has

$$s_a(L_{a,b}) \subset L_{a,b}$$

2.6.2. Comment. One would like to speak of the root subsystem generated by a, b. We plan to define later the notions of a root subsystem and of the root subsystem generated by a subset of R. I think everybody knows what these mean, but, strangely, there seems to be no precise discussion in the literature—comments and suggestions are welcome. (There is a small subtlety about changing the ambient vector space V.)

FIXME. The motivation for the following is to treat the cases

$$\operatorname{rank} L_{a,b} = 1, \qquad \operatorname{rank} L_{a,b} = 2$$

simultaneously. I am not sure yet whether this is a good idea or just an unnecessary complication. Anyway, the following presentation is preliminary.

Lemma (2.14) follows of course also from standard references on the classification of root systems of rank 2.

2.6.3. An abstract lattice. We consider an abstraction of $L_{a,b}$ together with the endomorphisms

$$S_a = s_a|L_{a,b}, \qquad S_b = s_b|L_{a,b}$$

Let

$$L_0 = \mathbf{Z}^2$$

and let h, $k \in \mathbf{Z}$. Then

$$\alpha = \begin{pmatrix} -1 & h \\ 0 & 1 \end{pmatrix} = 1 - \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 2 & -h \end{pmatrix}$$

$$\beta = \begin{pmatrix} 1 & 0 \\ k & -1 \end{pmatrix} = 1 - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} -k & 2 \end{pmatrix}$$

are reflections (in $L_0 \otimes \mathbf{R}$) with eigenvectors

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} h \\ 2 \end{pmatrix} \quad \text{resp.} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ k \end{pmatrix}$$

Note that

(2.19)
$$\gamma = \alpha\beta = \begin{pmatrix} hk - 1 & -h \\ k & -1 \end{pmatrix}$$

has trace

$$T(\gamma) = hk - 2$$

(2.20) Remark. Section 2.5.1 lists α, β, γ for the cases

$$hk \in \Omega = \{0, 1, 2, 3, 4\}$$
$$(h, k) = (0, 0), (1, 1), (1, 2), (1, 3), (1, 4), (2, 2)$$

Take

$$h = -a^*(b)$$
$$k = -b^*(a)$$

so that $hk = m$.

The epimorphism

$$\lambda\colon L_0 \to L_{a,b}$$
$$\lambda(x, y) = xa + yb$$

has the properties

$$\lambda \circ \alpha = S_a \circ \lambda \qquad \textbf{(2.21)}$$
$$\lambda \circ \beta = S_b \circ \lambda$$

2.6.4. The case $\operatorname{rank} L_{a,b} = 1$**.** In this case $U = \ker \lambda$ has rank 1. (2.21) shows $\alpha(U)$, $\beta(U) \subset U$. Hence U is contained in an eigenspace of α and of β. Since a, $b \neq 0$, the only possibilities are

$$\begin{pmatrix} h \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ k \end{pmatrix} \in U$$

But then

$$0 = \det \begin{pmatrix} h & 2 \\ 2 & k \end{pmatrix} = hk - 4 = m - 4$$

Hence $m = 4$ and, after possibly changing a sign of a or b and interchanging a, b, there are the two cases

$$a^*(b) = b^*(a) = 2 \qquad \textbf{(2.22)}$$
$$a^*(b) = 4, \qquad b^*(a) = 1$$

In the first case one gets $h = k = -2$ and U is generated by $(1, -1)$, hence $a = b$. We have the root system

$$\{\pm a\}$$

of type A_1.

In the second case U is generated by $(2, -1)$ and one gets $b = 2a$. We have the root system

$$\{\pm a, \pm 2a\}$$

of type BC_1.

2.6.5. Comment. We plan to describe details for at least some of the particular root systems of the various types A_n, B_n, ... later. For moment we refer to Bourbaki [3], Serre [15].

2.6.6. The case $\operatorname{rank} L_{a,b} = 2$**.** In this case λ is an isomorphism and γ has finite order (since $\lambda\gamma\lambda^{-1} = (s_a s_b)|L_{a,b}$ and $s_a s_b \in \operatorname{Aut}(V, R)$). By Lemma (2.13) one gets

$$m = 2 + T(\gamma) \in 2 + \{-2, -1, 0, 1, 2\} = \Omega$$

Moreover, if $m = 0$, then $\gamma = -1$ and (2.19) shows $a^*(b) = b^*(a) = 0$. And if $m = 4$, then $\gamma = 1$ which is impossible, cf. (2.19).

For the record:

$$m = 4 \quad \Leftrightarrow \quad \operatorname{rank} L_{a,b} = 1$$

and the first part of Lemma (2.14) is proved.

Finally let us show (2.18). If $\operatorname{rank} L_{a,b} = 1$, then $s_a = s_b$ and the claim is clear. Otherwise $m \neq 4$. The map

$$\Phi\colon \mathbf{R}^2 \xrightarrow{(a,\,b)} V \xrightarrow{(a^*,\,b^*)} \mathbf{R}^2$$

has matrix

$$\begin{pmatrix} 2 & a^*(b) \\ b^*(a) & 2 \end{pmatrix} \in M_2(\mathbf{Z})$$

with determinant $4 - m$. But $\det \Phi \neq 0$ means that the vector space V is the direct sum of $H_a \cap H_b$ and $L_{a,b} \otimes \mathbf{R}$. Since $1 - s_a s_b$ vanishes on $H_a \cap H_b$, its trace can be computed on $L_{a,b}$. One finds indeed

$$\operatorname{trace}(1 - s_a s_b) = \operatorname{trace}(1 - \gamma) = 4 - m$$

Lemma (2.14) is proved.

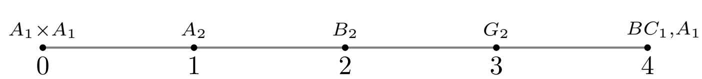
(2.23) Lemma. *If a, b are $\mathbf{R}$-proportional, say $b = ta$, then*

$$t \in \{\pm 1, \pm 2, \pm 2^{-1}\}$$

Proof: If a, b are $\mathbf{R}$-linearly dependent, then $\det \Phi = 0$. Hence $m = 4$ and we are in the case $\operatorname{rank} L_{a,b} = 1$ which falls into the cases described in and after (2.22). (For a simpler argument, see Serre [15, end of p. 25]). □

2.6.7. Summary. In the following $R(a, b)$ is meant to be the root system generated by a, b (as this notion is not yet defined, the reader may take for $R(a, b)$ the corresponding known root system of rank 2 with appropriate choices for a, b).

(1) If $m(a, b) = 0$, then $a^*(b) = b^*(a) = 0$ and $R(a, b)$ is of type $A_1 \times A_1$.
(2) If $m(a, b) = 1$, then $R(a, b)$ is of type A_2.
(3) If $m(a, b) = 2$, then $R(a, b)$ is of type B_2.
(4) If $m(a, b) = 3$, then $R(a, b)$ is of type G_2.
(5) If $m(a, b) = 4$ and $a^*(b) = 4$, then $b = 2a$ and $R(a, b)$ is of type BC_1.
(6) If $m(a, b) = 4$ and $a^*(b) = 2$, then $b = a$ and $R(a, b)$ is of type A_1.



2.6.8. Interlude. Here is a table from my schooldays. Its rows are related to the root systems BC_1, G_2, B_2, A_2, $A_1 \times A_1$, respectively.

Werte der trigonometrischen Funktionen für 0°, 30°, 45°, 60° und 90°.

(nach Bronstein-Semendjajew[1])

Winkel	Bogen	sin	cos	tan	cot	sec	csc
0°	0	0	1	0	$\mp\infty$	1	$\mp\infty$
30°	$\frac{1}{6}\pi$	$\frac{1}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{3}}{3}$	$\sqrt{3}$	$\frac{2\sqrt{3}}{3}$	2
45°	$\frac{1}{4}\pi$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{2}}{2}$	1	1	$\sqrt{2}$	$\sqrt{2}$
60°	$\frac{1}{3}\pi$	$\frac{\sqrt{3}}{2}$	$\frac{1}{2}$	$\sqrt{3}$	$\frac{\sqrt{3}}{3}$	2	$\frac{2\sqrt{3}}{3}$
90°	$\frac{1}{2}\pi$	1	0	$\pm\infty$	0	$\pm\infty$	1

2.6.9. Comment. Obviously we do not try be brief in our account of properties of root systems—in this regard, there is no better text than the booklet Serre [15].

Features of our treatment are:

- The use of the lattice L_0 clarifies, I think, the case distinction $\operatorname{rank} L_{a,b} = 1$, $\operatorname{rank} L_{a,b} = 2$.
- Weyl invariant quadratic forms are not used. The arguments are rather "local" at two roots (but use the finiteness of R).

2.6.10. Comment. Clearly Weyl invariant quadratic forms provide a very convenient tool (see Comment 2.4.1 for an example) and are normally used at a very basic level.

(And, by the way, the group of integral Weyl invariant quadratic forms appears for the cohomological H^3-invariant for the corresponding simply connected Chevalley group. Reference: Garibaldi-Merkurjev-Serre 2003 [8, 6.10, 6.12, p. 118].)

Weyl invariant quadratic forms are usually obtained by choosing some definite form and making it Weyl invariant by integration. Or one defines one right away by taking

$$\sum_{a \in R} (a^*)^2$$

as in Tits 1966 ("Sur les constantes...") [20, 3.2.1. La fonction λ, p. 38 (542)]. For two given roots, there is a rather delightful construction, see Section 2.6.11.

Note that the section "Invariant quadratic forms" in Serre [15, Chapter V. Root systems, 5. Invariant quadratic forms, p. 28] rather considers symmetric bilinear forms $\langle\ ,\ \rangle$. When starting with a quadratic form q, the coroot is given by the inversion formula

$$a^* = \frac{a}{q(a)} \in V = V^\vee$$

upon identifying V with its dual $V^\vee$ by means of the bilinear form $\langle\ ,\ \rangle$ of q. There is no factor 2 as in the customary formula

$$a^* = \frac{2a}{\langle a, a\rangle} \in V = V^\vee$$

[1] From [5, p. 79]. In a recent edition, the table got split: [21, p. 59, p. 65]

2.6.11. Prospect. Let L be a module of rank 2 (locally free, over some ring) and let $f \in \mathrm{End}(L)$. Consider the quadratic map

$$q_f \colon L \to \Lambda^2 L$$
$$q_f(x) = x \wedge f(x)$$

(This is actually a linear module homomorphism

$$S_2 L \to \Lambda^2 L$$
$$x^{\otimes 2} \mapsto x \wedge f(x)$$

where $S_2 L \subset L^{\otimes 2}$ is the submodule of tensors invariant under the switch involution.)

The map q_f is a quadratic form in the usual sense (taking values in the base ring) only after choosing a basis of the rank 1-module $\Lambda^2 L$.

The map q_f is equivariant under f:

$$q_f(f(x)) = f(x) \wedge f^2(x) = \Lambda^2(f) q_f(x)$$

(by the way, $\Lambda^2(f) = \det(f)$).

Applying this to $L = L_{a,b}$ (assuming the rank 2 case) and the rotation $S_a S_b$ (with $S_a = s_a | L_{a,b}$) yields the quadratic map

$$q_{a,b} \colon S_2 L \to \Lambda^2 L \simeq \mathbf{Z}$$
$$q_{a,b}(x) = x \wedge S_a S_b(x) = -S_a(x) \wedge S_b(x)$$

which can be turned into a quadratic form via

$$q'_{a,b}(x) = \frac{q_{a,b}(x)}{a \wedge b} \in \mathbf{Z}$$

The form $q'_{a,b}$ is invariant under the group $W \subset \mathrm{GL}(L_{a,b})$ generated by S_a, S_b. It is non-zero and definite if $m \neq 0, 4$ (if $m = 0, 4$, then $S_a S_b = \mp 1$ and $q_{a,b} = 0$).

One has for instance

$$q_{a,b}(b) = b \wedge S_a(-b) = -b \wedge (-a^*(b) a)$$

and so

$$q'_{a,b}(b) = -a^*(b)$$

We hope to discuss more details later. (Probably only after the inverse root system given by the coroots has been established.)

2.7. The $\mathcal{C}$-matrix of a root system. Definition (2.1), Lemma (2.14), and the coroot computation (2.11)

$$c = b - a^*(b)a$$
$$c^* = b^* - b^*(a)a^*$$

yield:

(2.24) Proposition. *A root system R defines a $\mathcal{C}$-matrix (R, τ, N) (called the $\mathcal{C}$-matrix of the root system) by taking*

$$\tau(a) = -a$$

and

$$N(a, b) = a^*(b)$$

where a^* is the coroot of a.

The function s is given by the reflections of the root system as follows:

$$s(a, b) = s_a(b)$$

□

If $S \subset R$ is a base of the root system, the restriction of N to $S \times S$ is known as the *Cartan matrix* with respect to S.

A root system with symmetric $\mathcal{C}$-matrix (or Cartan matrices) is usually called a *simply laced* root system.

§3. The root system of a finite $\mathcal{C}$-matrix

Our goal is to turn a finite $\mathcal{C}$-matrix into a root system. A first step is to construct the ambient vector space V.

Let (R, τ, N) be a finite $\mathcal{C}$-matrix.

We use the notations of Section 4.3.

We consider $N \colon R \times R \to \mathbf{Z}$ as bilinear map

$$N \colon \mathbf{Z}[R] \times \mathbf{Z}[R] \to \mathbf{Z}$$
$$\big(e(a), e(b)\big) \mapsto N(a, b)$$

Taking the dual of the first factor yields

$$\widetilde{N} \colon \mathbf{Z}[R] \to \mathbf{Z}[R]$$
$$e(a) \mapsto \sum_{d \in R} N(d, a) e(d)$$

One now puts

$$L = \operatorname{im} \widetilde{N}, \qquad V = L \otimes \mathbf{R}$$

(Taking the dual of the second factor yields the lattice and vector space of the inverse root system.)

To establish the desired properties needs some preparations.

To be continued…

CHAPTER II

Further sections

This “chapter” contains preliminary sections to be merged later.

§4. Preliminaries (notations for sets)

Let M be a set and let $k \geq 0$ be a non-negative integer.

The group of permutations of M is denoted by

$$\Sigma_M = \{ f\colon M \to M \mid f \text{ is bijective} \}$$

Particular cases are the standard permutation groups

$$\Sigma_k = \Sigma_{\{1,\ldots,k\}}$$

4.1. Subset notations. We write

$$\mathcal{S}_k M = \binom{M}{k} = \{ U \subset M \mid |U| = k \}$$

for the set of (unordered) k-element subsets of M. For an *injective* map $f\colon M \to N$ of sets let

$$\mathcal{S}_k f\colon \mathcal{S}_k M \to \mathcal{S}_k N$$
$$\mathcal{S}_k f(\{x_1,\ldots,x_k\}) = \{f(x_1),\ldots,f(x_k)\}$$

be the induced map.

Moreover let

$$S^k M = M^k/\Sigma_k$$

denote the set of unordered k-tuples in M (with possible repetitions). Its elements are denoted by

$$[x_1,\ldots,x_k] = \Sigma_k \cdot (x_1,\ldots,x_k)$$

For a map $f\colon M \to N$ of sets let

$$S^k f\colon S^k M \to S^k N$$
$$S^k f([x_1,\ldots,x_k]) = [f(x_1),\ldots,f(x_k)]$$

be the induced map.

The set $S^k M$ contains the subsets

$$M = \operatorname{diag}_k(M), \qquad \binom{M}{k}$$

containing the diagonal elements $[x,\ldots,x]$ and the tuples without repetitions, respectively. The latter elements will be denoted by the corresponding k-element set $\{x_1,\ldots,x_k\}$ as well.

Clearly

$$S^2 M = \binom{M}{2} \cup \operatorname{diag}_2(M)$$

For $k = 3$ there is the decomposition

$$S^3M = \binom{M}{3} \cup S^{2,1}M \cup \mathrm{diag}_3(M)$$

according to the cases $\{x_1, x_2, x_3\}$, $[x, x, y]$ $(x \neq y)$, $[x, x, x]$ (with $S^{2,1}M \subset S^3M$ the subset of triples with a single repetition).

4.2. Fix-point free involutions. Let

$$\tau\colon M \to M$$

be a fix-point free involution on M. This means $\tau(x) \neq x$ and $\tau(\tau(x)) = x$ for $x \in M$. In other words, the group $C_2 = \{1, \tau\}$ of order 2 acts freely on M.

Consider the natural action of τ on S^kM (via $S^k\tau$). For odd k it is fix-point free as well, since a fixed point $[x_1, \dots, x_k]$ decomposes into pairs $[x_j, \tau(x_j)]$.

4.3. The groups $\overline{\mathbf{Z}}[M]$. We denote by $\mathbf{Z}[M]$ the free abelian group on M. The generator for $x \in M$ is sometimes denoted by the same letter x, for instance in a group ring $\mathbf{Z}[G]$. For clarity and emphasis, we normally use the notation e_x or even $e(x)$. Thus

$$\mathbf{Z}[M] = \bigoplus_{x \in M} \mathbf{Z}e(x)$$

Given a fixed point free involution $\tau\colon M \to M$, we write

$$\overline{M} = M/\{1, \tau\}$$

for the set of orbits with the elements of $\overline{M}$ denoted as

$$[x] = \{x, \tau(x)\} \in \overline{M}$$

Further we put

$$\overline{\mathbf{Z}}[M] = \mathbf{Z}[M]/(1 + \tau)\mathbf{Z}[M]$$

FIXME. `This is an abuse of notation, it would be clearer to write something like`

$$\mathbf{Z}[M]_{-\tau} = \mathbf{Z}[M]/(1 + \tau)\mathbf{Z}[M]$$

The group $\overline{\mathbf{Z}}[M]$ has the presentation with generators

$$E(x) = e(x) \bmod (1 + \tau)\mathbf{Z}[M] \qquad (x \in M)$$

and relations

$$E(\tau(x)) = -E(x) \qquad (x \in M)$$

Thus

$$\overline{\mathbf{Z}}[M] = \bigoplus_{w \in \overline{M}} \mathbf{Z}_w$$

with the summands $\mathbf{Z}_{[x]} \simeq \mathbf{Z}$ generated by $E(x) = -E(\tau(x))$. The involution τ acts on $\overline{\mathbf{Z}}[M]$ by multiplication with -1, obviously.

(4.1) Remark. The group $\overline{\mathbf{Z}}[M] = \mathbf{Z}[M]/(1+\tau)\mathbf{Z}[M]$ could be called the group of anti-coinvariants. When allowing arbitrary involutions, there is a summand $\mathbf{Z}/2\mathbf{Z}$ for each fixed point.

In the case $M = \{1, \tau\}$ one gets

$$\mathbf{Z}(\tau) = \mathbf{Z}[\{1,\tau\}]/(1+\tau)\mathbf{Z}[\{1,\tau\}]$$

that is, the group $\mathbf{Z}$ with τ acting by -1. Then

$$\overline{\mathbf{Z}}[M] = H_0\big(\{1,\tau\}, \mathbf{Z}[M] \otimes \mathbf{Z}(\tau)\big)$$

4.3.1. Duals. The $\mathbf{Z}$-duals are

$$\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}[M], \mathbf{Z}) = \mathbf{Z}^M = \{f\colon M \to \mathbf{Z}\}$$

$$\mathrm{Hom}_{\mathbf{Z}}(\overline{\mathbf{Z}}[M], \mathbf{Z}) = \big(\mathbf{Z}(\tau)^M\big)^\tau = \{\, f\colon M \to \mathbf{Z} \mid f(\tau(x)) = -f(x) \,\}$$

There are the natural inclusions

$$\mathbf{Z}[M] \to \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}[M], \mathbf{Z})$$
$$e(a) \mapsto \delta_a$$

and

$$\overline{\mathbf{Z}}[M] \to \mathrm{Hom}_{\mathbf{Z}}(\overline{\mathbf{Z}}[M], \mathbf{Z})$$
$$E(a) \mapsto \delta_a - \delta_{-a}$$

where $\delta_a(b)$ is the Kronecker delta. If M is finite, these are bijections.

CHAPTER III

Appendices

§5. Traces of rotations of finite order

Here is a variation of the argument to get the possible traces as in Lemma (2.13).

For $f \in M_2(k)$ the Caley-Hamilton theorem (which for 2×2-matrices is quickly verified) says

$$f^2 = T(f)f - \det(f)$$

For $f \in \mathrm{SL}_2(k)$ one gets

$$f^2 = T(f)f - 1 \tag{5.1}$$

This gives a recursion for the powers f^n, and a fortiori for their traces $T(f^n)$. If f is of finite order, the sequence $T(f^n)$ is finite. So it is natural to check what happens when starting from an integer $T(f) \in \mathbf{Z}$.

In fact, one quickly succeeds to get the desired restrictions for $T(f)$ by iterating $f \mapsto f^2$: Taking in (5.1) the trace yields

$$T(f^2) = T(f)^2 - 2 \tag{5.2}$$

One now observes that for the iterates of the function

$$q\colon \mathbf{R} \to \mathbf{R}$$
$$q(n) = n^2 - 2$$

the sequence $q^{\circ k}(n)$ $(k \geq 1)$ is bounded exactly for $-2 \leq n \leq 2$. Hence, if $T(f) \in \mathbf{Z}$ and f has finite order, then indeed

$$T(f) \in \{-2, -1, 0, 1, 2\}$$

5.0.1. Comment 1. The behavior of the iterates is a bit easier to see after the change of variables $n \mapsto n + 2$. Namely for

$$p\colon \mathbf{R} \to \mathbf{R}$$
$$\begin{aligned} p(n) &= q(n-2) + 2 = \big((n-2)^2 - 2\big) + 2 \\ &= (n-2)^2 \\ &= n + (n-1)(n-4) \end{aligned}$$

it is pretty obvious that

$$\begin{aligned} n < 0 \quad &\Rightarrow \quad p(n) > 4 \\ n > 4 \quad &\Rightarrow \quad p(n) > n \end{aligned}$$

Hence the $p^{\circ k}(n)$ are bounded only for $0 \leq n \leq 4$. This gives the restriction

$$T(f) + 2 \in \{0, 1, 2, 3, 4\}$$

Note that in the context of "two roots" one has

$$m = T(f) + 2$$

cf. Section 2.5.1 and (2.18).

5.0.2. Comment 2. Let us also try for

$$T(1-f) = 2 - T(f)$$

The corresponding variable change (for q it is $n \mapsto 2-n$, for p it is $n \mapsto 4-n$) yields

$$\begin{aligned} r\colon \mathbf{R} &\to \mathbf{R} \\ r(n) &= 2 - q(2-n) = 2 - \big((2-n)^2 - 2\big) \\ r(n) &= 4 - p(4-n) = 4 - (4-n-2)^2 \\ &= 4 - (n-2)^2 = n(4-n) = 4n - n^2 \end{aligned}$$

This gives

$$T(1-f^2) = 4T(1-f) - T(1-f)^2 \tag{5.3}$$

The restriction for $T(f) \in \mathbf{Z}$ and f of finite order is

$$T(1-f) \in \{0,1,2,3,4\}$$

which is what we want anyway, cf. (2.18).

(5.4) Remark. We prefer (5.3) over (5.2) since it holds in any dimension for $f \in \mathrm{SL}_n(k)$ leaving a subspace of codimension ≤ 2 pointwise fixed.

5.0.3. Comment 3. The eigenvalues x, y of $f \in \mathrm{SL}_2(k)$ lie universally in the Laurent series ring

$$\mathbf{Z}[x,y]/(xy-1) = \mathbf{Z}[x^{\pm 1}]$$

with $T = x + y = x + x^{-1}$ corresponding to the trace of f. (5.2) is immediate:

$$(x^2 + x^{-2}) = (x + x^{-1})^2 - 2$$

5.0.4. Comment 4. (5.2) reflects the classical formula

$$2\cos 2\varphi = (2\cos\varphi)^2 - 2 \tag{5.5}$$

For (5.5) the iteration argument yields, well, $|\cos\varphi| \leq 1$.

Indeed, over $\mathbf{Z}[2^{-1}, i]$ one has

$$\mathbf{Z}[2^{-1}, i][x,y]/(xy-1) = \mathbf{Z}[2^{-1}, i][\cos, \sin]/(\cos^2 + \sin^2 - 1)$$

with $x, y = \cos \pm i \sin$ and $T = x + y = 2\cos$. This way the restriction $-2 \leq T \leq 2$ corresponds to $|\cos| \leq 1$.

5.0.5. Comment 5 (dynamical systems). Pushing the excursion further, we mention briefly the topic of dynamical systems and iteration of rational functions.

The complex selfmap

$$\begin{aligned} \mathbf{C} &\to \mathbf{C} \\ z &\mapsto z^2 - 2 \end{aligned}$$

is a very special example. Its Julia set is the interval $[-2, 2]$ (Beardon 1991 [1, p. 9, p. 14, p. 18]).

(So it is very hard to find fractal images of the Julia set of $z^2 - 2$. ☺)

Not surprisingly, $z^2 - 2$ is related to Chebyshev polynomials. Note that Beardon [1, p. 10] has two arguments to control iterations, one of them is using cosh, sinh.

For the record: The conjugates

$$\begin{aligned} \mathbf{C} &\to \mathbf{C} \\ z &\mapsto (z-2)^2 \\ z &\mapsto 4z - z^2 \end{aligned}$$

have Julia set $[0, 4]$.

(All this brings back memories to my talk "Sullivansche Lösung II" on the workshop Chaos in dynamischen Systemen, Arbeitsgemeinschaft, Oberwolfach, 1985.)

References: Sullivan 1985 [18], Beardon 1991 [1], Milnor 1993 [11], Milnor 2006 (1990) [12].

We conclude with some explicit computations.

(5.6) Lemma. *The selfmap $z \mapsto z^2 + c$ has as fixed points and points of period 2:*

$$\begin{aligned} z_{1,2} &= \frac{1 \pm \sqrt{1-4c}}{2} \\ z_{3,4} &= \frac{-1 \pm \sqrt{-3-4c}}{2} \end{aligned}$$

Proof: The fixed points are the zeros of

$$z^2 - z + c = 0$$

The points of period $1, 2$ are the zeros of

$$\begin{aligned} (z^2+c)^2 + c - z &= (z^2+c)^2 - z^2 + (z^2 + c - z) \\ &= (z^2 + c + z + 1)(z^2 + c - z) \end{aligned}$$

□

(5.7) Corollary. *The selfmap $z \mapsto z^2 - 2$ (which has Julia set $[-2, 2]$) has as fixed points and points of period 2:*

$$\begin{aligned} z_{1,2} &= 2, -1 \\ z_{3,4} &= \frac{-1 \pm \sqrt{5}}{2} = -1 + \{\eta, \overline{\eta}\} \end{aligned}$$

Here η denotes the golden ratio with conjugate $\overline{\eta} = 1 - \eta = -\eta^{-1}$:

$$\eta^2 = \eta + 1, \qquad \eta = \frac{1+\sqrt{5}}{2} = 1.618\ldots, \qquad \overline{\eta} = \frac{1-\sqrt{5}}{2} = -0.618\ldots$$

(5.8) Corollary. *The selfmap*

$$z \mapsto (z-2)^2$$

has as fixed points and points of period 2*:*

$$F_{1,2} = 4, 1$$

$$P_{1,2} = \frac{3 \pm \sqrt{5}}{2} = 1 + \{\eta, \overline{\eta}\}$$

where

$$P_1 = \frac{3+\sqrt{5}}{2} = 2.618\ldots, \qquad P_2 = \frac{3-\sqrt{5}}{2} = 0.381\ldots$$

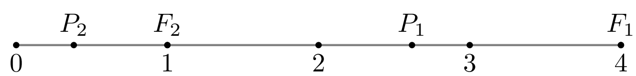
Summary:

$$[0,4] \to [0,4] \qquad \text{(Julia set)}$$

$$3 \mapsto 1 \mapsto 1$$

$$2 \mapsto 0 \mapsto 4 \mapsto 4$$

$$1+\eta \mapsto 1+\overline{\eta} \mapsto 1+\eta$$



5.0.6. Comment 6 (Ω again). Recall

$$m(a,b) = 4 - \text{trace}(1 - s_a s_b) \in \Omega = \{0,1,2,3,4\}$$

from Lemma (2.14). Hence

$$\Omega \to \Omega$$

$$m \mapsto (m-2)^2$$

corresponds to $s_a s_b \mapsto (s_a s_b)^2$. Cf. Section 2.5.1, Section 2.6.7.

§6. General reflections and rotations

This text rather belongs to an expansion of [14].

In the following, we consider finitely generated locally free modules over some ring k.

The exterior k-power of $f \in \mathrm{Hom}(V, W)$ is the homomorphism

$$\Lambda^k f \in \mathrm{Hom}(\Lambda^k V, \Lambda^k W)$$
$$\Lambda^k f(v_1 \wedge \ldots \wedge v_k) = f(v_1) \wedge \ldots \wedge f(v_k)$$

The following Lemma is a warm up. It emphasizes that we want to work over any ring (or scheme).

(6.1) Lemma. *Let* $t \in \mathrm{End}(V)$*. If*

$$\Lambda^2 t = 0$$

then

$$t^2 = T(t)t$$

Proof: Locally $V \simeq k^n$. For $t \in M_n(k)$ one has

$$\begin{aligned}\left(t^2 - T(t)t\right)_{ij} &= \sum_k t_{ik}t_{kj} - \sum_k t_{kk}t_{ij} \\ &= \sum_k (t_{ik}t_{kj} - t_{kk}t_{ij}) = \sum_k \Lambda^2(t)_{kj,ik}\end{aligned}$$

□

6.1. Reflections.

As noted in Lemma (2.5), over a field with char $\neq 2$ an endomorphism f is a reflection if and only if $t = 1 - f$ has the properties

$$\operatorname{rank} t = 1$$
$$\operatorname{trace} t = 2$$

In general, over any ring k (or any scheme), I like to define a (possibly degenerate) reflection as follows.

(6.2) Definition. An endomorphism $f \in \mathrm{End}(V)$ is called a *general reflection* if, with $t = 1 - f$,

$$\Lambda^2 t = 0$$
$$T(t) = 2$$

Note that Lemma (6.1) yields

$$f^2 = 1$$

Definition (6.2) yields a closed subscheme of the scheme of endomorphisms of the module V. If 2 is invertible in k, one necessarily has $\operatorname{rank} t = 1$, so one gets the standard definition of reflections. In general, one may call the open subscheme $t \neq 0$ (=complement of $t = 0$, same as $\operatorname{rank} t = 1$) the scheme of non-degenerate reflections/transvections.

Examples for $k = \mathbf{Z}$ (cf. Remark (2.3.2)):

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \qquad t_A = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$$

$$B = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \qquad t_B = \begin{pmatrix} 2 & -1 \\ 0 & 0 \end{pmatrix}$$

The reflection A is not non-degenerate while B is non-degenerate.

6.2. Rotations. Here is a sketch for a "dimension-free" setup for rotations.

Elements in $\mathrm{SL}_2(k)$ can be considered as (possibly degenerate) rotations, as they leave in the generic case a non-degenerate quadratic form invariant (see Section 2.6.11).

Let $f \in \mathrm{GL}_2(k)$ and put $t = 1 - f$. One finds that the condition

$$\det(f) = 1$$

is equivalent to

$$Q(t) = T(t)$$

where T is the trace and Q is the second coefficient of the characteristic polynomial:

$$Q(t) = T(\Lambda^2 t)$$

$$2Q(t) = T(t)^2 - T(t^2)$$

So one may think of an endomorphism $f \in \mathrm{End}(V)$ (with arbitrary rank of V and over any base ring or scheme) satisfying (with $t = 1 - f$).

$$\Lambda^3 t = 0$$

$$Q(t) = T(t)$$

as a sort of general rotation. For these one finds that the powers f^k have the same property. Moreover, (5.3) holds.

(Expanding this material should better be done in a separate paper.)

CHAPTER IV

Unordered snippets

This “chapter” contains what its title says. Currently there is nothing here.

Bibliography

[1] A. F. Beardon, *Iteration of rational functions*, Graduate Texts in Mathematics, vol. 132, Springer-Verlag, New York, 1991, Complex analytic dynamical systems. MR 1128089 29

[2] A. Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991. MR 1102012 12

[3] N. Bourbaki, *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines*, Actualités Scientifiques et Industrielles [Current Scientific and Industrial Topics], No. 1337, Hermann, Paris, 1968. MR 240238 11, 12, 15, 18, 35

[4] N. Bourbaki, *Lie groups and Lie algebras. Chapters 4–6*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 2002, Translated from the 1968 French original by Andrew Pressley [3]. MR 1890629 11, 12, 15

[5] I. N. Bronstein and K. A. Semendjajew, *Taschenbuch der Mathematik: für Ingenieure und Studenten der technischen Hochschulen*, B. G. Teubner Verlagsgesellschaft, Leipzig, 1958. MR 93476 20

[6] M. Demazure and A. Grothendieck (eds.), *Schémas en groupes. II: Groupes de type multiplicatif, et structure des schémas en groupes généraux*, Lecture Notes in Mathematics, Vol. 152, Springer-Verlag, Berlin-New York, 1970, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3), Dirigé par M. Demazure et A. Grothendieck. MR 274459 12

[7] W. Fulton and J. Harris, *Representation theory*, Graduate Texts in Mathematics, vol. 129, Springer-Verlag, New York, 1991, A first course, Readings in Mathematics. MR 1153249 12

[8] S. Garibaldi, A. Merkurjev, and J.-P. Serre, *Cohomological invariants in Galois cohomology*, University Lecture Series, vol. 28, American Mathematical Society, Providence, RI, 2003. MR 1999383 20

[9] J. E. Humphreys, *Linear algebraic groups*, Graduate Texts in Mathematics, No. 21, Springer-Verlag, New York-Heidelberg, 1975. MR 396773 12

[10] ______, *Reflection groups and Coxeter groups*, Cambridge Studies in Advanced Mathematics, vol. 29, Cambridge University Press, Cambridge, 1990. MR 1066460 12

[11] J. Milnor, *Geometry and dynamics of quadratic rational maps*, Experiment. Math. **2** (1993), no. 1, 37–83, With an appendix by the author and Lei Tan. MR 1246482 29

[12] ______, *Dynamics in one complex variable*, third ed., Annals of Mathematics Studies, vol. 160, Princeton University Press, Princeton, NJ, 2006. MR 2193309 29

[13] M. Rost, *Notes on root systems (two roots)*, Preprint, September 2024, `www.math.uni-bielefeld.de/~rost/hopf.html` [pdf]. 5

[14] ______, *On the adjunct of an endomorphism*, Preprint, 2017, `www.math.uni-bielefeld.de/~rost/exterior.html` [pdf]. 31

[15] J.-P. Serre, *Complex semisimple Lie algebras*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2001, Translated from the French by G. A. Jones, Reprint of the 1987 edition. MR 1808366 11, 12, 13, 15, 18, 19, 20

[16] T. A. Springer, *Reductive groups*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, RI, 1979, pp. 3–27. MR 546587 12

[17] ______, *Linear algebraic groups*, second ed., Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 2009. MR 2458469 12

[18] D. Sullivan, *Quasiconformal homeomorphisms and dynamics. I. Solution of the Fatou-Julia problem on wandering domains*, Ann. of Math. (2) **122** (1985), no. 3, 401–418. MR 819553 29

[19] J. Tits, *Normalisateurs de tores. I. Groupes de Coxeter étendus*, J. Algebra **4** (1966), 96–116. MR 206117 12

[20] ______, *Sur les constantes de structure et le théorème d'existence des algèbres de Lie semi-simples*, Inst. Hautes Études Sci. Publ. Math. (1966), no. 31, 21–58. MR 214638 5, 12, 20

[21] E. Zeidler (ed.), *Springer-Taschenbuch der Mathematik*, 3rd revised and expanded ed., Heidelberg: Springer Spektrum, 2013 (German), Founded by I.N. Bronstein und K.A. Semendjaew, Zbl 1276.00005. 20