Reductive Algebraic Groups

Benjamin Andersson & Victor Groth

Last updated February 2026

Contents

Please send any typos/mistakes to *benjamin35813@gmail.com*.

Chapter 1

Lecture 1

1.0.1 Background

- For background, see [1].
- For algebraic geometry, see e.g. [3, Chap. I].
- Beginning of [6].
- [2].
- [5]. Varieties are treated in chapter 1, algebraic curves in chapter 2, and elliptic curves in chapter 3.

1.0.2 What are reductive groups?

The prototypical example: $\mathsf{GL}(n)$. One may ask, what is $\mathsf{GL}(n)$? One answer is " The group of invertible $n \times n$ matrices".

$$\begin{aligned} F \text{ field} \longmapsto\ & \text{group}\, \mathsf{GL}(n, F) \\ &= n \times n \text{ invertible matrices with entries in the field } F. \end{aligned}$$

Similarly, we have

$$\begin{aligned} R \text{ commutative ring with } 1 \longmapsto\ & \text{group }\ \mathsf{GL}(n, R) \\ &= n \times n \text{ invertible matrices with entries in } R. \end{aligned}$$

Definition

Definition 1.0.1. Recall that $M_n(R)$ is the *ring* of all $n \times n$ matrices with elements from R, where R is a ring with 1.

Definition

Definition 1.0.2. If A is a not necessarily commuative ring with 1, then we define the **group of units of** A as

$$A^\times = \{a \in A \mid \exists b \in A \text{ s.t. } ab = ba = 1\}.$$

Example 1.0.3 **($M_n(R)^\times$).** Let $A = M_n(R)$ for a commutative ring R with 1. Then

$$A^\times = \mathsf{GL}(n, R).$$

We can think of this as a "function" (see **functor** from **CRing** to **Grp**)

$$\Big\{\text{Commutative ring with } 1\Big\} \xrightarrow{\mathsf{GL}(n)} \Big\{\text{Groups}\Big\}.$$

We then have

$$\Big\{(R \to S) \text{ ring homomorphism}\Big\} \xrightarrow{\mathsf{GL}(n)} \Big\{\ \mathsf{GL}(n, R) \to \mathsf{GL}(n, S) \text{ group homomorphism}\Big\}.$$

Similarly, we have a **functor**

$$\Big\{\text{Commutative rings with } 1\Big\} \xrightarrow{M_n(-)} \Big\{\text{rings with } 1\Big\},$$

explicitly defined as $R \xmapsto{M_n(-)} M_n(R)$ on objects R in source category **CRing**. On morphisms (i.e. ring-homomorphisms) in **CRing** $\varphi : R \to S$ we have that $M_n(\varphi) : M_n(R) \to M_n(S)$.

Furthermore, we have a **unit functor**

$$\Big\{\text{Rings with } 1\Big\} \longrightarrow \Big\{\text{Groups}\Big\}$$

$$R \longmapsto R^\times$$

$$(R \to S) \longmapsto (R^\times \to S^\times)$$

If we let $(-)^\times$ be the unit functor, then we see that $\mathsf{GL}(n) = (-)^\times \circ M_n(-)$, explicitly as

$$R \xmapsto{M_n(-)} M_n(R) \xmapsto{(-)^\times} (M_n(R))^\times = \mathsf{GL}(n, R).$$

We have that $\mathsf{GL}(n)$ is given by <u>polynomial equations</u> (one equation is enough for $\mathsf{GL}(n)$). We have

$$\mathsf{GL}(n, R) = \text{solutions in some } R^N \quad \text{where } N = n^2 + 1,$$

of a polynomial equation with coefficients in R. One may ask; what is this equation? For a field F, we have that

$$\mathsf{GL}(n, F) = \{A \in M_n(F) \mid \det(A) \neq 0\}.$$

When R is instead a ring with 1, we define

$$\mathsf{GL}(n, R) = \{A \in M_n(R) \mid \det(A) \in R^\times\}.$$

Notice that if $A = (a_{ij})$ is of dimension $n \times n$, then $\det(A)$ is a polynomial equation of degree n in the entries a_{ij} of A. For the simplest non-trivial case, let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightsquigarrow \det(A) = ac - bd \in R[a, b, c, d].$$

To get from $\det(A) \neq 0$ to $f(x) = 0$, i.e. a polynomial equation, we add a variable t. Then we get

$$\mathsf{GL}(n, R) = \left\{ (\underbrace{(a_{ij})}_{\in R^{n^2}}, t) \in R^{n^2+1} \;\middle|\; \det((a_{ij}))t = 1 \right\},$$

where (a_{ij}) represents the matrix $A \in M_n(R)$.

We say that $\mathsf{GL}(n)$ is a **group functor**, and it's given by polynomial equations.

Roughly: An **algebraic group** is a *group functor* given by polynomial equations.

Example 1.0.4 (Algebraic group: $\mathsf{GL}(n)$)**.** $\mathsf{GL}(n)$ is an *algebraic group* that has the reductive property (to be defined later).

Example 1.0.5 ($\mathsf{SL}(n)$)**.** We have

$$\mathsf{SL}(n, R) = \{A \in M_n(R) \mid \det(A) - 1 = 0\}.$$

Definition

Definition 1.0.6. Let R be a ring with 1, and let $A \in M_n(R)$ such that ${}^tA = A$. Then we say that A is a **symmetric matrix**.

Definition

Definition 1.0.7. Let R be a ring with 1, and let $A \in M_n(R)$ such that ${}^tA = -A$. Then we call A an **antisymmetric matrix**.

Remark 1.0.8. In 1.0.6, ${}^tA$ denotes the **transpose** of A.

Example 1.0.9 ($G^{\mathcal{J}}(R)$)**.** Let $\mathcal{J} \in \mathsf{GL}(n, R)$ be either a symmetric matrix (1.0.6) or an antisymmetric matrix (1.0.7). Then

$$G^{\mathcal{J}}(R) = \{A \in M_n(R) \mid {}^tA\mathcal{J}A = \mathcal{J}\}.$$

The claim is then that this is a polynomial equation in n^2 variables (each of the n^2 equations say, has the left hand side the i,j:th element of ${}^tA\mathcal{J}A$ [we know how to compute this from basic linear algebra] and the right hand side has the i,j:th element of $\mathcal{J}$).

With respect to example 1.0.9 we have the following two definitions.

Definition

Definition 1.0.10. If $\mathcal{J}$ in 1.0.9 is symmetric (1.0.6), then $G^{\mathcal{J}}$ is called the **orthogonal group of** $\mathcal{J}$.

Definition

Definition 1.0.11. If $\mathcal{J}$ in 1.0.9 is antisymmetric (1.0.7), $G^{\mathcal{J}}$ is called the **symplectic group** of $\mathcal{J}$.

Example 1.0.12 ($\mathcal{J} = I$)**.** Let $\mathcal{J} = I \in M_n(R)$, the identity matrix of dimension $n \times n$. Then

$$\begin{aligned} G^{\mathcal{J}}(R) &= G^I(R) \\ &= \{A \in M_n(R) \mid {}^tAA = I\}. \end{aligned}$$

Generally, $G^{\mathcal{J}}$ is a reductive algebraic group (for any $\mathcal{J}$ either symmetric or antisymmetric). To summarize; basic examples of reductive algebraic groups are $\mathsf{GL}(n), \mathsf{SL}(n)$ and $G^{\mathcal{J}}$ for $\mathcal{J}$ symmetric or antisymmetric. The last two are called the orthogonal (1.0.10) and symplectic groups (1.0.11).

Example 1.0.13 (The **Projective Linear Group**, $\mathsf{PGL}(n)$)**.** Let

$$\mathsf{PGL}(n) = \mathsf{GL}(n) \Big/ Z(\mathsf{GL}(n)),$$

where $Z(\mathsf{GL}(n)) = \{A \in \mathsf{GL}(n) \mid AB = BA, \forall B \in \mathsf{GL}(n)\}$ is the **center** of $\mathsf{GL}(n)$. Generally, for a commutative ring R with 1, we have that

$$\begin{aligned} \mathsf{PGL}(n, R) &= \mathsf{GL}(n, R) \Big/ Z(\mathsf{GL}(n, R)) \\ &= \mathsf{GL}(n, R) \Big/ R^{\times}. \end{aligned}$$

This follows from the fact that

$$Z(\mathsf{GL}(n, R)) = \{\lambda I \mid \lambda \in R^{\times}\},$$

and the right-hand side has a canonical isomorphism to $R^{\times}$ defined explicitly as $\lambda I \mapsto \lambda$. That $Z(\mathsf{GL}(n)) = \{\lambda I \mid \lambda \in R^{\times}\}$ follows from the following reasoning: Let $A \in \mathsf{GL}(n, R)$ be such that $AB = BA$ for all $B \in \mathsf{GL}(n, R)$. Then let I be the identity matrix, and let E_{ij} be the matrix in $M_n(R)$ with a zeroes everywhere except the i, j:th element, where $i \neq j$. Then notice that

$$\begin{aligned} \det(I + E_{ij}) &= \det(I) \\ &= 1. \end{aligned}$$

To see this, if we cofactor expand along the row i, we get $M_{ii} + M_{ij}$, where M_{ii}, M_{ij} are the two minorants corresponding to deleting row and column i, and deleting row i and column j respectively. We see that M_{ii} is the determinant of an $(n-1) \times (n-1)$ identity matrix, so is 1. For M_{ij}, when we come to the 1 at the spot i, j, we get a minor with a column that is all zeroes, corresponding to column i in the original matrix. This is because $i \neq j$, and we remove the only 1 at place i, i in column i of the original matrix (note that the "extra" 1 is in column $j \neq i$), leaving us with only zeroes in the "minor" column left. Therefore the columns are linearly dependent and so the determinant is 0. Therefore

$$\begin{aligned} \det(I + E_{ij}) &= M_{ii} + M_{ij} \\ &= 1, \end{aligned}$$

which implies that $I + E_{ij} \in \mathsf{GL}(n, R)$. So if A commutes with every matrix in $\mathsf{GL}(n, R)$, then we need $A(I + E_{ij}) = (I + E_{ij})A \rightsquigarrow A + AE_{ij} = A + E_{ij}A$. We need to find AE_{ij} and $E_{ij}A$.

We see that (with $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$)

$$AE_{ij} = \begin{pmatrix} 0 & \dots & a_{1i} & 0 & \dots & 0 \\ 0 & \dots & a_{2i} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & a_{ni} & 0 & \dots & 0 \end{pmatrix}$$

where ${}^{t}[a_{1i}, \dots, a_{ni}]$ is the j^{th} column of AE_{ij}.

Remark 1.0.14. Above is a little bit misleading since if $j = n$ then there are no columns after the column ${}^{t}[a_{1i}, \dots, a_{ni}]$; so take it as more of a helpful (but faulty) "pictorial" representation.

To summarize, AE_{ij} picks out column i and places it at column j in a matrix of dimension $n \times n$ with zeroes everywhere else.

We also see that

$$E_{ij}A = \begin{pmatrix} 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

where $[a_{j1}, \dots, a_{jn}]$ is placed at row i, so that $E_{ij}A$ picks out row j of A and places it at row i in a matrix with zeroes everywhere else except row j of A at row i.

Recall that we had $A + AE_{ij} = A + E_{ij}A \Leftrightarrow AE_{ij} = E_{ij}A$. But the only way this can happen is if $a_{ij} = 0$ for $i \neq j$, and $a_{ii} = a_{jj}$. Since i, j were arbitrary we find that $A = kI$. One then sees that we need $k \in R^\times$, since if $k \notin R^\times \Rightarrow k^n \notin R^\times \Rightarrow \det(kI) \notin R^\times \Rightarrow A = kI \notin \mathsf{GL}(n, R)$.

In relation to the example above, one might ask: Is $\mathsf{PGL}(n, R)$ defined by polynomial equations? The answer is yes. Similarly, one may define $\mathsf{PSL}(n, R) = \mathsf{SL}(n, R)/Z(\mathsf{SL}(n, R))$. Note that since $I + E_{ij}$ had determinant 1, one sees that $Z(\mathsf{SL}(n, R)) = \{\lambda I \mid \lambda^n = 1\}$ so that

$$\mathsf{PSL}(n, R) = \mathsf{SL}(n, R) \big/ \{\lambda I \mid \lambda^n = 1\}.$$

This is an example of a **group functor** not given by polynomial equations, in general. The *moral* is the following:

1. Quotients in algebraic geometry are *difficult*.
2. Many times do work and give new examples.

Reductive groups

A *rough* characterization of reductice groups, is as the smallest class of groups containing $\mathsf{GL}(n)$ and all the simple algebraic groups, that is *closed* under some natural operations.

Example 1.0.15. $\mathsf{GL}(n)$ reductive $\Rightarrow \mathsf{PGL}(n)$ reductive.

In this course, "reductive group" means "reductive *algebraic* group", unless otherwise stated. **But**, there are reductive Lie groups, and not every reductive Lie group is algebraic.

Definition

Definition 1.0.16 (Simple Algebraic Group)**.** An *algebraic group* is **simple** if it has no *infinite normal subgroups* (of dimension > 0;). We have $H \triangleleft G$ if $H(R) \triangleleft G(R)$ for all R (I presume R is a commutative ring with unity).

Remark 1.0.17. That H is **infinite** above means that there exists a ring R such that $H(R)$ is infinite.

Example 1.0.18 ($\mathsf{SL}(n)$)**.** Let μ_n be the n^{th} roots of unity. Then $\mu_n(\mathbb{C})$ is cyclic of degree n. We have that $\mu_n \subset \mathsf{SL}(n)$ is normal but finite, where

$$\mu_n = \mathcal{Z}(x^n - 1).$$

On the other hand, $\mathsf{SL}(n, \mathbb{C})$ is not a simple group, but still $\mathsf{SL}(n)$ is a simple algebraic group.

Rough definition (cf. 1.0.30)

Definition 1.0.19 (Group Scheme)**.** A **group scheme** is a *group functor* (target **Grp**) defined by polynomial equations.

Example 1.0.20. μ_n is a group scheme that is not an algebraic group over a field of characteristic dividing n.

We have the following inclusions

$$\text{reductive algebraic groups} \subset \text{algebraic groups} \subset \text{affine group schemes} \subset \text{group functors}.$$

Theorem

Theorem 1.0.21. *Let $\Bbbk$ be an algebraically closed field. Then, up to finite center, the simple (1.0.16) algebraic groups are precisely given by the four infinite families*

$$\mathsf{A_n}, \quad \text{for } n \geqslant 1$$

and

$$\mathsf{B}_n, \mathsf{C}_n, \mathsf{D}_n, \quad \text{for } n \geqslant 3$$

and five exceptional *families* $\mathsf{G}_2, \mathsf{F}_4, \mathsf{E}_6, \mathsf{E}_7, \mathsf{E}_8$ *with the isomorphisms*

$$\mathsf{A}_1 \cong \mathsf{B}_1 \cong \mathsf{C}_1 \cong \mathsf{D}_1,$$

$$\mathsf{B}_2 \cong \mathsf{C}_2,$$

and

$$\mathsf{A}_3 \cong \mathsf{D}_3.$$

Remark 1.0.22. The phrase "up to finite center" in 1.0.21 means (as far as I can tell) that if G, H are simple algebraic groups such that $G/Z(G) \cong H/Z(H) \Rightarrow G$ and H are of the same type, i.e. are classified by the same type of family from above. A simple algebraic (reductive) connected group seem to always have finite center, why this assumption is built in (i.e. this is why we say *finite* center).

Example 1.0.23 ($\mathsf{SL}(n-1)$.)**.** $\mathsf{SL}(n-1)$ is of type A_{n-1}.

Example 1.0.24 ($\mathsf{SO}(2n)$)**.** $\mathsf{SO}(2n)$ is of type D_n.

Example 1.0.25 ($\mathsf{SO}(2n+1)$)**.** $\mathsf{SO}(2n+1)$ is of type B_n.

Example 1.0.26 ($\mathsf{Sp}(2n)$)**.** $\mathsf{Sp}(2n)$ is of type C_n (where Sp we can think of as the symplectic group structure).

Example 1.0.27. $\mathsf{G}_2 =$ automorphisms of octonions.

Example 1.0.28 ($\mathsf{SO}(m)$)**.**

$$\mathsf{SO}(m) = \mathsf{SL}(m) \cap \mathsf{O}(m),$$

where $\mathsf{O}(m) = G^I$ or $\mathsf{O}(m) = G^{\mathcal{J}}$ for any symmetric + invertible $\mathcal{J}$. Furthermore, we have that $G^I \cong G^{\mathcal{J}}$ over any algebraically closed field $\Bbbk$ whenever $\mathcal{J}$ is symmetric + invertible, i.e.

1. $\exists \mathcal{J}^{-1}$ (invertible).
2. ${}^t\mathcal{J} = \mathcal{J}$ (symmetric).

Example 1.0.29 (More about $\mathsf{Sp}(2m)$)**.** We have that

$$G^{\mathcal{J}}(2m) \cong \mathsf{Sp}(2m),$$

for $\mathcal{J}$ such that:

1. $\exists \mathcal{J}^{-1}$ (invertible).
2. ${}^t\mathcal{J} = -\mathcal{J}$ (anti-symmetric).

Definition

Definition 1.0.30 (Group scheme)**.** A **group scheme over a commutative ring** R is a *group functor* G defined by polynomial equations with coefficients in R,

$$\mathbf{CAlg}_R \xrightarrow{G} \mathbf{Grp}$$

defined by

$$S \overset{G}{\longmapsto} G(S).$$

Remark 1.0.31. $\mathbf{CAlg}_R$ in 1.0.30 is a subcategory of $\mathbf{Alg}_R$ (the category of R-algebras), consisting of objects as commutative R-algebras and morphisms as R-algebra homomorphisms, i.e. ring homomorphisms between R-algebras which *respects the R-module structure*: If A, B are R-algebras and $f : A \to B$ is an R-algebra homomorphism then f is a ring homomorphism such that

$$f(r \cdot a) = r \cdot f(a), \quad \forall r \in R, \forall a \in A.$$

Chapter 2

Lecture 2

Definition

Definition 2.0.1. A **crystallographic root system** is a *triple* $(V, (\,,\,), \Phi)$ s.t.

- V is a $\mathbb{Q}$-vector space (v.s.).
- $(\,,\,)$ is a *symmetric* bilinear form. By symmetric, we mean that $(u, v) = (v, u)$, for all $u, v \in V$, and so that $(\,,\,)$ is *positive-definite* (in the sense of $(v, v) > 0$ for all $v \in V \setminus \{0\}$) on $V_{\mathbb{R}} := V \otimes_{\mathbb{Q}} \mathbb{R}$.
  - Think of $(\,,\,)$ as the *dot product* on $\mathbb{R}^n$, i.e.

$$u \cdot v = \sum u_i v_i.$$

- $\Phi \subseteq V \setminus \{0\}$ is a *finite* subset. In relation to Φ, we define, for all $\alpha \in \Phi$

$$\alpha^\vee = \frac{2 \cdot \alpha}{(\alpha, \alpha)}$$

  and $S_\alpha : V \to V$ explicitly defined by $x \mapsto x - (x, \alpha^\vee)\alpha$.

In relation to 2.0.1, we have the following <u>axioms</u>:

1. $V = \operatorname{span}_{\mathbb{Q}} \Phi$.
2. For all $\alpha \in \Phi$, we have $S_\alpha(\Phi) \subseteq \Phi$.
3. For all $\alpha, \beta \in \Phi$, we have $(\alpha, \beta^\vee) \in \mathbb{Z}$.

Definition

Definition 2.0.2. Elements of Φ in 2.0.1 are called the **roots**.

Definition

Definition 2.0.3. For $\alpha \in \Phi$, $\alpha^\vee$ is called the **coroot of the root of** α (cf. 2.0.2).

Definition

Definition 2.0.4.
$$\Phi^\vee := \{\alpha^\vee \mid \alpha \in \Phi\}$$
is the set of **coroots of the roots** (2.0.2).

We say that S_α in 2.0.1 is the **root reflection** of/in α.

We have that

$$\begin{aligned}
S_\alpha(\alpha) &= \alpha - (\alpha, \alpha^\vee)\alpha \\
&= \alpha(1 - (\alpha, \alpha^\vee)) \\
&= \alpha\left(1 - \left(\alpha, \frac{2 \cdot \alpha}{(\alpha, \alpha)}\right)\right) \\
&= \alpha\left(1 - \frac{2}{(\alpha, \alpha)}(\alpha, \alpha)\right) \\
&= -\alpha.
\end{aligned}$$

Since axiom 2 gives us that $S_\alpha(\Phi) \subseteq \Phi$, we have that if $\alpha \in \Phi$ then $-\alpha \in \Phi$, and if $-\alpha \in \Phi$, then $\alpha \in \Phi$. That is,
$$\alpha \in \Phi \Leftrightarrow -\alpha \in \Phi.$$

Then it follows that

$$\begin{aligned}
(S_\alpha \circ S_\alpha)(x) &= S_\alpha(x - (x, \alpha^\vee)\alpha) \\
&= (x - (x, \alpha^\vee)\alpha) - ((x - (x, \alpha^\vee)\alpha, \alpha^\vee)\alpha \\
&= S_\alpha(x) - (x, \alpha^\vee)\alpha + ((x, \alpha^\vee)\alpha, \alpha^\vee)\alpha \\
&= S_\alpha(x) - (x, \alpha^\vee)\alpha + (x, \alpha^\vee)(\alpha, \alpha^\vee)\alpha \\
&= S_\alpha(x) - (x, \alpha^\vee)(\alpha - (\alpha, \alpha^\vee)\alpha) \\
&= S_\alpha(x) - (x, \alpha^\vee)\underbrace{S_\alpha(\alpha)}_{=-\alpha} \\
&= S_\alpha(x) + (x, \alpha^\vee)\alpha \\
&= x - (x, \alpha^\vee)\alpha + (x, \alpha^\vee)\alpha \\
&= x,
\end{aligned}$$

so that $S_\alpha \circ S_\alpha = \mathrm{id}_V$.

Definition

Definition 2.0.5. We define

$$\alpha^{\vee,\perp} := \{v \in V \mid (v, \alpha^\vee) = 0\}$$

which is a *hyperplane* (codimension one subspace).

We note that for $v \in \alpha^{\vee,\perp}$, we have

$$\begin{aligned}
S_\alpha(v) &= v - \underbrace{(v, \alpha^\vee)}_{=0}\alpha \\
&= v.
\end{aligned}$$

If we think of S_α as a linear transformation $V \to V$ (we can think of representing it in some basis B), then we see that $\alpha^{\vee,\perp}$ is a 1-eigenspace of S_α, which we can call V_1. On the other hand, for

$$\operatorname{span}(\alpha) = \{\zeta\alpha \mid \zeta \in \mathbb{Q}\}$$

we have that

$$\begin{aligned} S_\alpha(\zeta\alpha) &= (\zeta\alpha - (\zeta\alpha, \alpha^\vee)\alpha \\ &= (\zeta\alpha - \zeta(\alpha, \alpha^\vee)\alpha) \\ &= \zeta(\alpha - (\alpha, \alpha^\vee)\alpha) \\ &= \zeta \underbrace{S_\alpha(\alpha)}_{=-1} \\ &= -\zeta\alpha, \end{aligned}$$

for $\zeta \in \mathbb{Q}$, so that $\operatorname{span}(\alpha) = V_{-1}$ is the (-1)-eigenspace.

Definition

Definition 2.0.6. We call $A \in \mathsf{GL}(V)$ a **reflection** if its 1-eigenspace has codimension 1, and its (-1)-eigenspace has dimension $1 \Leftrightarrow A$ is *conjugate* to $\operatorname{diag}(1, \ldots, 1, -1)$, in the sense that $\exists B \in \mathsf{GL}(V)$ such that $BAB^{-1} = \operatorname{diag}(1, \ldots, 1, -1)$.

Example 2.0.7 (Type A_{n-1})**.** Let

$$\begin{aligned} V &= \mathbb{Q}_0^n \\ &= \{a \in \mathbb{Q}^n \mid \sum_{i=1}^n a_i = 0\} \end{aligned}$$

so that $\dim(V) = n - 1$, where we are using the dot-product as our symmetric bilinear form $(,)$.

Furthermore, let $\Phi = \left\{e_i - e_j \mid {}^{1\leq i,j\leq n}_{i\neq j}\right\}$, where e.g. $e_1 = (1, 0, 0, \ldots, 0)$ and $e_2 = (0, 1, 0, 0, \ldots, 0)$.

<u>Claim</u>: $(V, (,), \Phi)$ in 2.0.7 is a crystallographic root system (2.0.1).

<u>Exercise</u>: $\Delta = \{e_1 - e_2, e_2 - e_3, \ldots, e_{n-1} - e_n\}$ is a basis of $\mathbb{Q}_0^n$, but does *not* generate $\mathbb{Z}_0^n$ over $\mathbb{Z}$.

Proof. (Exercise) We first show that Δ is a set of $n - 1$ linearly independent vectors:

Assume that

$$\begin{aligned} \sum_{i=1}^{n-1} \alpha_i(e_i - e_{i+1}) &= \alpha_1(e_1 - e_2) + \ldots + \alpha_{n-1}(e_{n-1} - e_n) \\ &= 0. \end{aligned} \tag{2.0.1}$$

By reorganizing (2.0.1) we find that

$$\alpha_1 e_1 + (\alpha_2 - \alpha_1)e_2 + \ldots + (\alpha_{n-1} - \alpha_{n-2})e_{n-1} - \alpha_{n-1}e_n = 0.$$

Since the e_i are linearly independent, we see that $\alpha_1 = 0$, but then $\alpha_2 = 0$ etc., i.e. so that $\alpha_i = 0$ for all $1 \leq i \leq n - 1$. Therefore Δ is linearly independent of dimension $n - 1$. There is a certain type of "telescoping" reasoning going on here, as we have just seen.

We also want to show that Δ *spans* $\mathbb{Q}_0^n$. So assume that there is some vector $a = (a_1, \dots, a_n) \in \mathbb{Q}_0^n$, i.e so that $\sum a_i = 0$. We want to find α_i for $1 \le i \le n-1$ such that $\sum \alpha_i(e_i - e_{i+1}) = a$.

We get a system of equations

$$\begin{aligned}
\alpha_1 &= a_1 \\
(\alpha_2 - \alpha_1) &= a_2 \\
&\vdots \\
(\alpha_{n-1} - \alpha_{n-2}) &= a_{n-1} \\
-\alpha_{n-1} &= a_n.
\end{aligned} \tag{2.0.2}$$

α_1 is obvious, and then

$$\begin{aligned}
\alpha_2 &= a_2 + \alpha_1 \\
&= a_2 + a_1.
\end{aligned}$$

For α_3, we have

$$\begin{aligned}
\alpha_3 - \alpha_2 &= a_3 \\
\Leftrightarrow \alpha_3 &= a_3 + \alpha_2 \\
&= a_3 + a_2 + a_1.
\end{aligned}$$

Following through on this argument up to $n-1$, it follows that $\alpha_i = a_i + a_{i-1} + \ldots + a_1$ for $i = \{1, \dots, n-1\}$, which solves the system of equations in (2.0.2).

Furthermore, we want to show that Δ *does not* generate $\mathbb{Z}_0^n$ over $\mathbb{Z}$. This means that there is some $b = (b_1, \dots, b_n) \in \mathbb{Z}_0^n$ such that $\sum b_i = 0$, so that there is no set of coefficients $\beta_1, \dots, \beta_{n-1} \in \mathbb{Z}$ such that

$$\sum_{i=1}^{n-1} \beta_i(e_i - e_{i+1}).$$

□

We note that if $\alpha = e_i - e_j$ for $i \neq j$, then

$$\begin{aligned}
(\alpha, \alpha) &= (e_i - e_j, e_i - e_j) \\
&= 2.
\end{aligned}$$

Therefore,

$$\begin{aligned}
(\alpha, \alpha^\vee) &= \frac{2 \cdot \alpha}{(\alpha, \alpha)} \\
&= \alpha.
\end{aligned}$$

We have

$$S_\alpha(x) = x - (x, \alpha^\vee)\alpha$$

We see that

$$\begin{aligned}
S_\alpha(x) &= x - (x, \alpha^\vee)\alpha \\
&= (x_1, \ldots, x_n) - (x, \alpha)\alpha \\
&= (x_1, \ldots, x_n) - (x, (e_i - e_j))(e_i - e_j) \\
&= (x_1, \ldots, x_n) - (x_i - x_j)(e_i - e_j) \\
&= (x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) - x_i e_i + x_i e_j + x_j e_i - x_j e_j \\
&= (x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n).
\end{aligned} \tag{2.0.3}$$

where we have used the definition of $(,)$. Note that originally we see $x = (x_1, \ldots, x_n)$ as a vector in $\mathbb{Q}^n$, but later on we view $(x_i - x_j)$ as a scalar in $\mathbb{Q}$. From (2.0.3) we see that S_α for $\alpha = e_i - e_j$ acts on $x \in \mathbb{Q}^n$ by permuting the arguments in position i and j. S_α leaves the other arguments in x *unchanged*, that is:

$$\begin{aligned}
x_i &\xmapsto{S_\alpha} x_j \\
x_j &\xmapsto{S_\alpha} x_i \\
x_r &\xmapsto{S_\alpha} x_r \qquad (r \neq i, j).
\end{aligned}$$

That is, we can identify S_α with a tranposition $\tau = (i\ j) \in S_n$ of its arguments.

Let $x = (e_r - e_s)$. Then we see that

$$\begin{aligned}
S_\alpha(x) &= S_{e_i - e_j}(e_r - e_{r+1}) \\
&= (e_r - e_{r+1}) - (e_r - e_{r+1}, e_i - e_j)(e_i - e_j) \\
&= e_{\tau(r)} - e_{\tau(s)}
\end{aligned}$$

Therefore, we conclude that $S_\alpha(\Phi) \subseteq \Phi$.

Lastly, we want to check that the last axiom hold, i.e. that for $\alpha, \beta \in \Phi$, we have that $(\alpha, \beta^\vee) \in \mathbb{Z}$. But this follows from the following fact:

We noted earlier that $\beta^\vee = \beta$. So if $\alpha = \beta$ then

$$\begin{aligned}
(\alpha, \beta^\vee) &= (\alpha, \beta) \\
&= (\alpha, \alpha) \\
&= 2
\end{aligned}$$

where we showed the last equality earlier.

Assume that $\alpha = e_i - e_j$ and that

$$\begin{aligned}
\beta^\vee &= \beta \\
&= e_r - e_s.
\end{aligned}$$

Then we have

$$(e_i - e_j, e_r - e_s)$$

If $i \neq r$ but $j = s$ we get 1, and similarly when $i = r$ but $j \neq s$. If $j = r$ and $i = s$ then we get -2. If $j = r$ but $i \neq s$ we get -1, and similarly we get -1 if $j \neq r$ but $i = s$.

We conclude that $(\alpha, \beta^\vee) \in \{-2, 1, 0, 1, 2\} \subseteq \mathbb{Z}$.

Therefore, $(\mathbb{Q}_0^n, (,), \Phi)$ is a crystallographic root system (2.0.1).

Remark 2.0.8. Note that we showed in the exercise that the subset $\Delta = \{e_1 - e_2, \ldots, e_{n-1} - e_n\} \subseteq \Phi$ spans $\mathbb{Q}_0^n$ over $\mathbb{Q}$, so that certainly Φ spans $\mathbb{Q}_0^n$ over $\mathbb{Q}$.

Definition

Definition 2.0.9. For a general root system $(V, (\,,\,), \Phi)$, we have that

$$\mathcal{W} = \langle S_\alpha \mid \alpha \in \Phi \rangle$$

is a *group*, generated by S_α for $\alpha \in \Phi$, called the **Weyl Group** of Φ. The group-operation is *composition* of reflections S_α.

We can view $\mathcal{W}$ as "sitting inside" $\mathsf{GL}(V)$ ($\mathcal{W} \subset \mathsf{GL}(V)$), where we know that for V finite-dimensional vector space, we have $\mathsf{GL}(V) \cong \mathsf{GL}(n, \Bbbk)$ where $\Bbbk$ is the field over which V is defined, as a v.s, and $n = \dim_{\Bbbk} V$.

Recall that $\mathsf{GL}(V) = \{A : V \to V \mid A \text{ is linear } + \text{ invertible}\}$, i.e. the set of *linear automorphisms* of V.

Furthermore, we have that $\mathcal{W} \subseteq O(V, (\,,\,)) \subset \mathsf{GL}(V)$ where $O(V, (\,,\,)) = \{g \in \mathsf{GL}(V) \mid (gv, gw) = (v, w), \forall v, w \in V\}$.

Remark 2.0.10. $\mathcal{W}(A_{n-1}) \cong S_n$; recall our earlier example with $S_\alpha \leftrightarrow \tau = (i\ j) \in S_n$.

Definition

Definition 2.0.11. Let Γ be a group. A (finite-dimensional) **representation of** Γ is a group-homomorphism $f : \Gamma \to \mathsf{GL}(n, \Bbbk)$ for some $n \in \mathbb{Z}_{\geq 1}$ and some field $\Bbbk$.

If $(V, (\,,\,), \Phi)$ is a root system, then there is a natural representation $\mathcal{W} \to \mathsf{GL}(V)$ where $\mathcal{W}$ as before is the weyl-group of the root-system $(V, (\,,\,), \Phi)$.

Remark 2.0.12. By *natural* here, we mean that since $\mathcal{W} \subseteq \mathsf{GL}(V)$, we see that the inclusion $\iota : \mathcal{W} \hookrightarrow \mathsf{GL}(V)$ is a representation.

Definition

Definition 2.0.13. A representation (V, ρ) of Γ is **reducible** if there exists a *non-zero, proper* subspace $U \subset V$ such that $\rho(\gamma)(U) \subseteq U$ for all $\gamma \in \Gamma$.

Definition

Definition 2.0.14. If a representation (V, ρ) of a group Γ is *not reducible* (cf. 2.0.13), we call it an **irreducible representation**.

Definition

Definition 2.0.15. A root system $(V, (\,,\,), \Phi)$ is **reduced** if $\lambda\alpha \in \Phi \Rightarrow \lambda = \pm 1$ for all roots (2.0.2) $\alpha \in \Phi$, and all $\lambda \in \mathbb{Q}$.

Definition

Definition 2.0.16. If a root system $(V, (\,,\,), \Phi)$ is *not reduced* (2.0.15), we call it **non-reduced**.

Definition

Definition 2.0.17.
$$(V, (\,,\,), \Phi) = (V_1, (\,,\,)_1, \Phi_1) \oplus (V_2, (\,,\,)_2, \Phi_2)$$
if $(V_i, (\,,\,)_i, \Phi_i)$ are crystallographic root systems (2.0.1), $V_1, V_2 \subset V$ are vector-*subspaces* of V, and $V = V_1 \oplus V_2$, such that
$$\Phi = \Phi_1 \coprod \Phi_2$$
i.e. $\Phi = \Phi_1 \cup \Phi_2$ and $\Phi_1 \cap \Phi_2 = \varnothing$. Furthermore, we want $(\,,\,)|_{V_i} = (\,,\,)_i : V_i \times V_i \to \mathbb{Q}$. Then we say that (V, Φ) is the **direct sum** of (V_i, Φ_i).

Definition

Definition 2.0.18. An **isomorphism of root systems** is a *linear isomorphism* $f : V_1 \xrightarrow{\sim} V_2$ such that the following holds:

1. f takes *roots to roots*, in the sense that $f(\Phi_1) = \Phi_2$.
2. $(f(u), f(v))_2 = (u, v)_1 \qquad (\forall u, v \in V_1)$.

Definition

Definition 2.0.19. A crystallographic root system (V, Φ) is **reducible** if
$$(V, \Phi) = \bigoplus_i (V_i, \Phi_i) \tag{2.0.4}$$
for some other *proper*, *non-zero* root systems (V_i, Φ_i) (cf. 2.0.13).

Remark 2.0.20. By *proper, non-zero* in 2.0.19, we mean that $0 \subsetneq V_i \subsetneq V$ for each V_i in (2.0.4).

Definition

Definition 2.0.21. If (V, Φ) is *not reducible*, then (V, Φ) is an **irreducible** (crystallographic) root system (cf. 2.0.14).

2.0.1 Classification of reduced and irreducible root systems

For all type $\mathsf{A}_n, \mathsf{B}_n, \mathsf{C}_n, \mathsf{D}_n$ with $n \geq 1$, and $\mathsf{G}_2, \mathsf{F}_4, \mathsf{E}_6, \mathsf{E}_7, \mathsf{E}_8$, there exists reduced and irreducible root systems (2.0.15 and 2.0.21, respectively). Two reduced and irreducible root systems are *isomorphic* $\Leftrightarrow$ they are of the same type.

That is:
$$\left\{\substack{\text{Reduced+irreducible} \\ \text{root systems (up to isomorphism)}}\right\} \overset{\text{1-1}}{\longleftrightarrow} \{\mathsf{A}_n, \mathsf{B}_n, \mathsf{C}_n, \mathsf{D}_n, \mathsf{G}_2, \mathsf{F}_4, \mathsf{E}_6, \mathsf{E}_7, \mathsf{E}_8\}.$$

Example 2.0.22 (type A_{n-1})**.**
$$\Phi_{\mathsf{A}}^{n-1} := \{e_i - e_j \mid 1 \leq i \neq j \leq n\}$$
is of type A_{n-1}, as in 2.0.7.

Example 2.0.23 (type D_n)**.** Let $\Phi_{\mathsf{D}}^n = \Phi_{\mathsf{A}}^{n-1} \cup \{\pm(e_i + e_j) \mid 1 \leq i \neq j \leq n\}$ where Φ_{A}^{n-1} is the same as in 2.0.22. Then $(\mathbb{Q}_0^n, \cdot, \Phi_{\mathsf{D}}^n)$ is a root system, called type D_n.

Remark 2.0.24. We will see that $(\mathbb{Q}_0^n, \cdot, \Phi_{\mathsf{D}}^n)$ in 2.0.23 is the root system of $\mathrm{SO}(2n)$, i.e. the special orthogonal group in $2n$ variables.

Remark 2.0.25. Presumably, $\cdot$ is the *dot product* $\cdot : V \times V \to \mathbb{Q}$ in 2.0.23.

Example 2.0.26 (type B_n)**.** $\Phi_{\mathsf{B}}^n = \Phi_{\mathsf{D}}^n \cup \{\pm e_i \mid 1 \leq i \leq n\}$ is a root system called type B_n.

Example 2.0.27 (type C_n)**.** $\Phi_{\mathsf{C}}^n = \Phi_{\mathsf{D}}^n \cup \{\pm 2e_i \mid 1 \leq i \leq n\}$ is a root system called type C_n.

Remark 2.0.28. In 2.0.26 and 2.0.27 we have that $e_i, 2e_i \in \Phi$.

Example 2.0.29 (type BC_n)**.** $\Phi_{\mathsf{BC}}^n = \Phi_{\mathsf{B}}^n \cup \Phi_{\mathsf{C}}^n$ is a (non-reduced; 2.0.16) root system called type BC_n.

$\mathsf{B}_n, \mathsf{C}_n, \mathsf{D}_n$ are all *reduced* and irreducible. BC_n is *non-reduced* and irreducible.

Theorem 2.0.30. (V, Φ) *non-reduced* $\Leftrightarrow \iota : \mathcal{W} \to \mathsf{GL}(V)$ *is an* irreducible *representation (2.0.14).*

Theorem 2.0.31. *Up to isomorphism, the* only *non-reduced irreducible systems are* BC_n*.*

Example 2.0.32 (type D_2)**.**

Take $V = \mathbb{Q}^2$ and let

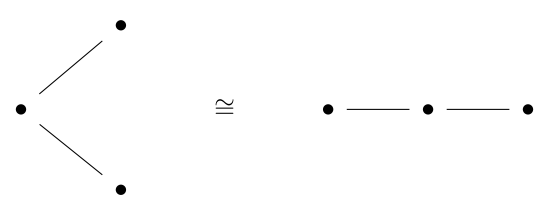
$$\begin{aligned}\Phi &= \{\pm(e_1 - e_2), \pm(e_1 + e_2)\}\\ &= \{e_1 - e_2, e_2 - e_1\} \cup \{e_1 + e_2, -e_1 - e_2\}\\ &= \{\pm(e_1 - e_2)\} \cup \{\pm(e_1 + e_2)\}\\ &= \Phi_{\mathsf{A}}^1 \cup \{\pm(e_1 + e_2)\},\end{aligned}$$

(cf. with 2.0.23). Note that (assuming $(,) = \cdot$, i.e. the dot-product)

$$\begin{aligned}(e_1 - e_2, e_1 + e_2) &= \begin{pmatrix}1\\-1\end{pmatrix} \cdot \begin{pmatrix}1\\1\end{pmatrix}\\ &= 0.\end{aligned}$$

$\rightsquigarrow \mathsf{D}_2 \cong \mathsf{A}_1 \oplus \mathsf{A}_1$, where $\Phi_1 = \{\pm(e_1 - e_2)\}$ and $\Phi_2 = \{\pm(e_1 + e_2)\}$

Example 2.0.33 ($\mathsf{D}_3 \cong \mathsf{A}_3$)**.**



2.0.2 Exceptional root systems

Example 2.0.34 (G_2)**.** Set $V = \mathbb{Q}_0^3$, and set

$$\Phi = \Phi_{\mathsf{A}}^2 \coprod \{\pm(2e_1 - e_2 - e_3), \pm(2e_2 - e_1 - e_3), \pm(2e_3 - e_2 - e_1)\},$$

where $\Phi_{\mathsf{A}}^2 = \{\pm(e_1 - e_2), \pm(e_1 - e_3), \pm(e_2 - e_3)\}$.

Just from counting the roots, i.e. the elements $\alpha \in \Phi$, we see that we have 12 roots. The 6 roots in Φ_{A}^2 are called the <u>short roots</u>, and the other 6 roots are called the <u>long roots</u>.

Theorem 2.0.35. (V, Φ) *irreducible (2.0.21)* $\Rightarrow$ *Either all roots have the same* length*, called <u>simply-laced</u>, or there are exactly <u>2</u> lengths for the roots, called <u>multi-laced</u>.*

Remark 2.0.36. $(,) \rightsquigarrow (v, v) =$ squared length of v.

Example 2.0.37 (type F_4)**.** Let $V = \mathbb{Q}_0^4$, and let

$$\Phi = \Phi_{\mathsf{B}}^4 \cup \left\{ \pm \frac{1}{2} \left(e_1 \pm e_2 \pm e_3 \pm e_4 \right) \right\}$$

where $\Phi_{\mathsf{B}}^4 = \{\pm(e_i + e_j), \pm e_i \mid 1 \leq i \neq j \leq 4\}$.

Chapter 3

Lecture 3

- Part 1: Coxeter groups.
- Part 2: Root-space decomposition for GL_n.

Recall the definition of a (crystallographic) root system (V, Φ) (2.0.1), where we omit the pairing $(,)$ from now on. We then had a *Weyl-group* $\mathcal{W}(\Phi) = \langle S_\alpha \mid \alpha \in \Phi \rangle \subset \mathsf{GL}(V)$ (2.0.9).

$$\begin{tikzcd}
\text{Root systems} \arrow[r] \arrow[dr] & \text{Coxeter groups} \arrow[d, hook] \\
& \text{Groups}
\end{tikzcd}$$

Definition

Definition 3.0.1. A **Coxeter system** is a *pair* $(\mathcal{W}, S)$ where
1. $\mathcal{W}$ is a group.
2. $S \subset \mathcal{W}$ *generates* $\mathcal{W}$, and every element $a \in S$ has *order* 2, i.e. is an *involution*.

Definition

Definition 3.0.2. A **presentation** for $\mathcal{W}$ in 3.0.1, is given by the relations:
1. $s^2 = 1$ for all $s \in S$.
2. $(st)^{m_{st}} = 1$, for all $s, t \in S$, where $m_{st} \in \mathbb{Z}_{\geq 1} \cup \{\infty\}$.

This leads to the following presentation (as most of you may have seen in group theory):

$$\mathcal{W} = \langle S \mid s^2 = (st)^{m_{st}} = 1, \forall s, t \in S \rangle,$$

where S is the set of *generators*, and the right-hand side of $\mid$ in $\langle \ldots \rangle$ above is called the *relations*.

Claim:

If there are $s, t \in S$, where S is as in 3.0.2, and $m_{st} = 1$, then this is *equivalent to* $st = 1$.

Proof.

$\Rightarrow$:

This direction is obvious: Assume that $s, t \in S$ such that $m_{st} = 1$. Then

$$\begin{aligned}(st)^{m_{st}} &= st \\ &= 1.\end{aligned}$$

$\underline{\Longleftarrow}$:

If $st = 1$, and we think of m_{st} as a positive integer (when it is not *infinite*) that gives the *minimal* positive integer k such that $(st)^k = 1$, then we see that by definition of m_{st} as a value in $\mathbb{Z}_{\geq 1} \cup \{\infty\}$, $m_{st} = 1$. □

Example 3.0.3. An example of a *presentation* (3.0.2) is

$$D_{2n} = \langle x, y \mid x^n = y^2 = 1, \underbrace{yxy^{-1} = x^{-1}}_{\Leftrightarrow yxy^{-1}x=1} \rangle. \tag{3.0.1}$$

3.0.1 Free groups

Definition

Definition 3.0.4. Let S be a set. Then $F(S) :=$ words in $S \cup S^{-1}$, e.g. for example $s_1 s_2 s_3^{-1} s_2^2 \in F(S)$ for $s_1, s_2, s_3 \in S$. The only *relations* (cf. 3.0.2) are $s \cdot s^2 = s^3$, $s^2 \cdot s^{-1} = s^1$ etc; i.e. we treat $s \in S$ as behaving as group-elements in $F(S)$, so that in particular we identify two words that are "same" up to *simplification* by the group axioms.
We call $F(S)$ the **free group on the set** S.

Remark 3.0.5. If G is a group *generated* by $S \subset G$, then we have a homomorphism $\varphi : F(S) \to G$ sending $s \overset{\varphi}{\longmapsto} s$. The *relations* satisfied by S in G are given by $\ker(\varphi)$, the "kernel of the relations". That is, it might be that $s_1 s_2 = e$ in G, but this is not "seen" in $F(S)$. But we have that

$$\begin{aligned}\varphi(s_1 s_2) &= s_1 s_2 \in G \\ &= 1, \\ \Rightarrow s_1 s_2 &\in \ker(\varphi)\end{aligned}$$

That is, the kernel of φ are the *relations* that the generators S *must satisfy in* G, since any *relation* can be rewritten with the *identity on one side of the equality*. Therefore, $F(S)/\ker(\varphi) \cong G$, by the first isomorphism theorem.

Definition

Definition 3.0.6. A group $\mathcal{W}$ is a **Coxeter group** if there exists $S \subset \mathcal{W}$ such that $(\mathcal{W}, S)$ is a *Coxeter system* (3.0.1).

Example 3.0.7. The group $\mathsf{I}_2(m)$, where $m \in \mathbb{Z}_{\geq 1} \cup \{\infty\}$ are the groups generated by 2 elements s, t, i.e. exists a subset S that generates the group. We get the *presentation*

$$\mathsf{I}_2(m) = \langle s, t \mid s^2 = t^2 = (st)^m = 1 \rangle. \tag{3.0.2}$$

We divide $\mathsf{I}_2(m)$:s behavior into two cases.

$\underline{m \neq \infty}$:

Assume that $m \neq \infty$. Then we claim that

$$\begin{aligned} \mathsf{I}_2(m) &\cong D_{2m} \\ &\cong \mathbb{Z}/m \rtimes \mathbb{Z}/2, \end{aligned} \tag{3.0.3}$$

where we can exhibit the first isomorphism in 3.0.3 given by the map $s \mapsto y$ and $st \mapsto x$. It is easy to see that they have the same presentation, hence must be isomorphic as groups:

1. We see from 3.0.2 that $(st)^m$ satisfy the same first relation as x, and that t satisfy the same first relation as y (in 3.0.1). We also want to show that $s(st)s^{-1} = (st)^{-1}$. We have

$$\begin{aligned} s(st)s^{-1} &= (s^2)ts^{-1} \\ &= ts^{-1} \\ &= t^{-1}s^{-1} \\ &= (st)^{-1} \end{aligned}$$

where we have used that $t^2 = 1 \Rightarrow t = t^{-1}$, and that $(st)^{-1} = t^{-1}s^{-1}$.

$m = \infty$:

If $m = \infty$, then $\mathsf{I}_2(m) \cong D_\infty$, the **infinite dihedral group**, with presentation given by

$$D_\infty = \langle x, y \mid y^2 = 1, yxy^{-1} = x^{-1} \rangle. \tag{3.0.4}$$

Remark 3.0.8. Note that in 3.0.7, when $m \neq \infty$, we have that D_{2m} is such that $\langle x \rangle$ is a *normal* subgroup of D_{2m}, of order m, and $\langle y \rangle$ is a subgroup of order 2. Recall that $D_{2m} = \{1, x, x^2, \ldots, x^{n-1}, y, yx, \ldots, yx^{n-1}\}$, i.e. every element can be written on the form $y^k x^i$ for $k \in \{0, 1\}$ and $i \in \{0, 1, \ldots, n-1\}$.

Furthermore, we claim that $\langle x \rangle$ is *normal* in D_{2m}. We see that $x^k x x^{-k} = x \in \langle x \rangle$, for every $k = 0, 1, \ldots, n-1$. For y, we see that $yxy^{-1} = x^{-1} \in \langle x \rangle$. Generally, we then have

$$\begin{aligned} x^k y^i x (x^k y^i)^- 1 &= x^k y^i x y^{-i} x^{-k} \\ &= x^k x x^{-k} \\ &= x \in \langle x \rangle \end{aligned}$$

if $i = 0$, and if $i = 1$ then we have

$$\begin{aligned} x^k y^i x (x^k y^i)^- 1 &= x^k y^i x y^{-i} x^{-k} \\ &= x^k x x^{-k} \\ &= x^{-1} \in \langle x \rangle \end{aligned}$$

where k was arbitrary. Hence $\langle x \rangle$ is normal. It is clear that $\langle x \rangle$ and $\langle y \rangle$ are disjoint. If we can show that

$$\langle x \rangle \langle y \rangle = \langle y \rangle \langle x \rangle \tag{3.0.5}$$

then by [1, prop. 3.2.14] $\langle x \rangle \langle y \rangle$ is a subgroup.

It is clear that any element x^k for $k = 0, 1, \ldots, n-1$ is contained in both sides of 3.0.5. If we have yx^k, by repeated application of $yxy^{-1} = x^{-1} \Leftrightarrow yx = x^{-1}y$, we have that $yx^k = x^{-k}y$, which is in $\langle x \rangle \langle y \rangle$. This exhaust all elements, so that $\langle x \rangle \langle y \rangle$ is a subgroup. Furthermore, from the fact that:

1. $\langle x \rangle$ is normal in D_{2m},
2. $\langle x \rangle \cap \langle y \rangle = \varnothing$,
3. $\langle x \rangle \langle y \rangle$ is a subgroup,

it follows that $\langle x\rangle \rtimes \langle y\rangle$. Furthermore, since $\langle y\rangle\langle x\rangle = \langle x\rangle\langle y\rangle$ and the LHS is equal to D_{2m} (just thinking about how the elements in D_{2m} are constituted), we see that $\langle x\rangle \rtimes \langle y\rangle = D_{2m}$. Note that $\langle x\rangle$ is cyclic of order m, so isomorphic to $Z_m = \mathbb{Z}/m$ and $\langle y\rangle$ is of order 2, so isomorphic to $\mathbb{Z}/2$. Therefore,

$$\begin{aligned} D_{2m} &= \langle x\rangle \rtimes \langle y\rangle \\ &\cong \mathbb{Z}/m \rtimes \mathbb{Z}/2. \end{aligned}$$

As far as I can tell, the same reasoning works to show that $\langle x\rangle$ is *normal* in D_∞, and that $\langle x\rangle$ and $\langle y\rangle$ are *disjoint*, and that their product gives us D_∞ (note that we only used the relations $y^2 = 1$ and $yxy^{-1} = x^{-1}$ for the *finite* case D_{2n}).

In this case, $\langle x\rangle$ is an infinite cyclic group; we have that $\varphi : \langle x\rangle \to \mathbb{Z}$ defined by $x^n \overset{\varphi}{\longmapsto} n$ is a group-isomorphism. Since $\langle y\rangle$ is still of order 2, we get that

$$D_\infty \cong \mathbb{Z} \rtimes \mathbb{Z}/2.$$

<u>Exercise</u>:

$$\begin{aligned} \mathcal{W}(\text{root system of type } G_2) &\cong D_{12} \\ &\cong \mathsf{I}_2(6). \end{aligned}$$

Theorem 3.0.9. *If (V, Φ) is a root system, then $\mathcal{W}(\Phi)$ is a Coxeter group (3.0.6) and $\mathcal{W}(\Phi)$ is finite.*

Example 3.0.10. Recall that the *symmetric group* of n letters, S_n, is generated by *adjacent* transpositions $\tau_i = (i\ i+1)$ for $1 \le i \le n-1$, subject to the following relations:

1. $\tau_i^2 = 1 \qquad (\forall i \in \{1, \dots, n-1\})$.
2. $(\tau_i\tau_j)^2 = 1 \Leftrightarrow \tau_i\tau_j = \tau_j\tau_i \qquad (\forall |i-j| \ge 2)$.
3. $(\tau_i\tau_{i+1})^3 = 1 \Leftrightarrow \tau_i\tau_{i+1}\tau_i = \tau_{i+1}\tau_i\tau_{i+1} \qquad (\forall i \text{ such that } 1 \le i \le n-2)$.

The relations are easy to check: (a) holds trivially, since the order of any transposition is 2. The second relation hold since disjoint transpositions commutes (disjointness assured by $|i-j| \ge 2$), so that

$$\begin{aligned} (\tau_i\tau_j)^2 &= \tau_i^2\tau_j^2 \\ &= 1 \end{aligned}$$

where the last equality follows from (a). For (c): note that $\tau_i(\tau_i+1) = (i\ i+1\ i+2)$, hence has order 3, and the result follows.

Let

$$\mathcal{W} = \left\langle s_1, \dots, s_{n-1} \;\middle|\; s_i^2 = 1, \text{ and } m_{ij} = \begin{cases} 3, & \text{if } |i-j| = 1, \\ 2, & \text{if } |i-j| \ne 1 \end{cases} \right\rangle. \tag{3.0.6}$$

We see that m_{ij} in 3.0.6 gives smallest positive integer m_{ij} such that $(s_is_j)^{m_{ij}} = 1$ (cf. 3.0.2).

$$\rightsquigarrow \quad \begin{tikzcd} F(s_1, \dots, s_{n-1}) \arrow[rr, two heads, "\varphi"] \arrow[dr] & & S_n \\ & \mathcal{W} \arrow[ur, two heads, "f"'] & \end{tikzcd} \tag{3.0.7}$$

In 3.0.7 we have the free group on the generators s_i. As in 3.0.5, we see that

$$\begin{aligned} F(s_1, \dots, s_{n-1})/\ker(\varphi) &= \mathcal{W} \\ &\cong S_n, \end{aligned}$$

by the first isomorphism theorem. I.e. we are essentially quoting by the relations in S_n.

Theorem 3.0.11 (Classification of finite Coxeter groups)**.** *Up to isomorphism, the* irreducible *finite Coxeter groups are precisely* $\mathcal{W}(\Phi)$ *(2.0.9) for* (V, Φ) *irreducible root system (2.0.21), together with* $\mathsf{I}_2(m)$ *for* $n \geq 3$*, and* $\mathsf{H}_3, \mathsf{H}_4$ *with the isomorphisms*

$$\begin{aligned} \mathcal{W}(\Phi \text{ of type } \mathsf{B}_m) &\cong \mathcal{W}(\Phi \text{ of type } \mathsf{C}_m) \\ \mathsf{I}_2(6) &\cong \mathcal{W}(\text{type } \mathsf{G}_2) \\ \mathsf{I}_2(4) &\cong \mathcal{W}(\text{type } \mathsf{B}_2 \cong \mathsf{C}_2) \\ \mathsf{I}_2(3) &\cong \mathcal{W}(\mathsf{A}_2). \end{aligned}$$

We have $\mathsf{I}_2(2) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. Note that $\mathsf{I}_2(2) = \langle s, t \mid s^2 = t^2 = (st)^2 = 1 \rangle$. But

$$\begin{aligned} \mathbb{Z}/2 \times \mathbb{Z}/2 &= \langle s_1, s_2 \mid s_1^2 = s_2^2 = 1, s_1 s_2 = s_2 s_1 \rangle \\ &= \langle s, t \mid s^2 = t^2 = (st)^2 = 1 \rangle, \end{aligned}$$

where we in the last equality used that

$$\begin{aligned} s_1 s_2 &= s_2 s_1 \\ \Leftrightarrow (s_1 s_2)(s_2 s_1)^{-1} &= 1 \\ \Leftrightarrow s_1 s_2 s_1^{-1} s_2^{-1} &= 1 \\ \Leftrightarrow s_1 s_2 s_1 s_2 &= 1 \\ \Leftrightarrow (s_1 s_2)^2 &= 1 \end{aligned}$$

since $s_i = s_i^{-1}$.

Similar to $\mathcal{W}(\Phi)$, if $\mathcal{W}$ is a Coxeter group (3.0.6), then there exists a *representation* (2.0.11) $\rho : \mathcal{W} \to \mathsf{GL}(V)$ such that $\rho(s)$ is a *reflection*, for all $s \in S$, where S *generates* $\mathcal{W}$ and such that all $s \in S$ has order 2 (see 3.0.1).

Remark 3.0.12. Unsure why such a reflection exists, above paragraph.

Definition

Definition 3.0.13. We say that $\mathcal{W}$ is **irreducible** if ρ is an irreducible representation (2.0.14).

If we have a reduced (2.0.15)+ irreducible (2.0.21) root system, then we find that its weyl group (2.0.9) will be a finite coxeter group (cf. 3.0.11).

Definition

Definition 3.0.14. If we have a Coxeter system $(\mathcal{W}, S)$ (3.0.1), then the *vertex set* of the corresponding **Coxeter Graph** will be the generating set of involutions S. $s, t \in S$ will *be connected* by an edge $\Leftrightarrow m_{st} \neq 2$.
We have that the associated graph is *connected* $\Leftrightarrow$ $\mathcal{W}$ is irreducible. Note that if $m_{st} = 2$ for all $s, t \in S$, then $\mathcal{W}$ is abelian, and therefore the representation $\rho : \mathcal{W} \to \mathsf{GL}(V)$ must be one-dimensional (the irreducible representations of an abelian group are all one-dimensional).

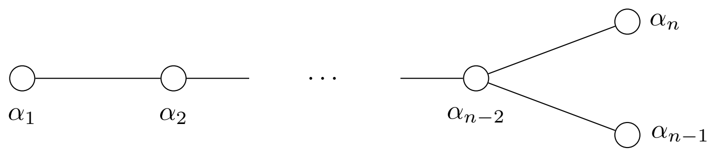
Below, we label an edge by m_{st} if $m_{st} > 3$. We exhibit the graphs of the *finite* + *irreducible* ones.

Remark 3.0.15. Below, a double edge indicates that $m_{st} > 3$. The *(double) arrow points from the generator associated with the shorter root to the generator associated with the longer root.*

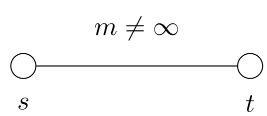
A_{n-1}

B_n

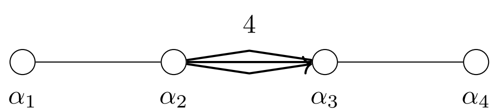
D_n



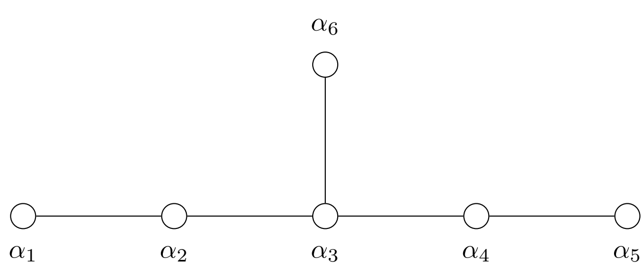
$\mathsf{I}_2(m)$



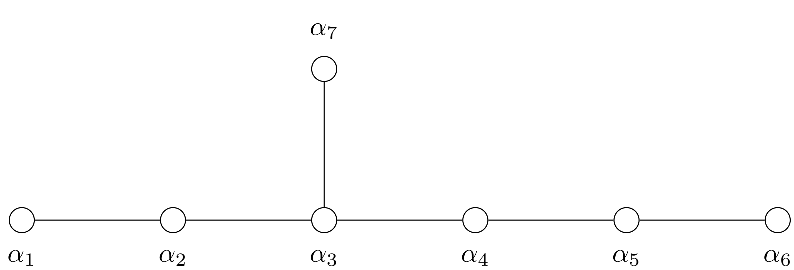
F_4



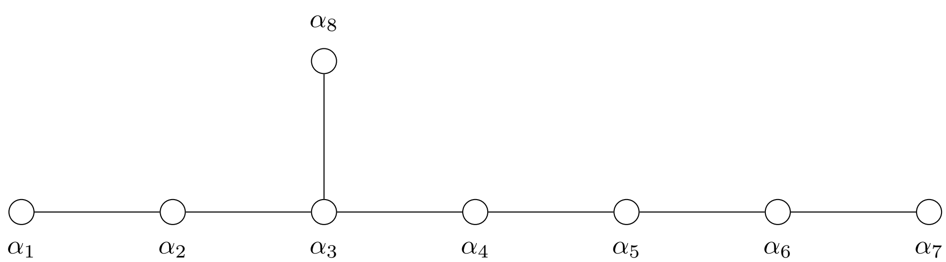
E_6



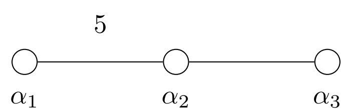
E_7



E_8



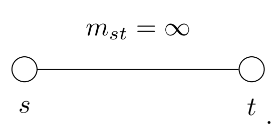
H_3



H_4

For an example of an *infinite Coxeter group with* 2 *generators, we have*

$\mathsf{I}_2(\infty)$



3.0.2 Root-space decomposition

We look at $\mathsf{GL}(n)$ with $\Bbbk$ a field. Let

$$\mathrm{Diag}(n, \Bbbk) = \left\{ t = \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix} \middle| \; t_1, \dots, t_n \in \Bbbk^\times \right\} \subset \mathsf{GL}(n, \Bbbk)$$

be the (commutative) *subgroup of diagonal matrices.* Let $M_n(\Bbbk)$ be the $\Bbbk$-algebra of all $n \times n$-matrices with elements from $\Bbbk$. Let $\mathsf{GL}(n, \Bbbk)$ act on $M_n(\Bbbk)$ by conjugation, i.e. we have

$$\begin{aligned} \mathsf{GL}(n, \Bbbk) \times M_n(\Bbbk) &\to M_n(\Bbbk) \\ (g, x) &\mapsto gag^{-1}. \end{aligned} \tag{3.0.8}$$

We can *restrict* the action in 3.0.8 to $\mathrm{Diag}(n, \Bbbk)$.

Linear algebra: If $S \subset \mathsf{GL}(n, \Bbbk)$ and $st = ts$ for all $s, t \in S$, and s is diagonalizable for all $s \in S$, then S is simultaneously diagonalizable.

Remark 3.0.16. Note that $M_n(\Bbbk)$ is a vector space over $\Bbbk$ of dimension n^2.

We want to diagonalize the action of $\mathrm{Diag}(n, \Bbbk)$ on $M_n(\Bbbk)$ by conjugation. We need $A \in M_n(\Bbbk)$ such that $tAt^{-1} = \lambda(t)A$, where λ is a *scalar eigenvalue* $\lambda \in \Bbbk$.

Let $\mathrm{diag}(n, \Bbbk)$ be the *set* of all *diagonal* matrices in $M_n(\Bbbk)$ (cf. with $\mathrm{Diag}(n, \Bbbk) \subset \mathsf{GL}(n, \Bbbk)$).

Note that since $\Bbbk$ is a field, we have that $\mathrm{diag}(n, \Bbbk) \subset \lambda = 1$-eigenspace of $\mathrm{Diag}(n, \Bbbk)$ in $\mathsf{GL}(n, \Bbbk)$. That is, $tAt^{-1} = A, \forall t \in \mathrm{Diag}(n, \Bbbk)$.

We have the **elementary matrices** E_{ij} in $M_n(\Bbbk)$, which is a basis for the n^2 vector space over $\Bbbk$ $M_n(\Bbbk)$.

Example 3.0.17. Let $E_{12} \in M_3(\Bbbk)$. Then

$$E_{12} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

We see that $tE_{ii}t^{-1} = E_{ii}$ for $t \in \mathrm{Diag}(n, \Bbbk)$. For $1 \leq i, j \leq n$ with $i \neq j$, we have

$$\begin{aligned}
tE_{ij}t^{-1} &= \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix} E_{ij} \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix}^{-1} \\
&= \begin{pmatrix} t_1 \cdot E^1 \\ t_2 \cdot E^2 \\ \vdots \\ t_n \cdot E^n \end{pmatrix} \begin{pmatrix} t_1^{-1} & & & \\ & t_2^{-1} & & \\ & & \ddots & \\ & & & t_n^{-1} \end{pmatrix} \\
&= \begin{pmatrix} \vdots \\ t_i E^i \\ \vdots \end{pmatrix} \begin{pmatrix} t_1^{-1} & & & \\ & t_2^{-1} & & \\ & & \ddots & \\ & & & t_n^{-1} \end{pmatrix} \\
&= t_i E_{ij} \begin{pmatrix} t_1^{-1} & & & \\ & t_2^{-1} & & \\ & & \ddots & \\ & & & t_n^{-1} \end{pmatrix} \\
&= t_i t_j^{-1} E_{ij} \\
&= \left(\frac{t_i}{t_j} \right) E_{ij}.
\end{aligned}$$

Remark 3.0.18. Above, we have used E^i for the i^{th} row of E_{ij}.

So, we have seen that $\lambda = t_i t_j^{-1}$ is the scalar eigenvalue under the conjugation-action by $\mathrm{Diag}(n, \Bbbk)$ on $E_{ij} \in M_n(\Bbbk)$. Now recall that $\{E_{ij} \mid 1 \leq i, j \leq n\}$ is a basis for $M_n(\Bbbk)$.

We have that

$$\mathrm{diag}(n, \Bbbk) \oplus \left(\bigoplus_{i \neq j} \mathrm{span}_{\Bbbk}(E_{ij}) \right).$$

The equation above is an eigenspace-decomposition. For some t the e-spaces can coalesce.

Example 3.0.19. Take

$$\begin{pmatrix} t_1 & & \\ & t_2 & \\ & & t_3 \end{pmatrix} \subseteq \mathrm{Diag}(3, \Bbbk)$$

with $t_1 \neq t_3$ and $t_1 = t_2 \Rightarrow \dfrac{t_1}{t_3} = \dfrac{t_2}{t_3}$.

We find that $\frac{t_1}{t_3}$:s eigenspace is spanned by E_{13}, E_{23}.

Definition

Definition 3.0.20. If $t \in \mathrm{Diag}(n, \Bbbk)$ with $t_i \neq t_j$ for $i \neq j$, then we call t **regular**.

The eigenvalues of the action $t \curvearrowright M_n(\Bbbk)$ are 1 with multiplicity n and $\frac{t_i}{t_j}$ with multiplicity 1 if $i \neq j$ for all i, j. By multiplicity here, we mean *geometric multiplicity*, in the sense of the number of linearly independent (eigen) vectors that span each eigenvalue.

Remark 3.0.21. Note that we can rewrite tAt^{-1} as

$$\begin{aligned} tAt^{-1} &= \sum_{i,j=1}^{n} t a_{ij} E_{ij} t^{-1} \\ &= \sum_{i,j=1}^{n} \frac{t_i}{t_j} a_{ij} E_{ij} \end{aligned} \tag{3.0.9}$$

where a_{ij} is the scalar in row i, column j of $A \in M_n(\Bbbk)$.

Definition

Definition 3.0.22. Let $e_i : \mathrm{Diag}(n, \Bbbk) \to \Bbbk^\times = \mathsf{GL}(1, \Bbbk)$, be defined explicitly by

$$t = \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix} \xmapsto{e_i} t_i.$$

This is a group-homomorphism, since we have

$$\begin{aligned} e_i(tt') &= t_i t_i' \\ &= e_i(t) e_i(t'). \end{aligned}$$

Definition

Definition 3.0.23. We define $\mathrm{Hom}(H, \mathsf{GL}(1))$ as the **characters of** H.

For all $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$, we have the character $a : \mathrm{Diag}(n, \Bbbk) \to \mathsf{GL}(1, \Bbbk)$, defined explicitly by $t \xmapsto{a} \prod_{i=1}^{n} t_i^{a_i}$.

We define $-e_j = t_j^{-1}$. Note that if a, b are characters in $\mathrm{Hom}(\mathrm{Diag}(n, k), \mathsf{GL}(1, \Bbbk))$, then $a + b \in \mathrm{Hom}(\mathbb{Z}^n, \mathsf{GL}(1, \Bbbk))$. Furthermore, we have an injection $\mathbb{Z}^n \hookrightarrow \mathrm{Hom}(\mathrm{Diag}(n, \Bbbk), \mathsf{GL}(n, \Bbbk))$ defined by $\mathbb{Z}^n \ni (a_1, \ldots, a_n) \mapsto \left(t \mapsto \prod_{i=1}^{n} t_i^{a_i} \right)$, which we note sends $e_i \mapsto e_i$.

We also have a map $\lambda_{ij} : \mathrm{Diag}(n, \Bbbk) \to \mathsf{GL}(1, \Bbbk)$ defined by $t \mapsto \frac{t_i}{t_j} = (e_i - e_j)(t)$, i.e. the eigenvalue of $t \curvearrowright E_{ij} \in M_n(\Bbbk)$ by conjugation.

We claim that λ_{ij} is a group homomorphism. We have

$$\begin{aligned}\lambda_{ij}(st)\frac{(st)_i}{(st)_j} &= \frac{s_i t_i}{s_j t_j} \\ &= \frac{s_i}{s_j}\frac{t_i}{t_j} \\ &= \lambda_{ij}(s)\lambda_{ij}(t).\end{aligned}$$

We see further that $0 \in \mathbb{Z}^n$ gets sent under the injection $\mathbb{Z}^n \hookrightarrow \operatorname{Hom}(\operatorname{Diag}(n, \Bbbk), \mathsf{GL}(n, \Bbbk))$ to the map that takes $t \mapsto 1$.

Remark 3.0.24. The eigenvalue 1 of the action of $t \in \operatorname{Diag}(n, \Bbbk)$ on $M_n(\Bbbk)$ thus corresponds to $0 \in \mathbb{Z}^n$ (have a hard time interpreting exactly what is going on here, the notes are hard to read). I think the notes read e-value $1 \Leftrightarrow$ char $0 \in \mathbb{Z}^n$. I think we identify $0 \in \mathbb{Z}^n$ with its image under the injection into $\operatorname{Hom}(\operatorname{Diag}(n, \Bbbk), \mathsf{GL}(1, \Bbbk))$.

The characters that occur in the decomposition of $M_n(\Bbbk)$ into a *simultaneous* eigenspace are 0, $e_i - e_j$ for $i \neq j$. The first one corresponds to the eigenvalue 1, the second to $\frac{t_i}{t_j}$. The non-zero class $\{e_i - e_j \mid i \neq j\}$ forms a A_{n-1} root system (2.0.1) in $\operatorname{span}_{\mathbb{Q}}\{e_i - e_j \mid i \neq j\}$ with the dot product $\cdot$ (symmetric bilinear form).

3.1 Application

Assume that $|\Bbbk| > 2$. $\operatorname{Cent}_{M_n(\Bbbk)}\operatorname{Diag}(n, \Bbbk) = \operatorname{diag}(n, \Bbbk)$, and $\operatorname{Cent}_{\mathsf{GL}(n,\Bbbk)}\operatorname{Diag}(n, \Bbbk) = \operatorname{Diag}(n, \Bbbk)$.

Let $A = (a_{ij}) \in M_n(\Bbbk)$. If $\exists\, i, j$ where $i \neq j$ such that $a_{ij} \neq 0$, take $t \in \operatorname{Diag}(n, \Bbbk)$ such that $t_i \neq t_j$. By using 3.0.9 we find that the coefficient in front of E_{ij} for A and tAt^{-1} respectively is $\dfrac{t_i}{t_j}a_{ij}$ and a_{ij}, which are not equal, since $\dfrac{t_i}{t_j} \neq 1$, and $a_{ij} \neq 0$. It follows that $tAt^{-1} \neq A$ with the given conditions.

Definition

Definition 3.1.1. A subset $H \subset \operatorname{Diag}(n, \Bbbk)$ is **regular** if it holds for all $i \neq j$ there exists $h \in H$ such that $h_i \neq h_j$.

The previous argument then shows that if $H \subset \operatorname{Diag}(n, \Bbbk)$ is regular (3.1.1), then $\operatorname{Cent}_{M_n(\Bbbk)}(H) = \operatorname{diag}(n, \Bbbk)$, and that $\operatorname{Cent}_{\mathsf{GL}(n,\Bbbk)}(H) = \operatorname{Diag}(n, \Bbbk)$.

Example 3.1.2. If $n = 2m$ then

$$H = \left\{\begin{pmatrix} s_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & s_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & s_m & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & s_m^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & s_1^{-1} \end{pmatrix}\right\}$$

is a *regular* (3.1.1) subgroup of $\mathsf{GL}(n, \Bbbk)$.

Remark 3.1.3. Note that in a field of char $p \neq 2$, the only solutions to $x^2 - 1 = 0 \in \Bbbk[x]$ are 1 and -1.

Corollary 3.1.4. *Diag*$(n, \Bbbk)$ *is a* maximal *commutative subgroup of* $\mathsf{GL}(n, \Bbbk)$.

$\mathrm{Diag}(n, \Bbbk)$ is an example of a <u>maximal torus</u>.

Future

We want to generalize

$$\begin{aligned} \mathsf{GL}(n, \Bbbk) &\rightsquigarrow \text{Reductive group}, \\ \mathrm{Diag}(n, \Bbbk) &\rightsquigarrow \text{maximal torus}, \\ M_n(\Bbbk) &\rightsquigarrow \text{Lie algebra of the group}. \end{aligned}$$

Chapter 4

Lecture 4

- Part 1: Irreducible components of root systems.
- Part 2: Root datum of $\mathsf{GL}(n)$.

We want $(\mathbb{Q}^n, \Phi) \to (\mathbb{Q}^n, 2\Phi)$ defined explicitly by $\mathbb{Q}^n \ni v \mapsto 2v$ to be an isomorphism. E.g. $\Phi = \{\pm(e_i \pm e_j)\}$, so for example that we have $(\mathbb{Q}, \Phi = \{\pm 2\}) \xrightarrow{\sim} (\mathbb{Q}, \Phi = \{\pm 4\})$.

Definition

Definition 4.0.1. $(V_1, \Phi_1, (,)_1) \to (V_2, \Phi_2, (,)_2)$ is an isomorphism if $f : V_1 \xrightarrow{\sim} V_2$ is an isomorphism of vector spaces, such that $f(\Phi_1) = \Phi_2$, and

$$\begin{aligned}(\alpha, \beta^\vee)_1 &= 2\frac{(\alpha, \beta)_1}{(\beta, \beta)_1} \\ &= 2\frac{(f(\alpha), f(\beta))_2}{(f(\beta), f(\beta))_2} \\ &= (f(\alpha), f(\beta)^\vee)_2, \qquad (\forall \alpha, \beta \in \Phi).\end{aligned}$$

Remark 4.0.2. Recall that $\beta^\vee = 2\dfrac{\beta}{(\beta, \beta)}$ is the *coroot* of β (2.0.3).

We also have the "crystallographic axiom" $(\alpha, \beta^\vee) \in \mathbb{Z}, \forall \alpha, \beta \in \Phi$.

If $(V, \Phi) = (V_1, \Phi_1) \oplus (V_2, \Phi_2)$ then multiplying by 2 on (V_2, Φ_2) will give an isomorphism (V_2, Φ_2), and multiplying by 1 on (V_1, Φ_1) is the same as the identity isomorphism on (V_1, Φ_1).

Note here that $v \overset{2}{\longmapsto} 2v$ is such that it is an isomorphism of $\mathbb{Q}$-vector spaces, that $2\Phi_2$ gives us another *finite* set, and that, if we fix $(,)$, we will have

$$2\frac{(2\alpha, 2\beta)_1}{(2\beta, 2\beta)_1} = 2\frac{(\alpha, \beta)_1}{(\beta, \beta)}, \qquad (\forall \alpha, \beta \in \Phi_2).$$

We will have $(\alpha, \beta^\vee) = 0$ for all $\alpha \in \Phi_1, \beta \in \Phi_2$. The rations of lengths can vary between different irreducible components.

Lemma 4.0.3. *Every root system (2.0.1) is a direct sum of irreducible root systems (2.0.21). That is*

$$(V, \Phi) = (V_1, \Phi_1) \oplus \ldots \oplus (V_1, \Phi_r), \qquad ((V_i, \Phi_i) \text{ irreducible rootsystem}). \tag{4.0.1}$$

The decomposition 4.0.1 is unique up to permuting the factors (not just up to isomorphism)!

Example 4.0.4.

$$\begin{aligned}\mathbb{Q}^2 &= \mathbb{Q}e_1 \oplus \mathbb{Q}e_2 \\ &= \mathbb{Q}(e_1+e_2) \oplus \mathbb{Q}(e_1-e_2).\end{aligned}$$

Note here that

$$\begin{aligned}a(e_1+e_2)+b(e_1-e_2) &= e_1(a+b)+e_2(a-b) \\ &= 0 \\ &\Rightarrow a+b=0 \Leftrightarrow a=-b \\ &\quad a-b=0 \Leftrightarrow -2b=0 \\ \\ &\Rightarrow a=b \\ &= 0.\end{aligned}$$

which shows *linear independence*, and furthermore, that

$$\begin{aligned}e_1 &= \frac{(e_1+e_2)+(e_1-e_2)}{2} \\ e_2 &= \frac{(e_1+e_2)-(e_1-e_2)}{2}\end{aligned}$$

To see that we can then express any vector $ce_1+de_2 \in \mathbb{Q}^2$ in this other basis, so that $\{e_1+e_2, e_1-e_2\}$ *span* $\mathbb{Q}^2$ We have

$$\begin{aligned}ce_1+de_2 &= a(e_1+e_2)+b(e_1-e_2) \\ \Leftrightarrow (c-a-b)e_1+(d-a+b)e_2 &= 0 \\ &\Rightarrow c=a+b \text{ and } d=a-b \\ &\Rightarrow c+d=2a \Leftrightarrow a=\frac{c+d}{2} \text{ and } c-d=2b \Leftrightarrow \frac{c-d}{2}=b,\end{aligned}$$

therefore, $\{e_1 \pm e_2\}$ spans $\mathbb{Q}^2$.

Remark 4.0.5. Note that the above reasoning just shows that $\{e_1 \pm e_2\}$ is a basis for $\mathbb{Q}^2$.

Since

$$\begin{aligned}a(e_1-e_2) &= be_1 \\ \Leftrightarrow e_1(a-b)+be_2 &= 0 \\ &\Leftrightarrow b=0 \text{ and } a-b=0 \Rightarrow b=a \\ &= 0,\end{aligned}$$

and

$$\begin{aligned}a(e_1-e_2) &= be_2 \\ \Leftrightarrow ae_1+e_2(-a-b) &= 0 \\ &\Leftrightarrow a=0 \text{ and } -a-b=0 \Leftrightarrow a=-b \Rightarrow b=0,\end{aligned}$$

we get

$$\begin{aligned}\mathbb{Q}(e_1-e_2) \cap \mathbb{Q}e_1 &= 0 \\ \mathbb{Q}(e_1-e_2) \cap \mathbb{Q}e_2 &= 0.\end{aligned}$$

We now prove 4.0.3

Proof. Existence of decomposition: By induction on $\dim(V)$. If (V,Φ) already is irreducible (2.0.21), then we are done. If not, then (V,Φ) is reducible, so we can write

$$(V,\Phi) = (V_1,\Phi_1) \oplus (V_2,\Phi_2)$$

with $\dim(V_1), \dim(V_2) < \dim(V)$; then by *strong induction* on the dimension, we see that (V_1,Φ) and (V_2,Φ_2) decompose as a direct sum of irreducible root systems.

Uniqueness: Assume that $(V,\Phi) = (V',\Phi') \oplus (V'',\Phi'')$. We claim that (V',Φ') is a direct sum of some factors (V_i,Φ_i).

"Exists To Show" (ETS): If $\Phi_i \cap \Phi' \neq \varnothing$ then $(V_i,\Phi_i) \subset (V',\Phi')$.

Proof. Assume that $\Phi_i \cap \Phi' \neq \varnothing$. Then $\Phi_i = (\Phi_i \cap \Phi') \coprod (\Phi_i \cap \Phi'')$. So

$$V_i = (V_i \cap V') \oplus (V_i \cap V''). \tag{4.0.2}$$

But the first summand in 4.0.2 is the span of $\Phi_i \cap \Phi'$ and the second is the span of $\Phi_i \cap \Phi''$. Since V_i is irreducible, we need $V_i \cap V'' = \varnothing$. Therefore, $V_i \cap V' = V_i \Rightarrow V_i \subset V'$. □

□

Definition

Definition 4.0.6. If we have a decomposition of a root system as in 4.0.3, i.e. assume we have a root system (V,Φ) such that

$$(V,\Phi) = \bigoplus_{i=1}^{n} (V_i,\Phi_i).$$

Then the (V_i,Φ_i) are called the **irreducible components of the root system** (V,Φ).

If $f : (V_1,\Phi_1) \xrightarrow{\sim} (V_2,\Phi_2)$ such that $f(\Phi_1) = \Phi_2$, then f is an isomorphism of root systems, such that $\frac{(\alpha,\alpha)_1}{(\beta,\beta)_1}$ is preserved on every irreducible component (α,β in the same component).

4.1 Part 2

Last time: Root space decomposition. Recall that $M_n(\mathbf{F})$ = all $n \times n$-matrices with elements from a field $\mathbf{F}$ (or more generally $M_n(R)$ with R the elements of a ring).

We have an action $\mathsf{GL}(n,\mathbf{F}) \curvearrowright M_n(\mathbf{F})$ by conjugation, and recall that $\mathrm{Diag}(n,\mathbf{F})$ is a subgroup of $\mathsf{GL}(n,\mathbf{F})$. We had the (eigenspace) decomposition

$$M_n(\mathbf{F}) = \mathfrak{diag}(n,\mathbf{F}) \bigoplus_{i\neq j} \mathrm{span}_{\mathbf{F}}(E_{ij}).$$

Let $t \in \mathrm{Diag}(n,\mathbf{F})$, so that t is on the form

$$t = \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix},$$

Then we saw that

$$\begin{aligned} tE_{ij}t^{-1} &= \frac{t_i}{t_j} \\ &= (e_i - e_j)(t)E_{ij}, \end{aligned}$$

where we recall that

$$\mathrm{Hom}(\mathrm{Diag}(n, \mathbf{F}), \mathsf{GL}(1, \mathbf{F})) \ni e_i : \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix} \mapsto t_i$$

Definition

Definition 4.1.1. We define $X^*(\mathrm{Diag}(n)) = \mathrm{Hom}(\mathrm{Diag}(n), \mathsf{GL}(1))$, the **group of characters of** $\mathrm{Diag}(n)$.

We have $X^*(\mathrm{Diag}(n)) = \left\{ \begin{smallmatrix} \forall R \text{ where } R \text{ is a commutative ring with } 1 \\ f_R \text{ such that the diagram below commutes} \end{smallmatrix} \right\}$

$$\begin{tikzcd} \mathrm{Diag}(n, R) \arrow[r, "f_R"] \arrow[d, "\mathsf{GL}(n,\varphi)"'] & \mathsf{GL}(1, R) \arrow[d, "\mathsf{GL}(1,\varphi)=\varphi"] \\ \mathrm{Diag}(n, S) \arrow[r, "f_S"'] & \mathsf{GL}(1, S) \end{tikzcd} \tag{4.1.1}$$

In 4.1.1 we see that $f : \mathrm{Diag}(n, -) \Rightarrow \mathsf{GL}(1, -)$ is a natural transformation between the <u>functors</u> $\mathrm{Diag}(n, -)$ and $\mathsf{GL}(1, -)$, and φ is a ring-homomorphism $\varphi : R \to S$; the map $\mathsf{GL}(n, \varphi)$ is obtained by

$$\mathrm{Diag}(n, R) \ni \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix} \xmapsto{\mathsf{GL}(n,\varphi)} \begin{pmatrix} \varphi(t_1) & & & \\ & \varphi(t_2) & & \\ & & \ddots & \\ & & & \varphi(t_n) \end{pmatrix} \in \mathrm{Diag}(n, S),$$

and $\mathsf{GL}(1, \varphi)$ is just φ, taking an element t in $\mathsf{GL}(1, R) \cong R^\times$ to $\varphi(t) \in \mathsf{GL}(1, S) \cong S^\times$. For f to be a <u>natural transformation</u>, 4.1.1 has to commute for all ring-homomorphisms $\varphi : R \to S$ where R, S are commutative rings with 1. We call f_R the **component of** f **at** R. $\mathrm{Diag}(n, -)$ and $\mathsf{GL}(1, -)$ are **group functors**.

We have that $\mathbb{Z}^n \subset X^*(\mathrm{Diag}(n))$, by looking at the $\mathbb{Z}$-span of the basis $\{e_i\}_{i=1}^n$, i.e. the map

$$\begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix} \mapsto t_i + t_j$$

is equal to $(e_i + e_j)(t)$.

$X^*(\mathrm{Diag}(n))$ is an *abelian group* under multiplication of maps as follows; for $f, g : \mathrm{Diag}(n, \mathbf{F}) \rightrightarrows \mathsf{GL}(1, \mathbf{F})$ we set $(fg)(t) := f(t)g(t)$. This is an abelian group since the target $\mathsf{GL}(1, \mathbf{F}) \cong \mathbf{F}^\times$ is abelian.

For $(a_1, \dots, a_n) \in \mathbb{Z}^n$, we have that

$$(a_1, \dots, a_n) : \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix} \mapsto \prod_{i=1}^n t_i^{a_i}$$

Fact: $\mathrm{Diag}(n) = \mathbb{Z}^n$, i.e. these are the "exotic" homs $\mathrm{Diag}(n) \to \mathsf{GL}(1)$.

Let $\mathbf{F} = k$ be algebraically closed (we can think of this as $\mathbb{C}$). Then $X^*(\mathrm{Diag}(n))$ can also be defined as $\mathrm{Hom}(\mathrm{Diag}(n), \mathsf{GL}(1))$, i.e. the homomorphisms of algebraic groups, thought of as varieties (to be defined); homomorphisms of groups $\mathrm{Diag}(n, k) \to \mathsf{GL}(1, k)$ given by rational functions.

We have seen that $X^*(\mathrm{Diag}(n)) \supset \mathbb{Z}^n \supset \{e_i - e_j \mid i \neq j\}$, where $\{e_i - e_j \mid i \neq j\}$ spans a root system of type A_{n-1} (2.0.7).

$\mathrm{span}_{\mathbb{Q}}(e_i - e_j \mid i \neq j) \subsetneq \mathbb{Z}^n$!.

Definition

Definition 4.1.2. *Elements* of X^* are called **characters**, i.e. homomorphisms to $\mathsf{GL}(1)$.
Definition 4.1.3. *Elements* of X_* are homomorphisms from $\mathsf{GL}(1)$, and are **cocharacters**.

So we have $X_*(\mathrm{Diag}(n)) = \mathrm{Hom}(\mathsf{GL}(1), \mathrm{Diag}(n))$ which are homomorphisms of *algebraic* groups. We can think of this both as homomorphisms of **group schemes** or homomorphisms of **group varieties**.

As homomorphisms of group schemes, we exhibit the diagram below (cf. with 4.1.1). We have a natural transformation $f : \mathsf{GL}(1, -) \Rightarrow \mathrm{Diag}(n, -)$, such that for all ring-homomorphisms $\varphi : R \to S$, we get the following commutative diagram

$$\begin{tikzcd} \mathsf{GL}(1,R) \arrow[r, "f_R"] \arrow[d, "\mathsf{GL}(1,\varphi)=\varphi"'] & \mathrm{Diag}(n,R) \arrow[d, "\mathrm{Diag}(n,\varphi)"] \\ \mathsf{GL}(1,S) \arrow[r, "f_S"'] & \mathrm{Diag}(n,S) \end{tikzcd}$$

Let $t \in \mathrm{Diag}(n, R)$, so that

$$t = \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix},$$

where $t_i \in R^\times$, then

$$\mathrm{Diag}(n, \varphi)(t) = \begin{pmatrix} \varphi(t_1) & & & \\ & \varphi(t_2) & & \\ & & \ddots & \\ & & & \varphi(t_n) \end{pmatrix}$$

where $\varphi(t_i) \in S^\times$ (since a ring-homomorphism φ has to take units to units; if $r \in R$ is a unit with inverse r^{-1}, then $\varphi(r)^{-1}$ is a unit for $\varphi(r)$).

Definition

Definition 4.1.4. X^* denote homomorphism **to** $\mathsf{GL}(1)$. Elements of X^* are called **characters**.
Definition 4.1.5. We let X_* denote homomorphisms **from** $GL(1)$. Elements of X_* are called **cocharacters**.

With 4.1.4 in mind, we have $X^*(\mathrm{Diag}(n)) = \mathrm{Hom}(\mathrm{Diag}(n), \mathsf{GL}(1))$, which are homomorphisms of **algebraic groups**; again, we can think of this as either homomorphisms of **group schemes**, are as homomorphisms of **group varieties**.

If we choose to $X^*(\mathrm{Diag}(n))$ as homomorphisms of **group schemes**:

- We have group homomorphisms f_R for all commutative rings R with unit, such that for all ring-homomorphisms $\varphi : R \to S$, we have the following *commutative* square:

$$\begin{tikzcd}
\mathsf{GL}(1,R) \arrow[r, "f_R"] \arrow[d, "\mathsf{GL}(1,\varphi)"'] & \mathrm{Diag}(n,R) \arrow[d, "\mathsf{GL}(n,\varphi)"] \\
\mathsf{GL}(1,S) \arrow[r, "f_S"'] & \mathrm{Diag}(n,S)
\end{tikzcd}$$

We have the following sequence of morphisms

$$\begin{tikzcd}
\mathsf{GL}(1) \arrow[r, "\mu", "\text{cocharacter}"'] \arrow[rr, bend right] & \mathrm{Diag}(n) \arrow[r, "\chi", "\text{character}"'] & \mathsf{GL}(1)
\end{tikzcd}$$

with μ a cocharacter (4.1.5) and χ a character (4.1.4). We have that $(\chi \circ \mu)(z) = z^n$. Furthermore, recall that $X^*(\mathrm{Diag}(n)) \cong \mathbb{Z}^n$ (or perhaps, under univalent identification, $=$). We further note that

$$\begin{aligned} X^*(\mathrm{Diag}(n)) &= X^*(\mathsf{GL}(1)) \\ &= \mathbb{Z}. \end{aligned}$$

Here, μ takes

$$z \overset{\mu}{\longmapsto} \begin{pmatrix} z & & & \\ & z & & \\ & & \ddots & \\ & & & z \end{pmatrix},$$

and then χ takes $\begin{pmatrix} z & & & \\ & z & & \\ & & \ddots & \\ & & & z \end{pmatrix}$ to z^n; or more generally, χ takes $\mathrm{diag}(t_1^{n_1}, \ldots, t_n^{n_n})$ to $t_1^{n_1} \cdots t_n^{n_n}$.

We have a map

$$X^*(\mathrm{Diag}(n)) \times X_*(\mathrm{Diag}(n)) \to \mathbb{Z}, \tag{4.1.2}$$

defined by taking (χ, μ) to n if $(\chi \circ \mu)(z) = z^n$. $X_*(\mathrm{Diag}(n))$ is also an abelian group. Generally, the cocharacters (4.1.5) of $\mathrm{Diag}(n)$ have the form

$$z \xmapsto{\mu} \begin{pmatrix} z^{b_1} & & & \\ & z^{b_2} & & \\ & & \ddots & \\ & & & z^{b_n} \end{pmatrix} \qquad ((b_1, \dots, b_n) \in \mathbb{Z}^n).$$

<u>Fact</u>: $X_*(\mathrm{Diag}(n)) = \mathbb{Z}^n$. Going back to 4.1.2, we can think of this as

$$\begin{tikzcd} X^*(\mathrm{Diag}(n)) \arrow[d, equal] & \times & X_*(\mathrm{Diag}(n)) \arrow[d, equal] \arrow[r] & X^*(\mathrm{Diag}(1)) \arrow[d, equal] \\ \mathbb{Z}^n & & \mathbb{Z}^n & X_*(\mathrm{Diag}(n)) \arrow[d, equal] \\ & & & \mathbb{Z} \end{tikzcd} \tag{4.1.3}$$

defined by $(\chi, \mu) \mapsto \langle \chi, \mu \rangle$, being a bilinear map. The map above in turn induces maps

$$\langle \chi, - \rangle : X_*(\mathrm{Diag}(n)) \to X_*(\mathrm{Diag}(1)) \tag{4.1.4}$$

and

$$\langle -, \mu \rangle : X^*(\mathrm{Diag}(n)) \to X^*(\mathrm{Diag}(n)). \tag{4.1.5}$$

If the maps that sends χ to $\langle \chi, - \rangle$ and μ to $\langle -, \mu \rangle$ are isomorphisms, then we call this a **perfect pairing**. This definition of perfect pairing is a *generalization* of *non-degenerate* (bilinear form) from *fields* to *rings*.

Using the identifications exhibited in 4.1.3, we can reframe the previous paragraph as saying that map defined in 4.1.3 is a perfect pairing if the maps

$$L : \mathbb{Z}^n \to \mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z})$$

and

$$R : \mathbb{Z}^n \to \mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z})$$

are isomorphism, where, explicitly, we have

$$\chi \xmapsto{L} \langle \chi, - \rangle$$
$$\mu \xmapsto{R} \langle -, \mu \rangle.$$

We state the above more formally below.

Definition

Definition 4.1.6. Let M, N be *abelian groups*. Then a **pairing** $M \times N \to \mathbb{Z}$, defined explicitly as $(m, n) \mapsto \langle m, n \rangle$ is **perfect** if the homomorphisms

$$\begin{aligned} M &\to \operatorname{Hom}(N, \mathbb{Z}) = N^\vee \\ m &\mapsto \langle m, - \rangle \\ &= (n \mapsto \langle m, n \rangle) \end{aligned}$$

and

$$\begin{aligned} N &\to \operatorname{Hom}(M, \mathbb{Z}) = M^\vee \\ n &\mapsto \langle -, n \rangle \\ &= (m \mapsto \langle m, n \rangle) \end{aligned}$$

are *isomorphisms* of abelian groups (or equivalently, $\mathbb{Z}$-modules).

Definition

Definition 4.1.7. If abelian groups M, N are in *perfect pairing* (4.1.6) by $\langle -, - \rangle$, then we say that M, N are in **duality** by $\langle -, - \rangle$.

Let F be a field, and let V be an F-vector space of finite dimension. Then there is a perfect pairing

$$V \times V^\vee \to F$$

given by $(v, f) \mapsto f(v)$. In relation to this, we have a canonical isomorphism $V \cong V^{\vee\vee}$, while the isomorphism $V \cong V^\vee$ is not canonical, in the sense that it require us to *specify a basis* for V.

For the field case, we have that for all $v \in V$, we get $\langle v, - \rangle : V^\vee \to F$. If $v \neq 0$, then $\langle v, - \rangle \neq 0 \Rightarrow$ surjective (note here that $\langle v, - \rangle$ is defined as $V^\vee \ni f \mapsto f(v) \in F$). To see this, we can from a basis $\{e_1, \ldots, e_n\}$ for V construct a basis for $V^\vee$ as $\{e_1^\vee, \ldots, e_n^\vee\}$, where $e_i^\vee$ is defined on the basis of V as

$$e_i^\vee(e_j) = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j \end{cases} .$$

From this, we see that if

$$\begin{aligned} v &= \sum_{i=1}^n a_i e_i \\ &\neq 0, \end{aligned}$$

then there is some $a_i \neq 0$. Then it follows that

$$\begin{aligned} e_i^\vee(v) &= a_i \\ &n \neq 0, \end{aligned}$$

and $e_i^\vee \in V^\vee$, since for $v = \sum_{i=1}^{n} a_i e_i, w = \sum_{i=1}^{n} b_i e_i \in V$, we have

$$\begin{aligned} e_i^\vee(v+w) &= e_i^\vee\left(\sum_{i=1}^{n} a_i e_i + \sum_{i=1}^{n} b_i e_i\right) \\ &= e_i^\vee\left(\sum_{i=1}^{n} (a_i + b_i) e_i\right) \\ &= a_i + b_i \\ &= e_i^\vee(v) + e_i^\vee(w), \end{aligned}$$

and

$$\begin{aligned} e_i^\vee(a_i e_i) &= a_i \\ &= a_i \cdot 1 \\ &= a_i \cdot e_i^\vee(e_i). \end{aligned}$$

If we let $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be defined by $(a,b) \mapsto ab$, then let $v = 2$, so that we get $\langle v, - \rangle : \mathbb{Z} \to \mathbb{Z}$ defined by $a \mapsto 2a$, it is clear that this map is not surjective, but rather is $2\mathbb{Z}$.

Remark 4.1.8. The notes where a bit unclear here, since there first was an exhibited map $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $(a,b) \mapsto 2ab$. I failed to see the connection with the above paragraph. In the above paragraph, I guessed that the map $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $(a,b) \mapsto ab$ was the intended map (this was not spelled out in the notes).

$\mathsf{GL}(n)$ is a reductive group with subgroup $\mathrm{Diag}(n)$. We have seen (atleast mentioned) that it is the maximal commutative subgroup of $\mathsf{GL}(n)$. Out of this, we have

$$((X^*(\mathrm{Diag}(n)), \Phi; X_*(\mathrm{Diag}(n)), \Phi^\vee), \langle -, - \rangle)$$

with $\langle -, - \rangle : X^*(\mathrm{Diag}(n)) \times X_*(\mathrm{Diag}(n)) \to \mathbb{Z}$, taking (χ, μ) to $\langle \chi, \mu \rangle \in \mathbb{Z}$.

$$\Phi = \{e_i - e_j \mid 1 \leqslant i \neq j \leqslant n\}$$

are the non-zero characters in the root space. We have the decomposition $(e_i - e_j)(t) = \frac{t_i}{t_j}$.

$(e_i - e_j)$ defines a map $z \mapsto \mathrm{diag}(1, \ldots, 1, z, 1, \ldots, 1, z^{-1}, 1 \ldots, 1)$ with z in the i^{th} place and z^{-1} in the j^{th} place.

Cocharacter called the *coroot* of the root of $e_i - e_j$.

Definition

Definition 4.1.9.

$$(X^*(\mathrm{Diag}(n)), \Phi; X_*(\mathrm{Diag}(n)), \Phi^\vee), \langle -, - \rangle)$$

is called the **root datum** of the $\mathsf{GL}(n)$ relative to $\mathrm{Diag}(n)$.

Next time: Define the **root datum** example of $\mathrm{SL}(n)$. $\mathsf{GL}(n)$ and $\mathrm{SL}(n)$ have *the same* **root system**, but *different* **root data**.

Chapter 5

Lecture 5

Last time: X^* = characters,

$$\begin{aligned} X^*(\mathrm{Diag}(n)) &= \mathrm{Hom}(\mathrm{Diag}(n), \mathsf{GL}(1)) \\ &= \mathbb{Z}^n. \end{aligned}$$

More generally, if H is a group scheme (i.e. **group functor** given by *polynomial equations*) then $X^*(H) = \mathrm{Hom}(H, \mathsf{GL}(1))$ is the characters (4.1.4) of H.

Remark 5.0.1. In the above paragraph, H does not have to be *commutative*, but $X^*(H)$ can behave badly when H is not commutative.

Example 5.0.2. $X^*(\mathrm{SL}(n)) = 1$.

Example 5.0.3. If H is **simple** (and non-abelian), then $X^*(H) = 1$.

If $\chi \in X^*(H)$ so that we have $\chi : H \to \mathsf{GL}(1)$, then $\mathrm{im}(\chi) \supsetneqq 1$, so that $\ker \chi \subsetneqq H$. But $\ker \chi$ is a normal subgroup of H. If $\ker \chi = \{1\}$, then we have an isomorphic copy of H inside $\mathsf{GL}(1)$, but for fields F and commutative rings R, $\mathsf{GL}(1)$ is abelian, but H was non-abelian. Therefore the only choice is that $\ker \chi = H$, since we can not have proper normal subgroups of H.

Also last time:

$$\begin{aligned} X_*(\mathrm{Diag}(n)) &= \text{cocharacters} \\ &= \mathrm{Hom}(\mathsf{GL}(1), \mathrm{Diag}(n)) \\ &= \mathbb{Z}^n. \end{aligned}$$

More generally, for all group schemes H, we have $X_*(H) = \mathrm{Hom}(\mathsf{GL}(1), H)$.

Let $K \subset H$ be a **subgroup scheme**.

$$\begin{tikzcd} K(R) \arrow[r, hook] \arrow[d] & H(R) \arrow[d] \\ K(S) \arrow[r, hook] & H(S) \end{tikzcd} \qquad \forall R \to S$$

K is normal in H in the sense that $K(R) \triangleleft H(R)$ for all commutative rings R with unit.

Let $\mu_n(R) = \{r \in R \mid r^n = 1\}$ (recall n^{th} roots of unity). We have that $\mu_n \subseteq \mathrm{SL}(n)$ (scalar matrices), and that μ_n is normal and finite in $\mathrm{SL}(n)$. Furthermore, $\mu_n(R)$ is *finite* for all for all rings R with unit.

Remark 5.0.4. $\mathsf{SL}(n)$ has a lot of cocharacters. Every cocharacter of $\mathsf{SL}(n) \cap \mathrm{Diag}(n)$ gives a cocharacter of $\mathsf{SL}(n)$.

More generally, if $K \subset H$ is a subgroup (perhaps subgroup scheme?) $\rightsquigarrow X_*(K) \hookrightarrow X_*(H)$. We have diagrams

$$\begin{tikzcd} \mathsf{GL}(1) \arrow[r] \arrow[rr, bend right] & K \arrow[r, hook] & H \end{tikzcd}$$

and

$$\begin{tikzcd} K \arrow[d, hook] \arrow[dr] & \\ H \arrow[r, dotted, "?"'] & \mathsf{GL}(1) \end{tikzcd}$$

Question: Can we extend $\chi \in \mathrm{Hom}(K, \mathsf{GL}(1))$ to H?

Answer: Generally, no! But in some special settings, yes.

Example 5.0.5.

$$\begin{tikzcd} \mathrm{Diag}(n) \arrow[d, hook] \arrow[dr] & \\ \mathsf{GL}(n) \arrow[r, dotted, "?"'] & \mathsf{GL}(n) \end{tikzcd}$$

$\det : \mathsf{GL}(n) \to \mathsf{GL}(1)$ is a *character* (4.1.4) of $\mathsf{GL}(n)$.

Fact: $\mathbb{Z} \cong X^*(\mathsf{GL}(n))$ defined by $n \mapsto \det^n$. Every character of $\mathsf{GL}(n)$ is a *power* of det. So if χ *extends* from $\mathrm{Diag}(n)$ to $\mathsf{GL}(n) \Leftrightarrow \chi = \det^m$ for some $m \in \mathbb{Z}$:

$$\begin{tikzcd} \mathrm{Diag}(n) \arrow[d, hook] \arrow[dr, "\chi"] & \\ \mathsf{GL}(n) \arrow[r, "\tilde{\chi} = \det^m"'] & \mathsf{GL}(n) \end{tikzcd}$$

For all H, we have that $X^*(H)$ and $X_*(H)$ are *abelian groups* (not algebraic groups, just groups).

We have

$$\begin{aligned} \langle -, - \rangle : X^*(H) \times X_*(H) &\to \mathbb{Z} \\ (\chi, \mu) &\mapsto \langle \chi, \mu \rangle = m \qquad (\text{if } \chi \circ \mu = (z \mapsto z^m)). \end{aligned}$$

$$
\begin{tikzcd}
\mathsf{GL}(1) \arrow[r, "\mu"] \arrow[rr, bend right, "\chi\circ\mu"'] & H \arrow[r, "\chi"] & \mathsf{GL}(1),
\end{tikzcd}
$$

Note that

$$
\begin{aligned}
\operatorname{Hom}(\mathsf{GL}(1), \mathsf{GL}(1)) &= \mathbb{Z} \\
&= X^*(\mathrm{Diag}(1)) \\
&= X^*(\mathsf{GL}(1)) \\
&= X_*(\mathrm{Diag}(1)) \\
&= X_*(\mathsf{GL}(1)).
\end{aligned} \tag{5.0.1}
$$

Note that 5.0.1 is the map $(z \mapsto z^m) \longleftarrow m$ (in the direction $f : \mathbb{Z} \cong \operatorname{Hom}(\mathsf{GL}(1), \mathsf{GL}(1))$).

If $H = \mathrm{Diag}(n)$ then $\langle -, - \rangle$ is a **perfect pairing** (4.1.6), so that

$$
\begin{cases}
X^*(H) \cong \operatorname{Hom}(X_*(H), \mathbb{Z}) \\
X_*(H) \cong \operatorname{Hom}(X^*(H), \mathbb{Z}).
\end{cases}
$$

This fails for H simple, non-abelian (see 5.0.3).

Definition 5.0.6. A **free abelian group** G, is an abelian group *with a basis*. If it also is of **finite rank**, then it has a *finite* basis $B = \{g_1, \ldots, g_n\}$ so that

$$
\begin{aligned}
G &\cong \bigoplus_{i=1}^{n} g_i \mathbb{Z} \\
&\cong \mathbb{Z}^n.
\end{aligned}
$$

Definition

Definition 5.0.7. A **root datum** is a *quadruple* $(X^*, \Phi, X_*, \Phi^\vee)$ and a pairing $\langle -, - \rangle : X^* \times X_* \to \mathbb{Z}$ s.t. X^*, X_* are *free abelian groups of finite rank* (5.0.6), i.e. X^*, X_* are isomorphic to $\mathbb{Z}^n$ (as abelian groups) for some positive integer (if we want to avoid trivial root systems, I suppose) n (it is not specified that it has to be the same n for X_* and X^*, but we will see that further conditions below imposes that it is the same n).

- $\langle -, - \rangle$ is a *perfect* pairing (4.1.6). Which means that $X^* \cong (X_*)^\vee$ and $X_* \cong (X^*)^\vee$. But then we see that

$$\begin{aligned} X_* &\cong (X^*)^\vee \\ &\cong (\mathbb{Z}^n)^\vee \\ &= \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^n, \mathbb{Z}) \\ &\cong \mathbb{Z}^n \\ &\cong X^*, \end{aligned}$$

  so that $X_* \cong X^*$, and therefore the rank n of X_* and X^* are equal.
- Φ is a *finite* subset of X^*.
- $\Phi^\vee$ is a finite subset of X_*.
- There is a *bijection* from Φ to $\Phi^\vee$ realized by the map $\alpha \mapsto \alpha^\vee$, such that:
  (1) $\langle \alpha, \alpha^\vee \rangle = 2$;
  (2) $S_\alpha(\Phi) \subset \Phi$ and $S_{\alpha^\vee}(\Phi^\vee) \subset \Phi^\vee$, for all $\alpha \in \Phi$, where $S_\alpha : X^* \to X^*$ is defined by $x \mapsto x - \langle x, \alpha^\vee \rangle \alpha$ and $S_{\alpha^\vee} : X_* \to X_*$ is defined by $y \mapsto y - \langle \alpha, y \rangle \alpha^\vee$.

We call Φ the **roots** of the root datum, and $\Phi^\vee$ the **coroots** of the root datum, and S_α and $S_{\alpha^\vee}$ are called the **root reflections** and **coroot reflections**, respectively, where

- S_α is a reflection of $X^* \otimes_{\mathbb{Z}} \mathbb{Q}$;
- $S_{\alpha^\vee}$ is a reflection of $X_* \otimes_{\mathbb{Z}} \mathbb{Q}$.

If $v_1, \ldots, v_n$ is a *minimal generating set* for X^*, then

$$X^* = \left\{ \sum_{i=1}^n a_i v_i \;\middle|\; a_i \in \mathbb{Z} \right\},$$

and

$$X^* \otimes_{\mathbb{Z}} \mathbb{Q} = \left\{ \sum_{i=1}^n a_i v_i \;\middle|\; a_i \in \mathbb{Q} \right\}.$$

Example 5.0.8 ($\mathsf{GL}(n)$)**.** Let

- $X^* = X^*(\mathrm{Diag}(n))$ and $X_* = X_*(\mathrm{Diag}(n))$.
- $\Phi = \{e_i - e_j \mid i \neq j\}$ and $\Phi^\vee = \{e_i - e_j \mid i \neq j\}$.
- $\langle -, - \rangle$ be the pairing between the characters (4.1.4) and the cocharacters (4.1.5), so

$$\langle -, - \rangle : \mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{Z}$$

  is the standard dot-product.
- $(e_i - e_j)^\vee = e_i - e_j$.

Example 5.0.9 ($\mathsf{SL}(n)$)**.** Replace M_n for $\mathsf{GL}(n)$ in 5.0.8, with $M_n^\circ = \{A \in M_n \mid \mathrm{tr}\ A = 0\}$, i.e. $M_n^\circ \subset M_n$ are the *traceless* matrices in M_n. $M_n^\circ(F)$ is a sub-vector space of $M_n(F)$, and furthermore, M_n° is a sub-vector functor of M_n.

We have an action $\mathsf{SL}(n) \curvearrowright M_n^\circ$ by conjugation. M_n° is *stable* under conjugation by $\mathsf{SL}(n)$; i.e. we have

$$\mathsf{SL}(n) \times M_n^\circ \ni (g, A) \mapsto gAg^{-1},$$

where we note that

$$\begin{aligned}\operatorname{tr}(gAg^{-1}) &= \operatorname{tr}(g(Ag^{-1}))\\ &= \operatorname{tr}(g(g^{-1}A))\\ &= \operatorname{tr}(A)\\ &= 0,\end{aligned}$$

so that $gAg^{-1} \in M_n^\circ$, where we have used *associativity* of matrix multiplication together with the fact that $\operatorname{tr}(AB) = \operatorname{tr}(BA)$.

We replace $\operatorname{Diag}(n)$ with

$$\begin{aligned}\operatorname{Diag}^1(n) &= \{t \in \operatorname{Diag}(n) \mid \det t = 1\}\\ &= \left\{ \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix} \in \operatorname{Diag}(n) \,\middle|\, \prod_{i=1}^n t_i = 1 \right\}\\ &\cong \operatorname{Diag}(n-1).\end{aligned} \tag{5.0.2}$$

The isomorphism 5.0.2 from $\operatorname{Diag}^1(n)$ to $\operatorname{Diag}(n-1)$ is realized explicitly as

$$\begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix} \mapsto \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_{n-1} \end{pmatrix}$$

We then restrict the action $\mathsf{SL}(n) \curvearrowright M_n^\circ$ to $\operatorname{Diag}^1(n) \curvearrowright M_n^\circ$ (recall, action by conjugation). The computations for $\mathsf{GL}(n)$ case then shows that

$$M_n^\circ = \operatorname{diag}^\circ(n) \oplus \bigoplus_{i \neq j} \operatorname{span}(E_{ij}),$$

the eigenvalue-decomposition ("e-space decomposition"), where

$$\begin{aligned}\operatorname{diag}^\circ(n) &= \operatorname{diag}(n) \cap M_n^\circ\\ &= \left\{ t = \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix} \,\middle|\, \sum_{i=1}^n t_i = 0 \right\}\end{aligned} \tag{5.0.3}$$

Remark 5.0.10. Note that elements in $\operatorname{diag}^\circ(n)$ (5.0.3) are not necessarily *invertible*.

We have

$$M_n^\circ = \operatorname{diag}^\circ(n) \oplus \bigoplus_{i \neq j} \operatorname{span}(E_{ij}),$$

which is the root-space decomposition for $\mathsf{SL}(n)$.

We have

$$t = \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & \ddots & \\ & & & t_n \end{pmatrix}$$

such that

$$\begin{aligned} t * E_{ij} &= tE_{ij}t^{-1} \\ &= \frac{t_i}{t_j} \cdot E_{ij} \\ &= (e_i - e_j)(t) \cdot E_{ij}, \end{aligned}$$

where $*$ is action by *conjugation*.

We define $(e_i - e_j)^\vee = e_i - e_j$. For root datum (5.0.7), we need X^*, X_* (?).

In general, if $\varphi : K \to H$ is a *homomorphism of group schemes*, then $\varphi^* : X^*(H) \to X^*(K)$ is a *homomorphism of character groups* (note the *contravariant* relation), where we by φ^* mean the pullback, in the sense that φ^* takes $\chi \in X^*(H)$ to $\chi \circ \varphi \in X^*(K)$ (since X^* is **to** $\mathsf{GL}(1)$; 4.1.4).

Our Setting:

$$\begin{aligned} \mathrm{Diag}^1(n) &\xhookrightarrow{\varphi} \mathrm{Diag}(n) \\ \rightsquigarrow X^*(\mathrm{Diag}(n)) &\xhookrightarrow{\varphi^*} X^*(\mathrm{Diag}^1(n)). \end{aligned}$$

Question: What is the kernel of φ^*?

Note here that φ is just the canonical injection of $\mathrm{Diag}^1(n)$ into $\mathrm{Diag}(n)$.

Answer: Recall that $X^*(\mathrm{Diag}(n)) \cong \mathbb{Z}^n$. Further, since for all $t \in \mathrm{Diag}^1(n)$ we have that $\det t = 1$, we must have (since $\det(AB) = \det(A)\det(B)$) that $\det(t^m) = 1$. We also see that t is invertible, and since $\det t = 1$ we must have $\det t^{-1} = 1 \Rightarrow \det t^{-m} = 1$ (again, by $\det(AB) = \det(A)\det(B)$). Therefore, we have that $\lambda(1, \ldots, 1) \subset \ker \varphi^*$ for $\lambda \in \mathbb{Z}$.

We note that φ^* is surjective, since φ is injective. More explicitly, any character of $X^*(\mathrm{Diag}^1(n))$ can be seen as the *restriction* of a character of $X^*(\mathrm{Diag}(n))$ to $\mathrm{Diag}^1(n)$.

Recall that we generally think of the t_i in $\mathrm{Diag}^1(n) \subset \mathrm{Diag}(n)$ as coming from $F^\times$ where F is an *infinite field*. But then we see that if $\kappa \in X^*(\mathrm{Diag}(n))$ such that $\varphi^*(\kappa) = \kappa \circ \varphi \in X^*(\mathrm{Diag}^1(n))$ is the *trivial* map, then, since under the identification $X^*(\mathrm{Diag}(n)) \cong \mathbb{Z}^n$, we must have that $\kappa \circ \varphi$ is a map on the form $t = \mathrm{diag}(t_1, \ldots, t_n) \mapsto t_1^{\alpha_1} \cdots t_n^{\alpha_n}$. But note that $\mathrm{diag}(t, 1, \ldots, 1, t^{-1}) \in \mathrm{Diag}^1(n)$, and so any other diagonal matrix with t, t^{-1} in the i^{th} and j^{th} place and 1s everywhere else. If $\alpha_i \neq \alpha_j$ for some $i \neq j$, assume without loss of generality that $\alpha_i > \alpha_j$. Then we see that the element $\mathrm{diag}(1, \ldots, \underbrace{t}_{i^{\text{th}}}, \ldots, \underbrace{t^{-1}}_{j^{\text{th}}}, \ldots, 1)$ is taken to

$$\begin{aligned} t^{\alpha_i} \cdot (t^{-1})^{\alpha_j} &= t^{\alpha_i} \cdot t^{-\alpha_j} \\ &= t^{\alpha_i - \alpha_j} \\ &\neq 1, \end{aligned}$$

if t is *not* an $(\alpha_i - \alpha_j)^{\text{th}}$ *root of unity*. Since there are only n such elements, we can just choose t to be any of an infinite number of non-roots of unity, to see that this will not be satisfied. From this reasoning applied to any $1 \leqslant i, j \leqslant n$ and non-root of unity $t \in F^\times$, we see that $\kappa \circ \varphi$ must be on the form $\alpha_1 = \ldots = \alpha_n$. Therefore, we conclude that $\{(\lambda, \ldots, \lambda) \mid \lambda \in \mathbb{Z}\} = \ker \varphi^*$.

We have a *short exact sequence*

$$1 \longrightarrow \mathrm{Diag}^1(n) \hookrightarrow \mathrm{Diag}(n) \twoheadrightarrow \mathsf{GL}(1) \longrightarrow 1$$

where the map $\mathrm{Diag}(n) \twoheadrightarrow \mathsf{GL}(1)$ is det. It follows that $\mathrm{Diag}^1(n)/\mathrm{Diag}(n) \cong \mathsf{GL}(1)$. Upon applying $X^* = \mathrm{Hom}(-, \mathsf{GL}(1))$ (contravariant **functor**), we get, since $\mathsf{GL}(1)$ (generally this is true only if $\mathsf{GL}(1)$ is an *injective* module),

$$0 \longrightarrow X^*(\mathsf{GL}(1)) \longrightarrow X^*(\mathrm{Diag}(n)) \longrightarrow X^*(\mathrm{Diag}^1(n)) \longrightarrow 0,$$

but as pointed out before, an exact sequence

$$1 \longrightarrow K \longrightarrow H \longrightarrow Q \longrightarrow 1$$

does not give an exact sequence

$$0 \longrightarrow X^*(Q) \longrightarrow X^*(H) \longrightarrow X^*(K) \longrightarrow 0,$$

in general.

We have

$$\begin{aligned} X^*(\mathrm{Diag}^1(n)) &= \mathbb{Z}^n / \langle (1, \ldots, 1) \rangle \\ &\cong \mathbb{Z}^{n-1}. \end{aligned}$$

and

$$\begin{aligned} X_*(\mathrm{Diag}^1(n)) &\cong \mathbb{Z}_0^n \\ &= \left\{ \sum_{i=1}^n b_i = 0 \;\middle|\; b_i \in \mathbb{Z} \right\}. \end{aligned}$$

$$\begin{tikzcd} \mathsf{GL}(1) \arrow[rr, "\mu"] \arrow[drr, dashed, "\text{for which?}"'] & & \mathrm{Diag}(n) \\ & & \mathrm{Diag}^1(n) \arrow[u, hook] \end{tikzcd}$$

$$z \xmapsto{(b_1, \ldots, b_n)} \begin{pmatrix} z^{b_1} & & & \\ & z^{b_2} & & \\ & & \ddots & \\ & & & z^{b_n} \end{pmatrix},$$

will lead in to $\mathrm{Diag}^1(n)$, for all $R \Leftrightarrow z^{b_1 + \ldots + b_n} = 1 \Leftrightarrow b_1 + \ldots + b_n = 0$ (this should hold for all rings R, but some rings have no non-trivial roots of unity, which I suppose is why we impose $b_1 + \ldots + b_n = 0$).

Example 5.0.11 (Root datum for $\mathsf{SL}(n)$)**.** $(X^*(\mathrm{Diag}^1(n), \{e_i - e_j\}; X_*(\mathrm{Diag}^1(n)), \{e_i - e_j\})$. If we view $X^*(\mathrm{Diag}^1(n))$ as $\mathbb{Z}^n/\langle(1,\ldots,1)\rangle$ then $e_i - e_j$ is viewed as $e_i - e_j + \langle(1,\ldots,1)\rangle$, i.e. as a coset element in $\mathbb{Z}^n/\langle(1,\ldots,1)\rangle$.

$$\langle -, - \rangle : \mathbb{Z}^n/\langle(1,\ldots,1)\rangle \times \mathbb{Z}^n_0 \to \mathbb{Z} \qquad \text{(perfect pairing; 4.1.6)}.$$

This is <u>well-defined</u>:

$$\begin{aligned} \langle (a_1,\ldots,a_n) + (m,\ldots,m), (b_1,\ldots,b_n)\rangle &= \sum_{i=1}^n a_i b_i + m \cdot \underbrace{\sum_{i=1}^n b_i}_{=0} \\ &= \sum_{i=1}^n a_i b_i. \end{aligned}$$

Definition

Definition 5.0.12 (Projective Linear Group)**.** $\mathsf{PGL}(n) := \mathsf{GL}(n)/\{\lambda I\}$.

$$\begin{tikzcd} \mathsf{GL}(1) \arrow[r, "\mu"] \arrow[dr] & \mathsf{GL}(n) \arrow[d, "\pi"] \\ & \mathsf{PGL}(n) \end{tikzcd}$$

Definition

Definition 5.0.13.

$$\begin{aligned} \mathsf{PDiag}(n) &= \mathrm{Diag}(n)/\{\lambda I\} \\ &\cong \mathrm{Diag}(n-1), \end{aligned}$$

with character group $X^*(\mathsf{PDiag}(n)) \cong \mathbb{Z}^n_0$.

There is an action $\mathsf{PDiag}(n) \curvearrowright M_n^\circ$.

$$\begin{tikzcd} \mathsf{GL}(1) \arrow[r, "\mu"] \arrow[dr] & \mathsf{GL}(n) \arrow[d, two heads, "\pi"] \\ & \mathsf{PGL}(n) \end{tikzcd}$$

$$
\begin{tikzcd}
\mathrm{Diag}(n) \arrow[r, "\chi=(a_1,\ldots,a_n)"] \arrow[d, two heads] & \mathsf{GL}(1) \\
\mathsf{PDiag}(n) \arrow[ur, "?"'] &
\end{tikzcd}
$$

$\{\lambda I\} \subset \ker\chi$, since we assume that $(a_1, \ldots, a_n) \in \mathbb{Z}_0^n$ so that $a_1 + \ldots + a_n = 0$, therefore,

$$
\begin{aligned}
\chi(\lambda I) &= \lambda^{a_1} \cdots \lambda^{a_n} \\
&= \lambda^{a_1+\ldots+a_n} \\
&= \lambda^0 \\
&= 1.
\end{aligned}
$$

$$
\begin{tikzcd}
\mathsf{GL}(1) \arrow[r] \arrow[dr] & \mathrm{Diag}(n) \arrow[d, two heads, "\pi"] \\
& \mathsf{PDiag}(n)
\end{tikzcd}
$$

$\rightsquigarrow X_*(\mathrm{Diag}(n)) \twoheadrightarrow X_*(\mathsf{PDiag}(n))$.

$$
\begin{aligned}
X_*(\mathsf{PDiag}(n)) &= X^*(\mathrm{Diag}^1(n)) \\
&= \mathbb{Z}^n/(\langle 1, \ldots, 1\rangle)
\end{aligned}
$$

$$
\begin{aligned}
\lambda I = \begin{pmatrix} \lambda & & & \\ & \lambda & & \\ & & \ddots & \\ & & & \lambda \end{pmatrix} &\xmapsto{(a_1,\ldots,a_n)\in\mathbb{Z}^n} \lambda^{a_1} \cdots \lambda^{a_n} \\
= 1 \qquad &(\text{if } a_1 + \ldots + a_n = 0).
\end{aligned}
$$

Example 5.0.14 (A root datum for $\mathsf{PGL}(n)$.)**.**

$$
\left(X^*(\mathsf{PDiag}(n)), \{e_i - e_j \mid 1 \leqslant i \neq j \leqslant n\}; X_*(\mathsf{PDiag}(n)), \{e_i - e_j \mid 1 \leqslant i \neq j \leqslant n\}\right),
$$

where we recall that

$$
\begin{aligned}
X^*(\mathsf{PDiag}(n)) &\cong \mathbb{Z}_0^n, \\
X_*(\mathsf{PDiag}(n)) &\cong \mathbb{Z}^n/\langle(1, \ldots, 1)\rangle.
\end{aligned}
$$

We have a pairing

$$\mathbb{Z}_0^n \times \mathbb{Z}^n/\langle(1,\dots,1)\rangle \to \mathbb{Z},$$

reverse from the pairing on the *root* datum on $\mathsf{SL}(n)$ (cf. 5.0.11).

In general, if $(X^*,\Phi;X_*,\Phi^\vee)$ is a root datum (5.0.7), the so is its **dual**.

Definition

Definition 5.0.15. If $(X^*,\Phi;X_*,\Phi^\vee)$ is a *root datum* (5.0.7), then we define the **dual root datum** as

$$(X_*,\Phi^\vee;X^*,\Phi),$$

that is, we exchange the place of the *characters* and *cocharacters*, and exchange the *roots* and *coroots*.

By comparing the examples of root datum for $\mathsf{SL}(n)$ and $\mathsf{PGL}(n)$ (5.0.11 and 5.0.14) we see that they are dual, since they have the same roots = coroots, and the characters of $\mathsf{SL}(n)$ are the cocharacters of $\mathsf{PGL}(n)$, and the cocharacters of $\mathsf{SL}(n)$ are the characters of $\mathsf{PGL}(n)$.

If $(X^*,\Phi;X_*,\Phi^\vee)$ is a root datum, then

$$\begin{cases}\left(\operatorname{span}_{\mathbb{Q}}(\Phi),\Phi\right)\\ \left(\operatorname{span}_{\mathbb{Q}}(\Phi^\vee),\Phi^\vee\right)\end{cases}$$

are both root systems (2.0.1). The root systems of $\mathsf{SL}(n),\mathsf{GL}(n)$ and $\mathsf{PGL}(n)$ are all *isomorphic* to $(\mathbb{Q}_0^n,\{e_i-e_j \mid 1\leqslant i\neq j\leqslant n\})$ of type A_{n-1}, but their <u>root data</u> (i.e. their respective <u>root datum</u>) are pairwise *non-isomorphic*.

With regards to their **Lie Algebras**, we have that

$$\begin{aligned}\operatorname{Lie}(\mathsf{SL}(n)) &= \operatorname{Lie}(\mathsf{PGL}(n))\\ &= M_n^\circ,\end{aligned}$$

and

$$\operatorname{Lie}(\mathsf{GL}(n)) = M_n.$$

Summarizing, we can say that the root datum is *finest* (in distinguishing algebraic groups, I presume), Lie algebras are coarser, and root *systems* is coarser.

Chapter 6

Lecture 6: More on root data and Lie Algebras

Recall the following examples of root datums for algebraic groups $\mathsf{GL}(n), \mathsf{SL}(n), \mathsf{PGL}(n)$.

Example 6.0.1 ($\mathsf{GL}(n)$)**.**

$$\left(\mathbb{Z}^n, \Phi_{\mathsf{A}}^{n-1}; \mathbb{Z}^n, \Phi_{\mathsf{A}}^{n-1}\right).$$

Example 6.0.2 ($\mathsf{SL}(n)$)**.**

$$\left(\mathbb{Z}^n/\langle(1,\ldots,1)\rangle, \Phi_{\mathsf{A}}^{n-1}; \mathbb{Z}_0^n, \Phi_{\mathsf{A}}^{n-1}\right).$$

Example 6.0.3 ($\mathsf{PGL}(n)$)**.**

$$\left(\mathbb{Z}_0^n, \Phi_{\mathsf{A}}^{n-1}; \mathbb{Z}^n/\langle(1,\ldots,1)\rangle, \Phi_{\mathsf{A}}^{n-1}\right).$$

In general, if $(X^*, \Phi; X_*, \Phi^\vee)$ is a *root datum* (5.0.7) for a group G, then "the" *root system* (2.0.1) of G up to isomorphism is $\left(\operatorname{span}_{\mathbb{Q}}(\Phi), \Phi\right)$. The root system $\left(\operatorname{span}_{\mathbb{Q}}(\Phi^\vee), \Phi^\vee\right)$ might *not* be isomorphic to $\left(\operatorname{span}_{\mathbb{Q}}(\Phi), \Phi\right)$.

Example 6.0.4. If $\left(\operatorname{span}_{\mathbb{Q}}(\Phi), \Phi\right)$ is of *type* B_n (and C_n, respectively), where we recall that a root system of type B_n is of the form

$$\Phi_{\mathsf{A}}^{n-1} \bigsqcup \{\pm(e_i + e_j) \mid 1 \leqslant i \neq j \leqslant n\} \bigsqcup \{\pm e_i \mid 1 \leqslant i \leqslant n\},$$

and a root system of type C_n is of the form

$$\Phi_{\mathsf{A}}^{n-1} \bigsqcup \{\pm(e_i + e_j) \mid 1 \leqslant i \neq j \leqslant n\} \bigsqcup \{2e_i \mid 1 \leqslant i \leqslant n\}.$$

Then $\left(\operatorname{span}_{\mathbb{Q}}(\Phi^\vee), \Phi^\vee\right)$ is of type C_n, and type B_n, respectively. We have that $\mathsf{B}_n \cong \mathsf{C}_n \Leftrightarrow n = 2$.

Remark 6.0.5. Note here that $\Phi^\vee = \{\alpha^\vee \mid \alpha \in \Phi\}$. The only roots that change when we dualize the system of type B_n is that the roots of the form $\pm e_i$ gets sent to

$$\begin{aligned} \pm e_i^\vee &= \frac{2 \cdot (\pm e_i)}{\langle e_i, e_i \rangle} \\ &= 2(\pm e_i) \\ &= \pm 2e_i. \end{aligned}$$

If we instead dualize a root system of type C_n, the only roots that change (are not invariant under dualization), are the roots of the form $\pm 2e_i$, which gets sent to

$$\begin{aligned}(\pm 2e_i)^\vee &= \frac{2\cdot(\pm 2e_i)}{\langle \pm 2e_i, \pm 2e_i\rangle} \\ &= \frac{\pm 4e_i}{4} \\ &= \pm e_i.\end{aligned}$$

This explains why, as pointed out above, we have

$$\mathsf{B}_n \overset{(-)^\vee}{\longleftrightarrow} \mathsf{C}_n.$$

Definition

Definition 6.0.6. Let k be an *algebraically closed field* (e.g. $K = \mathbb{C}$). We define a **Torus** over k as a *group scheme* T over k, such that

$$T \cong \mathrm{Diag}(n),$$

for some $n \geqslant 0$.
Over k, we have that $T : \mathbf{CAlg}_k \to \mathbf{Grp}$, i.e. T is acts as a **group functor**, where $\mathbf{CAlg}_k$ is the *category* of commutative k-algebras. In fact, the isomorphism $T \cong \mathrm{Diag}(n)$ can be written as $\alpha : T \Rightarrow \mathrm{Diag}(-, n)$, i.e. as a natural isomorphism. This means that for every morphism $f : R \to S$ of commutative k-algebras (i.e. $f \in \mathrm{Mor}(\mathbf{CAlg_k})$), the following diagram commutes.

$$\begin{tikzcd} R \arrow[d, "f"] & \rightsquigarrow & T(R) \arrow[r, "\alpha_R"] \arrow[d, "T(f)"] & \mathrm{Diag}(n, R) \arrow[d, "\mathrm{Diag}(n,f)"] \\ S & & T(S) \arrow[r, "\alpha_S"'] & \mathrm{Diag}(n, S) \end{tikzcd}$$

where α_R, α_S are the **components** of α at R, S, respectively.

Definition

Definition 6.0.7. If F is a not necessarily algebraically closed field, then a **Torus over** F is a *group scheme* T such that $T \cong \mathrm{Diag}(n)$ *after extending* F to some algebraically closed field k *containing* F, i.e. *a field extension* $k \supset F$.

Definition

Definition 6.0.8. T/F means "T over F" means we have

$$\{\mathbf{F}\text{-alg}\} \xrightarrow[T]{} \{\text{groups}\}.$$

If $k \supseteq F$, then

$$\{\mathbf{k}\text{-alg}\} \xrightarrow[T_k]{} \{\text{groups}\}.$$

Using the language of Tori: We have proved (have we?) that $\mathrm{Diag}(n)$ is a *maximal* torus of $\mathsf{GL}(n)$, i.e. it is a torus and if $\mathrm{Diag}(n) \subset T \subset \mathsf{GL}(n)$ where T is a torus, then $T = \mathrm{Diag}(n)$, since $\mathrm{Diag}(n)$ is a *maximal commutative* subgroup.

For $\mathsf{GL}(n)$ we have that maximal commutative = maximal torus (6.0.6). For general G (e.g. $\mathrm{SO}(m)$) there can be maximal commutative subgroups *other than maximal tori.*

In general, a root datum (5.0.7) is associated to (G,T) where G is *connected* and *reductive* (two words to be defined), and T is a maximal torus in G.

Remark 6.0.9. By definition, **maximal torus** makes sense in any group scheme.

Definition

Definition 6.0.10. Let $\mathcal{J} \in \mathsf{GL}(n)$. Then we define $\mathrm{SO}^{\mathcal{J}}(n) := \{A \in \mathsf{SL}(n) \mid A^T \mathcal{J} A = \mathcal{J}\}$.

Example 6.0.11 ($\mathsf{SO}^{\mathcal{J}}(2n)$)**.** Take $\mathsf{SO}^{\mathcal{J}}(2n)$, where

$$\mathcal{J} = \begin{pmatrix} & & & & 1 \\ & & & 1 & \\ & & \iddots & & \\ & 1 & & & \\ 1 & & & & \end{pmatrix},$$

(from exercise sessions). We have that

$$\mathrm{Diag}(2n) \cap \mathsf{SO}^{\mathcal{J}}(2n) = \left\{ \begin{pmatrix} t_1 & & & & & \\ & \ddots & & & & \\ & & t_n & & & \\ & & & t_n^{-1} & & \\ & & & & \ddots & \\ & & & & & t_1^{-1} \end{pmatrix} \right\}$$

is a maximal torus (6.0.6), since it is a torus and maximal commutative. Furthermore, there is an isomorphism from $\mathrm{Diag}(2n) \cap \mathsf{SO}^{\mathcal{J}}(2n)$ to $\mathrm{Diag}(n)$ $\psi : \mathrm{Diag}(2n) \cap \mathsf{SO}^{\mathcal{J}} \to \mathrm{Diag}(n)$ realized explicitly as

$$\begin{pmatrix} t_1 & & & & & \\ & \ddots & & & & \\ & & t_n & & & \\ & & & t_n^{-1} & & \\ & & & & \ddots & \\ & & & & & t_1^{-1} \end{pmatrix} \xmapsto{\psi} \begin{pmatrix} t_1 & & \\ & \ddots & \\ & & t_n \end{pmatrix}.$$

As a *function*, it is easy to see that it is a bijection, since it is clear that any matrix in $\mathrm{Diag}(2n) \cap \mathsf{SO}^{\mathcal{J}}$ is determined by $t_1, \ldots, t_n$. It is also easy to see that ψ extends naturally to a group-homomorphism, so is indeed a group isomorphism.

Example 6.0.12 ($\mathsf{SL}(n)$)**.** $\mathrm{Diag}^1(n) = \mathsf{SL}(n) \cap \mathrm{Diag}(n)$ is a maximal torus in $\mathsf{SL}(n)$.

Example 6.0.13 ($\mathsf{PGL}(n)$)**.** $\mathsf{PDiag}(n) = \pi(\mathrm{Diag}(n))$ where $\pi : \mathsf{GL}(n) \twoheadrightarrow \mathsf{GL}(n)/\{\lambda I \mid \lambda \neq 0\} = \mathsf{PGL}(\mathsf{n})$ is the canonical projection map. Then $\mathsf{PDiag}(n)$ is a maximal torus in $\mathsf{PGL}(n)$.

Example 6.0.14. <u>Scalars</u>, i.e. $\{\lambda I \mid \lambda \neq 0\}$ is a non-maximal torus in for all $n \geqslant 2$. Furthermore, we have that

$$\begin{aligned}\{\lambda I \mid \lambda \neq 0\} &\cong \mathsf{GL}(1)\\ &\cong \mathrm{Diag}(1)\\ &\subsetneqq \mathrm{Diag}(n) \qquad (\text{for } n \geqslant 2).\end{aligned}$$

If $g \in \mathsf{GL}(n)$, then $g\mathrm{Diag}(n)g^{-1}$ is a maximal torus in $\mathsf{GL}(n)$.

Going back to 6.0.1, 6.0.1, 6.0.3, we have that

$$\mathrm{span}_{\mathbb{Q}}(\Phi_{\mathsf{A}}^{n-1}) = \mathbb{Q}_0^n. \tag{6.0.1}$$

Furthermore,

$$\Delta = \{e_1 - e_2, e_2 - e_3, \dots, e_{n-1} - e_n\}$$

generates Φ_{A}^{n-1}, i.e. every $\alpha \in \Phi_{\mathsf{A}}^{n-1}$ is a *linear combination* of elements of Δ with $\mathbb{Z}$-coefficients. Note here that we can write $e_i - e_j$ for for $i < j$ as a "telescoping sum"

$$e_i - e_j = (e_i - e_{i+1}) + (e_{i+1} - e_{i+2}) + \ldots + (e_{j-1} - e_j) \tag{6.0.2}$$

where all coefficients are 0 (those not seen from Δ, in 6.0.2) and 1. Δ is a basis for $\mathbb{Q}_0^n$.

For $\mathsf{SL}(n)$ and $\mathsf{PGL}(n)$ we have $X_{\mathbb{Q}}^* := \mathrm{span}_{\mathbb{Q}}\Phi$, and $X_{*,\mathbb{Q}} = \mathrm{span}_{\mathbb{Q}}\Phi^{\vee}$. So that $X_{\mathbb{Q}}^* = \mathbb{Q}_0^n$, since $\Phi = \Phi_{\mathsf{A}}^{n-1}$ for $\mathsf{SL}(n)$ and $\mathsf{PGL}(n)$, together with 6.0.1. The *image* of $\mathrm{span}_{\mathbb{Q}}(\Phi_{\mathsf{A}}^{n-1})$ in $\mathbb{Q}^n/\mathrm{span}\{(1,\dots,1)\}$ is the whole space. We have that $\mathbb{Q}_0^n \cap \mathrm{span}\{(1,\dots,1)\} = \{0\}$. Furthermore, we have the following diagram.

$$\begin{tikzcd}
\mathbb{Q} \arrow[r, two heads, "\text{linear map}"] & \mathbb{Q}/\mathrm{span}\{(1,\dots,1)\} \\
\mathbb{Q} \arrow[u, hook] \arrow[ur, "\sim"'] &
\end{tikzcd}$$

But $X_{\mathbb{Q}}^* \supsetneqq \mathrm{span}_{\mathbb{Q}}(\Phi) = \mathbb{Q}_0^n$.

Remark 6.0.15. Under the assumption that we by $X_{\mathbb{Q}}^*$ mean $X^* \otimes_{\mathbb{Z}} \mathbb{Q}$, the explanation for why we have $X_{\mathbb{Q}}^* = \mathbb{Q}_0^n$ for $\mathsf{SL}(n)$ and $\mathsf{PGL}(n)$ but *not* for $\mathsf{GL}(n)$, is the following:

Note that both $\mathbb{Z}_0^n$ and $\mathbb{Z}^n/\langle(1,\dots,1)\rangle$ are isomorphic to $\mathbb{Z}^{n-1}$. We have that

$$\begin{aligned}X_{\mathbb{Q}}^* &\cong \mathbb{Z}^{n-1} \otimes_{\mathbb{Z}} \mathbb{Q}\\ &\cong \mathbb{Q}^{n-1}\\ &\cong \mathbb{Q}_0^n,\end{aligned}$$

(where we in the second equality used the canonical isomorphisms for the tensor product, i.e. that $R \otimes_R A \cong A$ for A an R-module, and that $(R \oplus R) \otimes_R A \cong (R \otimes_R A) \oplus (R \otimes_R A)$). On the other hand, we have that the character group X^* for $\mathsf{GL}(n)$ is isomorphic to $\mathbb{Z}^n$. Then we have

$$\begin{aligned}X_{\mathbb{Q}}^* &\cong \mathbb{Z}^n \otimes_{\mathbb{Z}} \mathbb{Q}\\ &\cong \mathbb{Q}^n\\ &\ncong \mathbb{Q}^{n-1}\\ &\cong \mathbb{Q}_0^n\\ \Rightarrow X^* &\ncong \mathbb{Q}_0^n,\end{aligned}$$

where we again used the canonical isomorphisms for tensor products described in the previous paragraph.

Example 6.0.16 ($n = 2$)**.** If we look at $\mathsf{SL}(2)$ and $\mathsf{PGL}(2)$, then we have the following root datum, for $\mathsf{SL}(2)$:

$$\left(\mathbb{Z}^2/\langle(1,1)\rangle, \Phi^1_{\mathsf{A}}, \mathbb{Z}^2_0, \Phi^1_{\mathsf{A}}\right).$$

Question I: Does Φ^{n-1}_{A} span $\mathbb{Z}^n_0$ (or perhaps, we restrict to looking explicitly at $\mathbb{Z}^2_0$) over $\mathbb{Z}$. **Question II**: Is $\mathbb{Z}^n_0 = \operatorname{span}_{\mathbb{Z}} \Phi^{n-1}_{\mathsf{A}}$?

Answer I: For $n = 2$, we have $\mathbb{Z}^2_0 = \{(a, -a) \mid a \in \mathbb{Z}\}$, where $(a, -a) = a(e_1 - e_2)$. Is $\mathbb{Z}^2/\langle(1,1)\rangle$ spanned by $(1,-1)+\langle(1,1)\rangle$? No, because $(1,0)+\langle(1,1)\rangle$ is not in the $\mathbb{Z}$-span, since the sum of entries is *odd*/entries of different parity. To say a bit more, note that $(a,b) \sim (c,d) \in \mathbb{Z}^2/\langle(1,1)\rangle \Leftrightarrow (a-c, b-d) = \lambda(1,1)$ for some $\lambda \in \mathbb{Z}$. We want to answer whether or not, for every $(a,b)+\langle(1,1)\rangle \in \mathbb{Z}^2/\langle(1,1)\rangle$ there is some $\lambda \in \mathbb{Z}$ such that

$$\begin{aligned} \lambda(1,-1) + \langle(1,1)\rangle &= (a,b) + \langle(1,1)\rangle \\ \Leftrightarrow ((\lambda,-\lambda) - (a,b)) + \langle(1,1)\rangle &= 0 + \langle(1,1)\rangle \\ \Leftrightarrow (\lambda - a, -\lambda - b) &= (k,k), \qquad (k, \lambda \in \mathbb{Z}). \end{aligned}$$

This means that

$$\begin{cases} \lambda - a &= k \\ -\lambda - b &= k \end{cases}$$

Let $a = 1$ and $b = 0$. Then we have

$$\begin{cases} \lambda - 1 &= k \\ -\lambda &= k, \end{cases} \tag{6.0.3}$$

it follows by adding the second row to the first in 6.0.3 that $-1 = 2k$, which is impossible, since $k \in \mathbb{Z}$.

Answer II: For the case of $\mathbb{Z}^2_0$, we see that $(a,-a) = a(e_1 - e_2)$, and $e_1 - e_2 \in \Phi^1_{\mathsf{A}}$ and $a \in \mathbb{Z}$, so clearly $\subseteq \mathbb{Z}^2_0 \subseteq \operatorname{span}_{\mathbb{Z}} \Phi^1_{\mathsf{A}}$. On the other hand, $\operatorname{span}_{\mathbb{Z}} \Phi^1_{\mathsf{A}} = \operatorname{span}_{\mathbb{Z}}(e_1 - e_2)$, so that $\operatorname{span}_{\mathbb{Z}} \Phi^1_{\mathsf{A}} = \mathbb{Z}^2_0$.

More generally, let $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n_0$. We have

$$\begin{aligned} \sum_{i=1}^{n} v_i &= 0 \\ \Leftrightarrow -\sum_{i=1}^{n-1} v_i &= v_n \end{aligned} \tag{6.0.4}$$

We write

$$\begin{aligned} v &= \sum_{i=1}^{n} v_i e_i \\ &= \sum_{i=1}^{n-1} v_i e_i + v_n e_n \\ &= \sum_{i=1}^{n-1} v_i e_i + \left(-\sum_{i=1}^{n-1} v_i\right) e_n \\ &= \sum_{i=1}^{n-1} v_i (e_i - e_n), \end{aligned} \tag{6.0.5}$$

where we used 6.0.4 in the third equality. From 6.0.5 we see that $v \in \mathbb{Z}_0^n \subseteq \operatorname{span}_{\mathbb{Z}} \Phi_{\mathsf{A}}^{n-1}$. On the other hand, note that each "basis-vector" $e_i - e_j$ is such that it sums to 0, e.g. take $e_2 - e_3$ in Φ_{A}^2, then we have that

$$\begin{aligned} e_2 - e_3 &= (0,1,0) - (0,0,1) \\ &= (0,1,-1), \end{aligned}$$

and $1 - 1 = 0$. More rigorously, if $v \in \operatorname{span}_{\mathbb{Z}} \Phi_{\mathsf{A}}^{n-1}$, then we can write v on the form

$$v = \sum_{\substack{1 \leqslant i,j \leqslant n \\ i \neq j}} c_{ij}(e_i - e_j)$$

We see that $v_k = \sum_{\substack{1 \leqslant i,j \leqslant n \\ i \neq j}} c_{ij} \Gamma_k(e_i - e_j)$ where $\Gamma_k : \Phi_{\mathsf{A}}^{n-1} \to \{\pm 1, 0\}$ is defined as

$$\Gamma_k(e_i - e_j) = \begin{cases} 1, \text{ if } i = k; \\ -1, \text{ if } j = k; \\ 0, \text{ otherwise.} \end{cases}$$

We then have that

$$\begin{aligned} \sum_{k=1}^n v_k &= \sum_{k=1}^n \left(\sum_{\substack{1 \leqslant i,j \leqslant n \\ i \neq j}} c_{ij} \Gamma_k(e_i - e_j) \right) \\ &= \sum_{\substack{1 \leqslant i,j \leqslant n \\ i \neq j}} c_{ij} \left(\sum_{k=1}^n \Gamma_k(e_i - e_j) \right) \\ &= \sum_{\substack{1 \leqslant i,j \leqslant n \\ i \neq j}} c_{ij} \cdot 0 \qquad (6.0.6) \\ &= 0, \end{aligned}$$

where we have used that as we let k go from 1 to n in the inner sum in 6.0.6, we see that when $i = k$ we get a contribution of 1 in the sum, and when $k = j$ we get a contribution of -1, and if $k \neq i, j$ then we get a contribution of 0, so a net total contribution of 0, for each pair $1 \leqslant i \neq j \leqslant n$. Therefore, $\operatorname{span}_{\mathbb{Z}} \Phi_{\mathsf{A}}^{n-1} \subseteq \mathbb{Z}_0^n \Rightarrow \operatorname{span}_{\mathbb{Z}} \Phi_{\mathsf{A}}^{n-1} = \mathbb{Z}_0^n$.

We conclude that Φ_{A}^{n-1} spans $\mathbb{Z}_0^n$ over $\mathbb{Z}$, but it does not span $\mathbb{Z}^n / \langle (1, \dots, 1) \rangle$ over $\mathbb{Z}$.

From what we have just showed, regarding **Question I** and **Question II**, we can conclude the following: For $\mathsf{SL}(n)$, coroots span cocharacters over $\mathbb{Z}$, but the root do not span the characters over $\mathbb{Z}$, and for $\mathsf{PGL}(n)$, roots span characters over $\mathbb{Z}$, but coroots do not span cocharacters over $\mathbb{Z}$.

Exercise:

$$\mathbb{Z}^n / (\langle 1, \dots, 1) \rangle \Big/ \operatorname{span}_{\mathbb{Z}} \{ e_i - e_j + \langle (1, \dots, 1) \rangle \ : \ 1 \leqslant i \neq j \leqslant n \} \cong \mathbb{Z}/n$$

.

Definition

Definition 6.0.17. A *root datum* (5.0.7) is **semisimple** if $X^*_{\mathbb{Q}} = \operatorname{span}_{\mathbb{Q}} \Phi^\vee$.

Example 6.0.18. $\mathsf{SL}(n)$ and $\mathsf{PGL}(n)$ have semisimple (9.0.21) root datums, but $\mathsf{GL}(n)$ does not.

Definition

Definition 6.0.19. A *root datum* is **simply-connected** if $\mathbb{Z}\Phi = X^*$, where $\mathbb{Z}\Phi = \operatorname{span}_{\mathbb{Z}}\Phi$, i.e. the $\mathbb{Z}$-span of the roots of the root datum gives the characters.

Definition

Definition 6.0.20. A *root datum* is **adjoint** if

$$\begin{aligned}\mathbb{Z}\Phi^\vee &= \operatorname{span}_{\mathbb{Z}}\Phi^\vee \\ &= X_*.\end{aligned}$$

That is, a root datum is adjoint if the cocharacters (4.1.5) are equal to the $\mathbb{Z}$-span of the coroots (2.0.3).

Example 6.0.21. $\mathsf{SL}(n)$ has simply-connected root datum (6.0.19), but not adjoint root datum (6.0.20).

Example 6.0.22. $\mathsf{PGL}(n)$ has adjoint root datum, but not simply-connected root datum.

Definition

Definition 6.0.23. A group G is **adjoint** if the center of G, $Z(G)$, is trivial, i.e.

$$Z(G) = \{1\}.$$

A **connected reductive group** G is adjoint $\Leftrightarrow$ its root data is adjoint for all maximal tori $T \subset G$.

Assume $G/\mathbb{C}$ with $k = \mathbb{C}$. Then $G(\mathbb{C}) =$ are the complex solutions to equations *defining* G, and is a topological space with the *subspace topology* inherited from the usual topology on $\mathbb{C}^n$, if given by equations in n variables, i.e. $f_i(x_1, \dots, x_n) = \dots = f_i(z_1, \dots, z_n) = 0$ where $(z_1, \dots, z_n) \in \mathbb{C}^n$, say for $f_1, \dots, f_r$.

For all *connected, reductive groups* G over $\mathbb{C}$, we have the following theorem.

Theorem 6.0.24. *$G(\mathbb{C})$ is simply-connected as a* topological space $\Leftrightarrow$ *the* root data *of G are simply-connected.*

Example 6.0.25. $\mathsf{SO}^{\mathcal{J}}(2n)$ where

$$\mathcal{J} = \begin{pmatrix} & & & & 1 \\ & & & 1 & \\ & & \iddots & & \\ & 1 & & & \\ 1 & & & & \end{pmatrix},$$

we want to compute a root datum for *relative* to a maximal torus $\operatorname{Diag}(2n) \cap \hat{\mathrm{SO}}^{\mathcal{J}}(2n)$. We have

$$(\mathbb{Z}^n, \Phi^n_{\mathsf{D}}; \mathbb{Z}^n, \Phi^n_{\mathsf{D}}),$$

where $\Phi^n_{\mathsf{D}} = \{\pm(e_i + e_j) \mid 1 \leqslant i \neq j \leqslant n\}$. We have

$$\mathbb{Z}^n / \operatorname{span}_{\mathbb{Z}}\Phi^n_{\mathsf{D}} \cong \mathbb{Z}/2,$$

which implies that $\mathbb{Z}\Phi_{\mathsf{D}}^n \neq \mathbb{Z}^n$, the characters, therefore not simply-connected (6.0.19). By 6.0.24 $\mathrm{SO}(2n, \mathbb{C})$ not simply connected.

Let $\mathrm{Spin}(2n, \mathbb{C}) = \widetilde{\mathrm{SO}}(2n, \mathbb{C})$, the **universal cover**.

Theorem 6.0.26. *For all connected, reductive groups G, we have that $\pi_1(G(\mathbb{C})) = X^*(T)/\mathbb{Z}\Phi$, where $T \subset G$ is a maximal torus.*

6.0.1 Lie Algebras

Definition

Definition 6.0.27. Let F be a field. A **Lie Algebra** A/F is an F-vector space together with a *pairing*/lie-multiplication ("bracket")

$$[-,-] : A \times A \to A,$$

that satisfies the following:

1. $[x, x] = 0, \forall x \in A$ ("Anti-commutativity"). If the *characteristic of F* is not equal to 2, then this is *equivalent* to $[x, y] = -[y, x], \forall x, y \in A$.
2. $[x, [y, z]] + [z, [x, y]] + [y, [z, x]] = 0, \forall x, y, z \in A$ ("Jacobi-identity"). An easy way to remember this is to start with $[x, [y, z]]$ and then successively move every letter one step to the right, until x ends up at the last spot (of course also recalling that it should be a sum summing to 0).
3. A is an F-algebra (but not associative).

6.0.2 How to construct Lie-algebras from algebras

If R is an F-algebra (associative, but not neccessarily commutative), then if we let $[-,-] : R \times R \to R$ be defined by $[a, b] = ab - ba$, then $(R, [-,-])$ is a Lie algebra (6.0.27).

Definition

Definition 6.0.28. A Lie algebra $\mathfrak{g}$ is **commutative** if $[-,-] \equiv 0$, i.e. in the sense that $[x, y] = 0, \forall x, y \in \mathfrak{g}$.

Remark 6.0.29. $\mathfrak{g}$ seems to be a conventional way to denote a Lie algebra. You should think of $\mathfrak{g}$ as A/F in 6.0.27, for some fixed field F.

Example 6.0.30. Let $R = M_n(F)$. Then $\mathfrak{gl}(n, F) = (R, [-,-])$ with $[a, b] = ab - ba$ is a Lie algebra.

Recall, that if $\mathcal{J} \in \mathsf{GL}(n, F)$ is symmetric or anti-symmetric, then we have

$$\mathrm{G}^{\mathcal{J}}(F) = \{A \in \mathsf{GL}(n, F) \mid {}^tA\mathcal{J}A = \mathcal{J}\}.$$

Example 6.0.31. $\mathrm{SO}^{\mathcal{J}}$ is symmetric.

Example 6.0.32. $\mathrm{Sp}^{\mathcal{J}}$ is anti-symmetric.

With Lie algebras in mind (6.0.27), we have that

$$\mathrm{SO}^{\mathcal{J}}(F) = \{A \in \mathfrak{gl}(n, F) \mid {}^tA\mathcal{J} + \mathcal{J}A = 0\},$$

where we $\mathfrak{gl}(n, F) = M_n(F)$. One needs to check that $\mathrm{SO}^{\mathcal{J}}$ and $\mathrm{Sp}^{\mathcal{J}}$ in examples 6.0.31, 6.0.32 are *closed* under $[-,-]$.

Chapter 7

Lecture 7

Reductive and semisimple Lie algebras are "avatars" of reductive and semisimple algebraic groups (a bit like finite coxeter groups, another avatar).

Example 7.0.1. Recall 6.0.30. If $R \subset M_n(F)$ is an associative subalgebra, then $ab - ba \in R, \forall a, b \in R$. Therefore, $(R, [-,-])$ is (we claim) is a Lie algebra. This is quite natural to see, since looking at the axioms for a Lie algebra (6.0.27) we see that the only thing that needs to be checked is that the codomain of the restriction map $[-,-] : M_n(F) \times M_n(F) \to M_n(F)$ to $[-,-]_R : R \times R \to M_n(F)$ is contained within R (perhaps). In our case this follows from the claim that $ab - ba \in R$. We would then call $(R, [-,-])$ a **Lie subalgebra** of the Lie algebra $(M_n(F), [-,-])$.

Every algebraic group G has a Lie algebra. This is usually denoted (as remarked earlier) with $\mathrm{Lie}(G) = \mathfrak{g}$, or in the case of the general linear group, as

$$\begin{aligned} M_n &= \mathfrak{gl}_n \\ &= \mathrm{Lie}(\mathsf{GL}(n)). \end{aligned}$$

On the group level, we have: $\mathsf{GL}(n, F) \supset \mathsf{Triag}^+(n, F) \supset \mathrm{Diag}(n, F)$ where $\mathsf{Triag}^+(n, F)$ is an example of a **Borel subgroup**, where we recall that $\mathrm{Diag}(n, F)$ is a *maximal torus*. We also have an inclusion $\mathsf{Triag}^+(n, F) \supset \mathsf{Uniag}^+(n, F)$.

On the Lie algebra level: $\mathfrak{gl}_n(F) \supset \mathfrak{triag}^+(n, F) \supset \mathfrak{diag}(n, F)$, where $\mathfrak{diag}(n, F)$ is an *abelian* Lie subalgebra (recall example 7.0.1 for an example of a Lie subalgebra). We also have the inclusion $\mathfrak{triag}^+(n, F) \supset \mathfrak{uniag}^+(n, F)$ where $\mathfrak{uniag}^+(n, F)$ we claim to have 0:s on the diagonal. Further, $\mathfrak{gl}_n(F) = M_n(F)$, and $\mathfrak{triag}^+(n, F)$ is all upper triangular matrices, and $\mathfrak{diag}(n, F)$ is all diagonal matrices. The denotations here have the "obvious" interpretations, i.e.

$$\begin{aligned} \mathfrak{diag}(n, F) &= \mathrm{Lie}(\mathrm{Diag}(n, F)); \\ \mathfrak{triag}^+(n, F) &= \mathrm{Lie}(\mathsf{Triag}^+(n, F)). \end{aligned}$$

Definition

Definition 7.0.2. An **ideal in a Lie algebra** A/F is the same as an ideal in an associative algebra. That is, $I \subset A$ is an ideal if I is a vector subspace of A and if $[a, i] \in I$ for all $a \in A$ and for all $i \in I$.

Remark 7.0.3. In a general non-commutative ring one makes a distinction between *left* ideals and *right* ideals. But I suppose what we want here is that both $[a, i] \in I, \forall a \in A, \forall i \in I$ and $[i, a] \in I, \forall a \in A, \forall i \in I$.

Note that by 6.0.27 we have that $[a, i] = -[i, a]$ (assuming we are in characteristic different from 2). Further. note that we have $[a+b, a+b] = [a, a] + [b, b] + [a, b] + [b, a]$. But the first two terms on the right-hand side vanish (since $[x, x] = 0$ for all x in some Lie algebra $\mathfrak{g}$). And since we know that $[a+b, a+b] = 0$, we get

$$\begin{aligned}[a+b, a+b] &= [a, b] + [b, a] \\ \Leftrightarrow 0 &= [a, b] + [b, a] \\ \Leftrightarrow -[a, b] &= [b, a].\end{aligned}$$

We claim here that $\mathfrak{diag}(n, F)$ is *not* an ideal of $\mathfrak{triag}^+(n, F)$. We have that

$$\mathfrak{triag}^+(F, n) = \mathfrak{uniag}^+(n, F) \oplus \mathfrak{diag}(n, F),$$

which is a direct sum as vector spaces, *not as Lie algebras*.

We have the usual quotient+isomorphism theorems for Lie algebras. We can define a map $\varphi : \mathfrak{triag}^+(n, F) \to \mathfrak{diag}(n, F)$, explicitly by $\mathfrak{triag}^+ \ni A \mapsto \operatorname{diag}(a_{11}, \ldots, a_{nn})$, i.e.

$$\mathfrak{triag}^+ \ni A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ & \ddots & \vdots \\ & & a_{nn} \end{pmatrix} \overset{\varphi}{\mapsto} \begin{pmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn}. \end{pmatrix} \in \mathfrak{diag}(n, F)$$

We have that

$$\begin{aligned}\varphi([a, b]) &= \varphi(ab - ba) \\ &= \varphi(ab) - \varphi(ba) \\ &= \varphi(a)\varphi(b) - \varphi(b)\varphi(a) \\ &= [\varphi(a), \varphi(b)],\end{aligned}$$

since φ is an F-linear transformation of vector spaces, and it is easily checked that $\varphi(ab) = \varphi(a)\varphi(b)$. The kernel of this map is precisely the subgroup $\mathfrak{uniag}^+(n, F)$, so $\ker \varphi = \mathfrak{uniag}^+(n, F)$. φ is surjective, so then by isomorphism theorems we have that

$$\mathfrak{triag}^+(n, F)/\mathfrak{uniag}^+(n, F) \cong \mathfrak{diag}(n, F).$$

We claim that there is also an isomorphism

$$\mathsf{Triag}^+(n, F)/\mathsf{Uniag}^+(n, F) \cong \mathrm{Diag}(n, F).$$

Definition

Definition 7.0.4. A ring R is **simple** if it has no 2-sided ideals other than $(0), (1) = R$.

Example 7.0.5. We claim that $M_n(F)$ is simple as a ring. It has *non*-trivial right and left-ideals, but we claim that it has no non-trivial *two-sided* ideals (See perhaps [1, Chap. 18]).

Definition

Definition 7.0.6. A Lie algebra (6.0.27) is **simple** if it is *simple* as a ring (7.0.4).

Theorem 7.0.7. *Let F be an algebraically closed field of characteristic 0. Then the (finite-dimensional) Lie algebras over F are precisely the following.*

$$\begin{aligned}
\mathrm{Lie}(\mathsf{SL}(n,F)) &= \mathfrak{sl}(n,F) \\
&= \{A \in M_n(F) \mid \mathrm{tr}(A) = 0\} \quad (\textit{“traceless matrices”}); \\
\mathrm{Lie}(\mathrm{SO}(2n+1,F)) &= \mathfrak{so}(2n+1,F) \\
&= \{A \in M_{2n+1}(F) \mid {}^tA = -A\} \quad (\textit{“skew symmetric matrices” of type } \mathsf{B}_n) \\
\mathrm{Lie}(SO(2n,F)) &= \mathfrak{so}(2n,F) \quad (\textit{of type } \mathsf{D}_n,\ \textit{for } n \neq 2); \\
\mathrm{Lie}(Sp(2n,F)) &= \mathfrak{sp}(2n,F) \quad (\textit{of type } \mathsf{C}_n);
\end{aligned}$$

together with $\mathrm{Lie}(\mathsf{G}_2), \mathrm{Lie}(\mathsf{F}_4), \mathrm{Lie}(\mathsf{E}_6), \mathrm{Lie}(\mathsf{E}_7), \mathrm{Lie}(\mathsf{E}_8)$, *with the coincidental isomorphisms*

$$\begin{aligned}
\mathsf{A}_1 &\cong \mathsf{B}_1 \\
&\cong \mathsf{C}_1 \\
&\cong \mathsf{D}_1; \\
\mathsf{B}_2 &\cong \mathsf{C}_2; \\
\mathsf{A}_3 &\cong \mathsf{D}_3,
\end{aligned}$$

and no others.

In other words, we have the following claims.

(a) There exists a simple Lie algebrra over F for all the reduced, irreducible root systems.

(b) Two such simple Lie alebras are isomorphic $\Leftrightarrow$ they arise from isomorphic reduced and irreducible root systems.

(c) Every finite-dimensional simple Lie algebra from a reduced, irreducible root system.

Diagrammatically, we have the following bijection.

$$\left\{\text{Simple Lie algebras} \Big/ \overline{F}\right\} \Big/ \sim \; \xleftrightarrow{\text{bijection}} \; \left\{\text{Reduced and irreducible root systems}\right\} \Big/ \sim \tag{7.0.1}$$

where $\sim$ is the equivalence-relation induced by isomorphism.

Example 7.0.8. We have that $\mathfrak{gl}(n,F)$ is not simple, and decomposes as the direct sum

$$\mathfrak{gl}(n,F) = \mathfrak{sl}(n,F) \oplus Z(\mathfrak{gl}(n,F)),$$

where

$$\begin{aligned}
Z(\mathfrak{gl}(n,F)) &= Z(M_n(F)) \\
&= F,
\end{aligned}$$

so we can write $\mathfrak{gl}(n,F) = \mathfrak{sl}(n,F) \oplus F \cdot I$. Note that $\mathfrak{gl}(n,F) = M_n(F)$ we claimed earlier was simple *as a ring*, but it is *not* simple as a Lie algebra; to see this, note that we can define a center with respect to the Lie-algebra structure as $Z(\mathfrak{gl}(n,F)) = \{A \in \mathfrak{gl}(n,F) \mid [A,B] = AB - BA = 0, \forall B \in \mathfrak{gl}(n,F)\}$. This is precsily the center of $M_n(F)$, i.e. the scalar-matrices. We claim that this is an ideal of $\mathfrak{gl}(n,F)$. Recall 7.0.2; we see that

$$\begin{aligned}
[B, I\lambda] &= B\lambda - \lambda B \\
&= 0 \in Z(\mathfrak{gl}(n,F)),
\end{aligned}$$

similarly we have that $[I\lambda, B] = 0$ for $\lambda \in F$. Therefore, since $Z(\mathfrak{gl}(n,F))$ is an associative subalgebra (it is in fact a subring of $M_n(F)$), we see that $\mathfrak{gl}(n,F)$ has nontrivial 2-sided ideals as a Lie algebra and is therefore not simple.

Remark 7.0.9. We claim that $\mathfrak{sl}(n,F)$ is of type A_{n-1}.

7.0.1 Constructing a root system from a simple Lie algebra

Let F be an algebraically closed field. If A is a simple Lie algebra (7.0.6), then to get a root system (2.0.1), take $D \subset A$ that is a maximal abelian subalgebra such that $[a,b] = 0, \forall a, b \in D$, and such that the "action" (we don't mean group action, here) of D on A by $[-,-]$ is diagonalizable for all $a \in D$.

Remark 7.0.10. What we mean by action here is that we have an **adjoint** action induced by $\mathrm{ad}(a)(x) = [a,x]$. This is a F-linear map ($[-,-]$ is linear in each argument), so $\mathrm{ad}(a) : A \to A$ is a F-linear endomorphism, hence $\mathrm{ad}(a) \in \mathrm{End}_F(A)$.

The above is the analogoue of $\mathfrak{diag}(n) \subset \mathfrak{gl}(\mathfrak{n})$, where $\mathrm{Diag}(n) \subset \mathsf{GL}(n)$ is the maximal torus in G, for G connected and reductive. One can show that $\mathrm{End}_F(A) \cong M_n(F)$ as F-vector spaces, where $n = \dim_F A$. If we let $A = \mathfrak{gl}(n,F) = M_n(F)$, then we see that $\mathrm{End}_F(A) \cong M_{n^2}(F)$, since $\dim_F M_n(F) = n^2$.

Again, let $F = \overline{F}$ be algebraically closed. Let A be a (simple) Lie algebra. We have an "action" $D \curvearrowright A$ by the Lie-bracket $[-,-]$. This induces a root-space decomposition

$$A = D \oplus \bigoplus A_\chi,$$

where A_χ is zero for all but finitely many χ, where $D = A_D$, and where $0 \neq \chi \in \mathrm{Hom}(A,F) = A^\vee$, the dual space of A (as a vector space). We define

$$A_\chi := \{a \in A \ : \ [d,a] = \chi(a)a, \forall d \in D\},$$

the "χ **eigenspace**" of A. We let

$$\Phi := \{\chi \in A^\vee \mid A_\chi \neq 0\},$$

which we call the **roots of** A. Recall here that

$$\begin{aligned}\mathfrak{gl}(n,F) &= M_n(F)\\ &= \mathrm{diag}(n,F) \oplus \bigoplus_{i,j} E_{ij}\\ &= \mathfrak{diag}(n,F) \oplus \bigoplus_{i,j} E_{ij}.\end{aligned}$$

Then we have that $(\mathrm{span}_{\mathbb{Q}}\Phi, \Phi, [-,-])$ is the **root system of** A **relative to** D.

Remark 7.0.11. If F is *not algebraically closed*, and A is a Lie algebra over F, then if we let $K \supset F$ be a field extension, we get a Lie algebra $A \otimes_F K$ over K. It seems like often, one has Lie algebras A_1, A_2 over some field F, that are not isomorphic as Lie algebras over F, but where $A_1 \otimes_F K \cong A_2 \otimes_F K$. K could for example be $\overline{F}$, the *algebraic closure* of F (the since it is unique, up to isomorphism). If it holds that $A_1 \otimes_F K \cong A_2 \otimes_F K$, then we say that A_1 and A_2 are F**-forms** of one another.

If A_1, A_2 are Lie algebras, then $A_1 \oplus A_2$ is the Lie algebra with vector space $A_1 \oplus A_2$, and $[a_1, a_2] = 0$, for all $a_1 \in A_1$ and all $a_2 \in A_2$. We have

$$\begin{aligned}\big[(a_1,a_2),(a_1',a_2)\big] &= (a_1,a_2)(a_1',a_2') - (a_1',a_2')(a_1,a_2)\\ &= (a_1a_1', a_2a_2') - (a_1'a_1, a_2a_2')\\ &= (a_1a_1' - a_1'a_1, a_2a_2' - a_2'a_2)\\ &= \big([a_1,a_1'],[a_2,a_2']\big).\end{aligned}$$

Recall: If N_1, N_2 are subgroups of a group G, then G is isomorphic as a group to the direct product of N_1, N_2,

$$G \cong N_1 \times N_2,$$

if the following holds:

1. N_1, N_2 are both *normal* subgroups of G, i.e. $N_1, N_2 \triangleleft G$.
2. $N_1 \cap N_2 = 1_G$, where 1_G is the identity element of the group G.
3. $N_1 N_2 = G$.

Analogously, we have that

$$\begin{aligned} B &\cong A_1 \oplus A_2 \\ &= A_1 \times A_2, \end{aligned}$$

if it holds that

(i) A_1, A_2 are sub Lie algebras of B, that are ideals (with respect to the Lie bracket; see 7.0.2).

(ii) $A_1 \cap A_2 = (0)$.

(iii) $A_1 + A_2 = B$ (where this is the sum of [Lie-bracket] ideals A_1, A_2 of B).

Remark 7.0.12. Note that it is an *internal direct sum* above; in the sense that we start with a larger object B and decompose it into smaller ones. Cf. *external direct sum*, where we would instead *start with smaller objects* (in the sense of inclusion) and construct *larger ones* from the smaller ones (roughly).

Definition

Definition 7.0.13. A Lie algebra (6.0.27) is **semisimple** if it is a *finite direct sum* of simple (7.0.6), finite-dimensional Lie algebras.

In particular, from the definition above, we have that a semisimple Lie algebra must be finite-dimensional. Before the next definition, we will formally state the definition of the center $\mathfrak{z}(A)$ of a Lie algebra A.

Definition

Definition 7.0.14. Given a Lie algebra A, we define its **center relative to the Lie bracket**, as

$$\mathfrak{z}(A) = \{a \in A \ : \ [a, b] = 0, \forall b \in A\}.$$

Definition

Definition 7.0.15. A Lie algebra A is **reductive** if

$$A = B \oplus \mathfrak{z}(A),$$

where B is *semisimple* (7.0.13).

Definition

Definition 7.0.16. If A is a *reductive* Lie algebra, then $B = [A, A]$, is the **derived subalgebra/commutator subalgebra**.

We have a map $G \longmapsto \mathsf{Lie}(G)$, that takes an *algebraic group* G to its Lie algebra. We have that G is connected and semisimple *if and only if* $\mathsf{Lie}(G)$ is semisimple (7.0.13). Furthermore, if G is connected and reductive, then we claim that $\mathsf{Lie}(G)$ is reductive (7.0.15).

Example 7.0.17. We have that $\mathbb{G}_a(F) = (F, +)$ is the additive group-functor, that takes a field (or perhaps more generally an F-algebra) to its underlying abelian group structure with respect to addition. $\mathbb{G}_a$ is in fact an affine group scheme, which is represented by $F[x]$, given that the source of $\mathbb{G}$ has source $\mathbf{Alg}_F$ (see appendix). We then have that

$$\begin{aligned}\mathsf{Lie}(\mathbb{G}_a) &= \mathsf{Lie}(\mathsf{GL}(1)) \\ &= M_1,\end{aligned}$$

which is abelian. We claim that $\mathbb{G}_a$ is not reductive, but $\mathsf{GL}(1)$ is. This gives an example that the above implication noted above, does not hold the other way around.

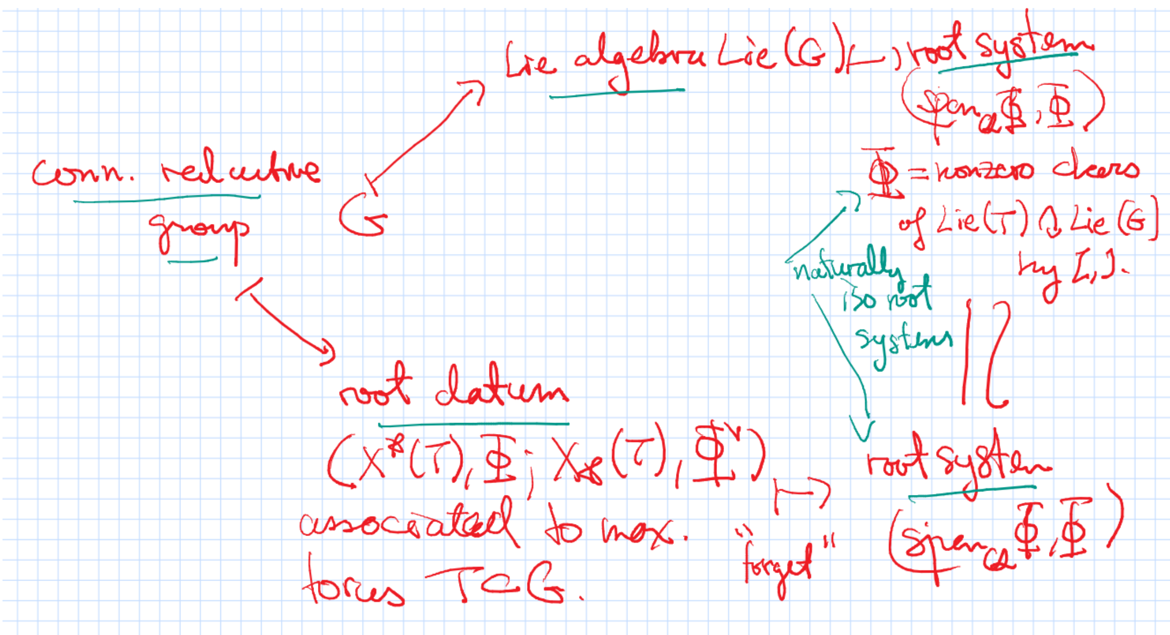


Figure 7.1: Addendum to lecture 7.

Chapter 8

Lecture 8

8.0.1 Pairwise commuting endomorphisms (equivalently; matrices)

Note (or perhaps recall) that a Linear endomorphism = Linear transformation $T : V \to V$.

Theorem 8.0.1. *Assume that S is a set of pairwise commuting linear endomorphisms of a finite-dimensional vector space V, that is, $S \subset \mathrm{End}_F(V)$, such that*

$$st = ts, \forall s, t \in S.$$

Then the following holds.

1. *If every $t \in S$ is* triagonalizable *(that is, conjugate to an upper-triangular matrix), then S is* *simultaneously* triagonalizable, *i.e. there is some $g \in \mathsf{GL}(V)$ such that for all $s \in S$, we have that gsg^{-1} is upper-triangular (note that we are not claiming that $gsg^{-1} = gs'g^{-1}$ for all $s, s \in S$, only that the result after conjugation by the same element g gives something on upper-triangular form; the same comment holds in the context of diagonalization, below).*
2. *If every $t \in S$ is* diagonalizable, *then S is* *simultaneously* diagonalizable. *That is, there exists some $g \in \mathsf{GL}(V)$ such that gsg^{-1} is* diagonal, *for all $s \in S$.*

Remark 8.0.2. In theorem (8.0.1), there is no assumption being made on the field F over which the vector-space V is defined.

Corollary 8.0.3. *If F in 8.0.1 is algebraically closed, then a set S that pairwise commutes is simultaneously triagonalizable, i.e. there is some $g \in \mathsf{GL}(V)$ such that gsg^{-1} is upper triangular, for all $s \in S$.*

This follows from the claim that over algebraically closed fields, every $s \in \mathrm{End}_F(V)$ is triagonalizable, so by a) of 8.0.1 the result follow.

Lemma 8.0.4. *If $S \subset \mathrm{End}_F(V)$ pairwise commutes, then for all $t \in S$, the* eigenspaces *of t are S-stable. That is, if $t_\lambda := \{v \in V \mid t \cdot v = \lambda v\}$, then $s(t_\lambda) \subset t_\lambda$, for all $s \in S$.*

Proof. Let $v \in t_\lambda$. Then

$$\begin{aligned} t(s(v)) &= (ts)(v) \\ &= (st)(v) \\ &= s(t(v)) \\ &= s(\lambda v) \\ &= \lambda s(v), \end{aligned}$$

therefore, $s(v) \subset t_\lambda$. Hence $s(t_\lambda) \subset t_\lambda$. □

Remark 8.0.5. 8.0.1 + 8.0.4 usually false without pairwise commuting S.

We now prove part b) of 8.0.1.

Proof. If $S \subseteq \{\lambda I \mid \lambda \in F\}$, then it is already on diagonal form, hence this is trivially true (take $g = I \in \mathsf{GL}(V)$). So assume that $S \not\subset \{\lambda I \mid \lambda \in F\}$, and let $t \in S$ such that t is not a scalar. By assumption, t is diagonalizable, so it admits an eigenvalue λ with *geometric multiplicity* m_λ where $0 < m_\lambda < \dim_F V$. By definition, $m_\lambda = \dim_F(t_\lambda)$. By 8.0.4, t_λ is S-stable. We proceed by *induction* over the **dimension** of the vector space V: The action of S on t_λ is simultaneously diagonalizable. Note that t is diagonalizable $\Leftrightarrow V = \bigoplus\limits_{\mu \in F} t_\mu$. 8.0.4 applies to all t_μ. Since each t_μ is a vector subspace of dimension atleast 1, and V is *finite-dimensional*, there has to be some integer r and some eigenvalues $\mu_1, \ldots, \mu_r$ such that

$$V = \bigoplus_{i=1}^{r} t_{\mu_i}. \tag{8.0.1}$$

We note that each $s \in S$ takes each $s(t_{\mu_i}) \subseteq t_{\mu_i}$. Let $n_i = \dim_F t_{\mu_i}$. If we choose a basis for each t_{μ_i} in 8.0.1, then we note that each $s \in S$ by 8.0.4 and their is no cross-over. This means that we can represent s in block-diagonal form

$$S = \begin{pmatrix} s_1 & & \\ & \ddots & \\ & & s_r \end{pmatrix}$$

where the matrix is divided into blocks $s_1, \ldots, s_r$ of size $n_1, \ldots, n_r$. This means that for all $s \in S$, we have

$$s = \bigoplus_{i=1}^{r} s_i, \tag{8.0.2}$$

and there the action of s on t_{μ_i} is by the i^{th} component s_i. Since we are assuming that t is *not* on scalar form, $r > 1$, and therefore $1 \leqslant n_i < n$. So by induction, there is some $g_i \in \mathsf{GL}(t_{\mu_i})$ such that $g_i s_i g_i^{-1}$ is diagonal, for each $i = 1, \ldots, r$ and for all $s_i \in \mathsf{GL}(t_{\mu_i})$. Define

$$\begin{aligned} G &= \begin{pmatrix} g_1 & & \\ & \ddots & \\ & & g_r \end{pmatrix} \\ &= g_1 \oplus \ldots \oplus g_r. \end{aligned}$$

We claim (without proof, but it seems intuitively clear) that if one has block-diagonal matrices $A = \operatorname{diag}(A_1, \ldots, A_m)$ and $B = \operatorname{diag}(B_1, \ldots, B_m)$ where $\dim A_i = \dim B_i$, then when one multiplies A with B, the multiplication happens *solely within the blocks*. It follows from similar reasoning that the inverse of G is

$$\begin{aligned} G^{-1} &= \begin{pmatrix} g_1^{-1} & & \\ & \ddots & \\ & & g_r^{-1} \end{pmatrix} \\ &= g_1^{-1} \oplus \ldots \oplus g_r^{-1}. \end{aligned}$$

It follows that

$$\begin{aligned} GSG^{-1} &= \begin{pmatrix} g_1 & & \\ & \ddots & \\ & & g_r \end{pmatrix} \begin{pmatrix} s_1 & & \\ & \ddots & \\ & & s_r \end{pmatrix} \begin{pmatrix} g_1^{-1} & & \\ & \ddots & \\ & & g_r^{-1} \end{pmatrix} \\ &= g_1 s_1 g_1^{-1} \oplus \ldots \oplus g_r s_r g_r^{-1}, \end{aligned}$$

which is diagonal, by definition. The statement now follows by (strong) induction together with 8.0.2. □

Below, we give the proof for a) of 8.0.1.

Proof. By 8.0.4 we can assume that t_λ is S-stable, for any $t \in S$. We claim that then also the quotient space V/t_λ is s-stable. To expand on what we just said, since t_λ is s-stable, so that $s(t_\lambda) \subseteq t_\lambda$, for all $s \in S$, we have a map $\varphi : S \to \mathrm{End}_F(t_\lambda)$ defined explicitly by $S \ni s \overset{\varphi}{\longmapsto} s|_{t_\lambda} \in \mathrm{End}_F(t_\lambda)$. Then since t_λ is s-stable, we get a well-defined map $\psi : S \to \mathrm{End}_F(V/t_\lambda)$, defined by $S \ni S \overset{\psi}{\longmapsto} \tilde{s} \in \mathrm{End}_F(V/t_\lambda)$. Since s behavior on V/t_λ is inherited from how it "acts" on V, this map is well-defined. We need to show that the induced map $\tilde{s}$ is well-defined. So assume that $v + t_\lambda = w + t_\lambda \Leftrightarrow (v - w) + t_\lambda = 0 + t_\lambda$. Then $v - w \in t_\lambda$, so that

$$\begin{aligned} \tilde{s}((v-w)+t_\lambda) &= (s(v-w)) + t_\lambda \\ &= 0 + t_\lambda \\ \Leftrightarrow (s(v) - s(w)) + t_\lambda &= 0 + t_\lambda \\ \Leftrightarrow \tilde{s}(v + t_\lambda) - \tilde{s}(w + t_\lambda) &= 0 + t_\lambda \\ \Leftrightarrow \tilde{s}(v + t_\lambda) &= \tilde{s}(w + t_\lambda), \end{aligned}$$

where we in the first equality used that s is linear, and so $\tilde{s}$ inherits this linearity, and that s takes $v \in t_\lambda$ to t_λ.

We proceed by (strong) induction on the **dimension** (as in the proof of b); note that for $n = 1$ the statement is trivially true) there are $g_1 \in \mathsf{GL}(V), g_2 \in \mathsf{GL}(V/t_\lambda)$ such that for all $s \in S$ we have $g_1 \varphi(s) g_1^{-1}$ and $g_2 \psi(s) g_2^{-1}$ on *upper triangular form.* NOT FINISHED □

Example 8.0.6. Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : F^2 \to F^2$ with $\mathrm{span}(e_1)$ stable, but it has no stable complement; $\dim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}_1 = 1$ (geometric multiplicity) with $\lambda = 1$, and with characteristic polynomial $(x-1)^2$. That it has no stable complement can be seen from the fact that for any vector $\begin{pmatrix} a \\ b \end{pmatrix}$ we have that

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} &= \begin{pmatrix} a+b \\ b \end{pmatrix} \\ &= (a+b)e_1 + be_2. \end{aligned}$$

It follows that if $W \subset F^2$ is a non-trivial subspace that is not contained in $\mathrm{span}(e_1)$, it will have a vector with on the form $\begin{pmatrix} a \\ b \end{pmatrix}$ with $b \neq 0$. But then the result, as above, will be $(a+b)e_1 + be_2$. But since we want $F^2 = \mathrm{span}(e_1) \oplus W$ for some complement $W \subseteq F^2$, and $be_2 \notin \mathrm{span}(e_1)$, we must have $be_2 \in \mathrm{span}(e_1)$. But now note that for $A(W) \subseteq W$ to hold, we need $(a+b)e_1 + be_2 \in W$. But then we have both $e_2 b$ and $(a+b)e_1 + be_2 \in W$, so that $((a+b)e_1 + be_2) - be_2 = (a+b)e_1 \in W$, but then $W \cap \mathrm{span}(e_1) \neq (0)$, since $b \neq 0$, contradiction!

This is the first example of "local versus global conjugacy" (local or elementwise; global or simultaneous).

8.0.2 Applications

Question: Is every *abelian* subgroup of $\mathsf{GL}(n)$ contained in a maximal torus?

Answer: Take

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle,$$

or

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in F \right\}.$$

since neither of these groups can be simultaneously diagonalizable (or even diagonalized, in the two examples given); why is this relevant? Recall that all maximal tori are *conjugate*, and that $\mathrm{Diag}(n) \leq \mathsf{GL}(n)$ was a maximal torus; hence for either of these two groups above to be included in a maximal torus in $\mathsf{GL}(n)$, they would have to be simultaneously diagonalizable.

Theorem 8.0.7. *All maximal tori (plural of "torus") of* $\mathsf{GL}(n)$ *are conjugate (so in particular conjugate to* $Diag(n)$*).*

Theorem 8.0.8. *Every subgroup* H *of* $\mathsf{GL}(n)$ *which is both commutative and all of its elements are diagonalizable, is conjugate to some subgroup of* $Diag(n)$*.*

Proof. Take $S = H$ in part b) of 8.0.1. $\square$

Example 8.0.9.

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}.$$

We have an (group) isomorphism

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in F \right\} \xrightarrow{\simeq} F$$

defined explicitly by

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \longmapsto a \in F.$$

Definition

Definition 8.0.10. Let F be an algebraically closed field. Then $s \in \mathsf{GL}(n, F)$ is **semisimple** if it is diagonalizable.

Definition

Definition 8.0.11. Let F be an algebraically closed field. Then $s \in \mathsf{GL}(n, F)$ is **unipotent** if $s - I$ is **nilpotent** $\Leftrightarrow (s - I)^m = 0$ for some $m \geqslant 1$.

Definition

Definition 8.0.12. If F is a field which is *not* algebraically closed, then $s \in \mathsf{GL}(n, F)$ is **semisimple** if $s \in \mathsf{GL}(n, \overline{F})$ is semisimple (in the sense of 8.0.10; i.e. diagonalizable), where $\overline{F}$ is an algebraic closure for F.

Definition

Definition 8.0.13. If F is a field which is not algebraically closed, then $s \in \mathsf{GL}(n, F)$ is **unipotent** if $s \in \mathsf{GL}(n, \overline{F})$ is unipotent (in the sense of 8.0.11), where $\overline{F}$ is an algebraic closure of F.

Definition

Definition 8.0.14. If G is an algebraic group, then $s \in G(F)$ is **semisimple** if for some *faithful* representation (2.0.11) $\varphi : G \to \mathsf{GL}(n)$, we have that $\varphi(s) \in \mathsf{GL}(n, \overline{F})$ is semisimple (8.0.10), and similarly for unipotent (8.0.11).

Theorem 8.0.15. *If $s \in G(F)$ is a semisimple respectively unipotent element, then for all faithful representations $\varphi : G \to \mathsf{GL}(n)$, $\varphi(s)$ is semisimple, respectively unipotent.*

Definition

Definition 8.0.16. A **Torus** T is an algebraic group such that
1. T is connected;
2. T is commutative;
3. Every element of T is semisimple.

Example 8.0.17. $\mathbb{G}_a(R) = (R, +)$ is connected and commutative, called the **additive group**, but none of its elements (other than 0) are semisimple. We have $\mathbb{G}_a \hookrightarrow \mathsf{GL}(2)$ defined by $r \longmapsto \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$.

Definition

Definition 8.0.18. Let F be a field. Then a group G is **unipotent** over F if g is unipotent, for all $g \in G$.

In [4]: One definition of unipotent group over more general rings R, is that G/R is unipotent if the only irreducible representation of G is the trivial one.

$\mathbb{G}_a$ is a unipotent group. The definition of unipotent is "elementwise". A naive conception is that "a group is unipotent if all of its elements are semisimple". A prototypical example of a semisimple group is $\mathsf{SL}(n)$ with unipotent elements such as

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

for $n \geqslant 2$.

8.0.1 and 8.0.15 (the latter not proven) together gives us that

1. Every torus of $\mathsf{GL}(n)$ is conjugate to a subtorus of $\mathrm{Diag}(n)$.
2. All maximal tori in $\mathsf{GL}(n)$ are conjugate.

Theorem 8.0.19. *Let G be an algebraic group over an algebraically closed field F. Then all maximal tori in G are conjugate.*

Example 8.0.20. Let

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \subset \mathsf{SL}(2, \mathbb{R}) \subset \mathsf{GL}(2, \mathbb{R}).$$

A is *semisimple* (8.0.10) since

$$A \sim_{\mathsf{GL}(2,\mathbb{C})} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

where $\sim_{\mathsf{GL}(2,\mathbb{C})}$ is the equivalence relation induced by the conjugacy-classes in $\mathsf{GL}(2,\mathbb{C})$. Hence A is a semisimple element according to 8.0.12. It is however not diagonalizable over $\mathbb{R}$, since As characteristic polynomial over $\mathbb{R}$ is x^2+1, which does not split.

Example 8.0.21. Let

$$T(R) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; a^2+b^2 \neq 0 \text{ and } a,b \in R \right\},$$

is a maximal torus in $\mathsf{GL}(2)_{\mathbb{R}}$, but it is not conjugate to $\mathrm{Diag}(2)_{\mathbb{R}}$ in $\mathsf{GL}(2)_{\mathbb{R}}$, but $T_{\mathbb{C}} \simeq \mathrm{Diag}(2)_{\mathbb{C}}$. In particular

$$\begin{aligned} T(\mathbb{R}) &\ncong \mathrm{Diag}(2,\mathbb{R}) \\ T(\mathbb{C}) &\cong \mathrm{Diag}(2,\mathbb{C}). \end{aligned}$$

T is called a **Deligne torus**.

A simpler example, is the following.

Example 8.0.22. Let S^1 denote the circle. Then

$$\begin{aligned} S^1(R) &= \left\{ (a,b) \in R^2 \;\middle|\; \begin{matrix} f(a,b) = 0 \\ f(x,y) = x^2+y^2-1 \end{matrix} \right\} \\ &= \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; \begin{matrix} a^2+b^2 = 1 \\ \begin{vmatrix} a & -b \\ b & a \end{vmatrix} = 1 \end{matrix} \right\}. \end{aligned}$$

S^1 is a maximal torus in $\mathsf{SL}(2)_{\mathbb{R}}$, and is a subgroup of the Deligne torus in the previous example. It is not conjugate to $\mathrm{Diag}^1(2)_{\mathbb{R}} \cong \mathrm{Diag}(1)_{\mathbb{R}}$ over $\mathbb{R}$, but $S^1_{\mathbb{C}}$ is conjugate to $\mathrm{Diag}^1(2)_{\mathbb{C}}$ in $\mathsf{GL}(2)_{\mathbb{C}}$.

Remark 8.0.23. Recall that $\mathrm{Diag}^1(n) = \left\{ \begin{pmatrix} t_1 & & \\ & \ddots & \\ & & t_n \end{pmatrix} \in \mathrm{Diag}(n) \;\middle|\; \prod_{i=1}^n t_i = 1 \right\}.$

So we have that

$$\begin{aligned} S^1(\mathbb{R}) &\ncong \mathsf{GL}(1,\mathbb{R}) \\ &= \mathbb{R}^\times \end{aligned}$$

Note that there is an isomorphism $\mathrm{Diag}^1(2) \to \mathrm{Diag}(1)$ given explicitly by

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \longmapsto t,$$

since

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

is completely determined by t. This is a group-homomorphism (hence not just a set-bijection). Here we note further that since $\mathrm{Diag}^1(2)_{\mathbb{R}} \cong \mathbb{R}^\times$, and the torsion-elements, i.e. elements of finite order, are only $\{\pm 1\} \subset \mathbb{R}^\times$, or $\mathbb{R}^\times_{\text{tors}} = \{\pm 1\}$. But in $S^1(\mathbb{R})$, we have the torsion-element

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

where

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

so that

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

has order 4. But we just saw that $\mathsf{GL}(1,\mathbb{R}) \cong \mathbb{R}^\times$ has no element of finite order 4. Therefore, since isomorphic groups need to have corresponding torsion elements of the same order for there to be a group-isomorphism between them, we can not have an isomorphism between $S^1(\mathbb{R})$ and $\mathrm{Diag}^1(2)_\mathbb{R}$. Instead, we claim that there is an isomorphism

$$\left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \,\middle|\, \begin{matrix} a^2+b^2=1 \\ a,b\in\mathbb{R} \end{matrix} \right\} \xrightarrow{\simeq} \left\{ a+bi \in \mathbb{C} \,\middle|\, \begin{matrix} a,b\in\mathbb{R} \\ a^2+b^2=1 \end{matrix} \right\},$$

defined explicitly as

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \longmapsto a+bi.$$

Definition

Definition 8.0.24. Let F be an algebraically closed field, and let G be an algebraic group. Then the **unipotent radical** $R_u(G)$ of G is the maximal, connected, normal, unipotent subgroup of G.

Definition

Definition 8.0.25. G is **reductive** if $R_u(G) = 1$.

Next time: Assume that $G \subset \mathsf{GL}(n,F)$ is a group. If G is unipotent (i.e., all its elements are unipotent), then there exists a $x \in \mathsf{GL}(n,F)$ such that $xGx^{-1} \subset \mathrm{Uniag}^+(n,F)$.

Chapter 9

Lecture 9: Solvable and Nilpotent groups

Recall that $u \in \mathsf{GL}(n, F)$ is unipotent (8.0.11) if $u - I$ is nilpotent.

We say that $A \in M_n(F)$ is nilpotent if $A^m = 0$ for some $m \geqslant 1$. This is equivalent to $A^n = 0$ (where n is from $M_n(F)$).

Recall:

Definition

Definition 9.0.1. $s \in M_n(F)$ is **semisimple** if s is diagonalizable in $M_n(k)$ where k is an algebraically closed field containing F, e.g. $k = \overline{F}$ an algebraic closure.

Fact: Every element of a Torus (6.0.6) is semisimple (9.0.1).

Let G be an algebraic group. Then $g \in G(F)$ is unipotent, respectively semisimple if for *some* (equivalently, *every*) faithful representation $G \xrightarrow{r} \mathsf{GL}(n)$, $r(g)$ is semisimple, respectively nilpotent.

Definition

Definition 9.0.2. Let k be an algebraically closed field. Then

1. G is unipotent if every element of $G(k)$ is unipotent.
2. The unipotent radical $R_u G$ of G is the maximal, connected, unipotent normal subgroup of G.
3. G is reductive if $R_u G = 1$.

Example 9.0.3. $\mathsf{SL}(2), \mathsf{GL}(2)$ are both reductive.

Example 9.0.4.

$$\mathsf{Uniag}^+(2) = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$$

is a unipotent algebraic subgroup of $\mathsf{SL}(2)$, but is highly not normal.

Definition

Definition 9.0.5. The **radical** $R(G)$ of G is the maximal, connected, normal solvable subgroup of G.

Example 9.0.6.

$$\begin{aligned} R(\mathsf{GL}(n)) &= Z_{\mathsf{GL}(n)} \\ &= \text{scalars} \\ &\cong \mathsf{GL}(1). \end{aligned}$$

In general, the unipotent radical is a subset of the radical, i.e. $R_uG \subset R(G)$, since $R_uG = (R(G))_u$, i.e. the unipotent radical of G is the set of unipotent elements in the radical $R(G)$ of G.

Definition

Definition 9.0.7. Let $G_u := \{g \in G \mid g \text{ is unipotent}\}$ and $G_u(F) := \{g \in G(F) \mid g \text{ is unipotent}\}$.

In general G_u is *not* a subgroup.

Theorem 9.0.8. *If G is a connected, solvable group, then G_u is a subgroup of G. Here $G_u \triangleleft G$.*

Example 9.0.9. (Prototypical examples)

$\mathsf{Triag}^+(n)$ is a connected solvable group. We then see that

$$(\mathsf{Triang}^+(n))_u = \mathsf{Uniag}^+(n) \triangleleft \mathsf{Triag}^+(n).$$

In general, the set G_u is stable under conjugation, i.e. G_u is a disjoint union of conjugacy classes. If G_u is a subgroup, it is normal.

Definition

Definition 9.0.10. Let G be a group. The commutator subgroup of G (can be written as G') is the subgroup of G generated by all the commutators $[a,b] := aba^{-1}b^{-1}$.

Notice that $[a,b] = 1 \Leftrightarrow ab = ba$. Also pay attention to the fact that the **set** of commutators $[a,b]$ may not form a subgroup (think about what it means that a subset of elements generates a group).

$$\begin{aligned} x[a,b]x^{-1} &= xaba^{-1}b^{-1}x^{-1} \\ &= (xax^{-1})(xbx^{-1})(xa^{-1}x^{-1})(xb^{-1}x^{-1}) \\ &= [xax^{-1}, xbx^{-1}] \end{aligned}$$

which implies that G' is normal in G (we get back a commutator for arbitrary elements $x \in G$). In fact, the stronger statement that G' is *characteristic* in G holds (we claim).

We also have $G^{\mathrm{ab}} = G/G'$, the abelianization of G. This is a *maximal* abelian quotient of G. If $N \triangleleft G$ and G/N is abelian, then $G' \subseteq N$.

Definition

Definition 9.0.11. Let $G^{(n)} := (G^{(n-1)})'$. Then G is **solvable** if $G^{(m)} = 1$ for some $m \geqslant 1$.

$G' = 1 \Leftrightarrow G$ is abelian. Another notation is that $G' = [G, G]$. If H_1, H_2 are subgroups of G then we define

$$[H_1, H_2]$$

as the subgroup generated by $\{[h_1, h_2] \mid h_1 \in H_1, h_2 \in H_2\}$. Note that $G^{(2)} = [G', G']$ and that $[G', G] \supset [G', G']$.

Let $G_{(n)} = [G, G_{(n-1)}]$ where

$$\begin{aligned} G_{(1)} &= [G, G] \\ &= G' \end{aligned}$$

and notice that this (and the previous definition for $G^{(n)}$) are **recursive** definitions). We have $G, [G, G], [G, (G, G)], \ldots, .$

Definition

Definition 9.0.12. We have that G is **nilpotent** if $G_{(n)} = 1$ for some $n \geqslant 1$.

Theorem 9.0.13. *If a group G is nilpotent $\Rightarrow G$ is solvable.*

Proof. Follows by definition. □

Example 9.0.14. For finite groups, G is nilpotent $\Leftrightarrow G$ is a direct product of its sylow subgroups.

Example 9.0.15. S_4 is solvable, but not nilpotent.

Example 9.0.16. $\mathsf{Uniag}^+(n)$ is nilpotent.

$G, Z_1 = Z_G$ and $Z_2 =$ preimage in G of $Z_{G/G_1} \subseteq G/Z_1$ so that $Z_1 \subset Z_2 \subset \ldots$. Then G is nilpotent if $Z_n = G$ for some $n \geqslant 1$.

Definition

Definition 9.0.17. A **Borel subgroup** of G is a *maximal* connected,solvable subgroup.

Example 9.0.18. $\mathsf{Triag}^+(n)$ is a Borel subgroup of $\mathsf{GL}(n)$.

For the structure of the proof that all maximal tori are conjugate:

(a) Theorem gives that all Borel subgroups of G are conjugate.

(b) Another theorem gives that all maximal tori of a connected solvable group are conjugate.

Definition

Definition 9.0.19. G is semisimple if $R(G) = 1$, where $R(G)$ is the radical of G (9.0.5).

Recall that a Lie-algebra $\mathfrak{g}$ is semisimple if $\mathfrak{g}$ is a direct sum

$$\mathfrak{g} = \mathfrak{g}_1 \oplus \ldots \oplus \mathfrak{g}_n$$

of simple Lie algebras $\mathfrak{g}_i$ (7.0.6).

Theorem 9.0.20. *G semisimple $\Leftrightarrow$ $\mathsf{Lie}(G)$ is semisimple.*

Definition

Definition 9.0.21. A root datum (5.0.7) $(X^*, \Phi; X_*, \Phi^\vee)$ is **semisimple** if

$$\begin{aligned}\mathrm{span}_{\mathbb{Q}} \Phi &= X^*_{\mathbb{Q}} \\ &= X^* \otimes_{\mathbb{Z}} \mathbb{Q}.\end{aligned}$$

Theorem 9.0.22. *A reductive group G is semisimple if and only if its root datum is semisimple (in the sense of 9.0.21).*

Chapter 10

Lie-Kolchin, characters and Jordan Decomposition

Unless otherwise specified, we assume that F is algebraically closed. Recall that we proved:

(a) If S is a commutative algebraic group with all elements semisimple, then S is *simultaneously diagonalizable.*

In Homework-2, we saw that if $a, b \in M_n(F)$ are both semisimple/nilpotent/unipotent and $ab = ba \Rightarrow ab$ is semisimple/nilpotent/unipotent.

(b) If $U \subseteq \mathsf{GL}(n, F)$ is unipotent (i.e. all elements are unipotent) then there exists a $g \in \mathsf{GL}(n, F)$ such that $gUg^{-1} \subseteq \mathsf{Uniag}^{+}(n, F)$.

We stated:

(c) Theorem (Lie-Kolchin): If $G \subseteq \mathsf{GL}(n, F)$ is connected and solvable, then there exists $x \in \mathsf{GL}(n, F)$ such that $xGx^{-1} \subset \mathsf{Triag}^{+}(n)$.

Another way it seems to state Lie-Kolchin is the following way.

Theorem

Theorem 10.0.1. *Let G be a linear algebraic, connected, solvable group. If there exists a representation $r : G \to \mathsf{GL}(V)$ where V is finite-dimensional and r is irreducible, then r must be of dimension 1, i.e. the action is by scalars, so that $r(g) = \lambda \in F^{\times}$ for all $g \in G$. Perhaps more generally, if r is not neccessarily irreducible then there must be a 1-dimensional subspace $W \subset V$, in the sense that $r(g)(W) \subset W$ for all $g \in G$ (and then the former conclusion follows directly when r is irreducible).*

Very general: If we have an action $G \curvearrowright X \rightsquigarrow$ an action $G \curvearrowright \mathrm{Fun}(X, k)$ defined explicitly as

$$G \times \mathrm{Fun}(X, k) \ni (g, f) \mapsto g \cdot f$$

defined on $x \in X$ as $(g \cdot f)(x) = f(g^{-1}(x))$ (here $\mathrm{Fun}(X, k) = X^{\vee}$, so we can see this induced action as the **dual action** induced from the original group action).

For Lie-Kolchin: If H char G this induces an action $\mathrm{Aut}(H) \curvearrowright G$ which then in turn induces a dual action $\mathrm{Aut}(H) \curvearrowright X^*(H)$, where

$$X^*(H) := \mathrm{Hom}_{\text{alg. groups}}(H, \mathsf{GL}(1)).$$

Explicitly, we have

$$\mathrm{Aut}(H) \times X^*(H) \to X^*(H)$$

defined explicitly as $\mathrm{Aut}(H) \times X^*(H) \ni (\sigma, \chi) \mapsto \sigma\chi \in X^*(H)$ which acts on $h \in H$ as $(\sigma\chi)(h) = \chi(\sigma^{-1}(h))$.

Recall that we have $\mathbb{G}_m$ where $m =$ multiplicative, and $\mathbb{G}_m = \mathsf{GL}(1)$, $R \mapsto R^\times$ and $F \mapsto F^\times$. If $g \in H$, then $g \cdot \chi = \chi$, since

$$\begin{aligned} \chi(g^{-1}hg) &= \chi(g)^{-1}\chi(h)\chi(g) \\ &= \chi(h). \end{aligned}$$

This is because $G \curvearrowright X^*(H)$ then takes g to $\mathrm{int}(g)$ which acts on x as gxg^{-1} so then $g \cdot \chi$ acts on h as

$$\begin{aligned} (g \cdot \chi)(h) &= \chi(g^{-1} \cdot h) \\ &= \chi(g^{-1}hg) \\ &= \chi(h), \end{aligned}$$

since the image of $\chi, \mathsf{GL}(1)$, is commutative and χ is a homomorphism.

Proof. As in the unipotent case, we proceed by induction, so it enough to show:

<u>1st reduction</u>: G has a <u>simultaneous e-vector</u> $v \in F^n$ such that $gv = \lambda_g v$ for all $g \in G$ and where λ_g is a scalar e-value that depend on g. We then extend v to a basis for F^n, the matrix of every $g \in G$ is block-upper triangular on the form

$$\begin{bmatrix} \lambda_g & A \\ 0 & B \end{bmatrix}$$

Then repeat (by induction) with $G \curvearrowright F^n \big/ \mathrm{span}(v)$.

Remark 10.0.2. Notice that $g \overset{\chi}{\longmapsto} \lambda_g$ is a homomorphism $G \to \mathsf{GL}(1) = F^\times$.

Proof.

$$\begin{aligned} (gh)v &= \lambda_g\lambda_h v \\ &= \chi(g)\chi(h)v \\ &= \chi(gh)v. \end{aligned}$$

□

Recall that the image of a connected set under a continuous function is connected. We have

$$G \longrightarrow \mathrm{Aut}\left(F^n \big/ \mathrm{span}(v)\right) = \mathsf{GL}\left(F^n \big/ \mathrm{span}(v)\right).$$

If G is connected, then the image is connected, and if G is solvable, then the image is solvable.

<u>Useful fact about solvable groups</u>:

$$1 \to N \hookrightarrow G \twoheadrightarrow G/N \to 1$$

where $N \triangleleft G$, then $G/N, N$ solvable $\Leftrightarrow G$ solvable.

<u>2nd reduction</u>: Look at $[G,G] = G'$, the commutator subgroup of G. We have that $G' \subsetneqq G$ since G is solvable; to expand on this point, note that by 9.0.11 we need there to be some $m \geqslant 1$ such that $G^{(m)} = 1$, where $G^{(1)} = G'$. But if $G' = G$, then we get "stuck" at G so we can not reach 1. If G is solvable $\Rightarrow G'$ is solvable (we can start the series from G' instead of G).

<u>Exercise</u>: Show that if G is connected, then G' is connected (perhaps see [8]).

By induction on the dimension of G, we may assume that this holds for G'. So assume that the theorem holds for G', then we want to show that it holds for G. We look at $G \overset{X}{\hookrightarrow}{}^{*}(H)$ with $H = G'$, and note that G' char G. Let $\chi \in X^*(H)$. Then the **weight-space** of χ is

$$F^n_\chi := \{v \in F^n \ : \ h \cdot v = \chi(h)v, \forall h \in H\}.$$

Here F^n_χ can be zero. In fact, $F^n_\chi = 0$ for all but at most n distinct characters.

By assumption, there exists a $\chi \in X^*(H)$ such that $F^n_\chi \neq 0$, and this is because $G' \subsetneqq G$ and we found that $\exists v \in F^n$ such that

$$\begin{aligned} h \cdot v &= \lambda_g v \\ &= \chi(h)v, \end{aligned}$$

for all $h \in H = G'$. Hence taking χ as the morphism $g \overset{\lambda}{\longmapsto}_g$ gives us a non-zero weight space.

If F^n_χ is G-stable, we win. <u>Claim</u>: $g(F^n_\chi) = F^n_{g\chi}$.

Notice that if we take χ such that $F^n_\chi \neq 0$, and $v \in F^n_\chi$, then $gv \in F^n_{g\chi}$, since

$$\begin{aligned} h(gv) &= g(g^{-1}hgv) \\ &= g \cdot \chi(g^{-1}hg)v \\ &= \chi(g^{-1}hg)gv \\ &= (g\chi)(h)gv, \end{aligned}$$

which shows that, indeed, $gv \in F^n_{g\chi}$, where we used the normality of $H = G'$ in G in the second equality.

Consider the action $G \curvearrowright \{\chi' \mid F^n_{\chi'} \neq 0\}$ where the the set G acts on is non-empty by assumption. This induces a group homomorphism from G to $S_{\left\{\chi' \,:\, F^n_{\chi'} \neq 0\right\}}$. We claim that if G is connected, then $g\chi = \chi, \forall g \in G$. Since $\{g \in G \mid g\chi = \chi\} \subset G$ is defined by polynomial equations, it is closed, where $\chi : H \to \mathbb{G}_m \subset \mathbb{A}^1$ is a **regular function** (roughly defined by polynomial equations).

- $[H : G] = n < \infty$ so that $G(k) = \bigsqcup_{i=1}^n g_i H$.

- Assuming that each g_i acts as a homeomorphism on H, it follows that $g_i H$ is closed for every $i = 1, \dots, n$. Then also all $g_i H$ is open (in the zariski-topology; it is the complement of a closed set of a union of other [closed] cosets). Therefore the cosets disconnect G.

But this means that (by our earlier claim)

$$\begin{aligned} g(F^n_\chi) &= F^n_{g\chi} \\ &= F^n_\chi, \end{aligned}$$

so that F^n_χ is G-stable. If $F^n_\chi \subsetneqq F^n$ then apply induction to the image of $G \to \mathsf{GL}(F^n_\chi)$.

If $F^n_\chi = F^n$ then this means that $hv = \chi(h)v, \forall v \in V, \forall h \in H$, i.e. H acts by <u>scalars</u> on F^n. Recall that

$$H = G' \subset G \subset \mathsf{GL}(n).$$

We have

$$\begin{aligned}\det[x,y] &= \det(xyx^{-1}y^{-1}) \\ &= \det(x)\det(y)\det(x)^{-1}\det(y)^{-1} \\ &= 1,\end{aligned}$$

so that $H \subset \mathsf{SL}(n)$. Hence $H \subset \{\lambda I\} \cap \mathsf{SL}(n) \rightsquigarrow H = \{\lambda I \ : \ \lambda^n = 1\}$, i.e. $\lambda \in \mu_n$, the group of n^{th} roots of unity. Hence H is finite (since there are only finitely many such λ) and connected. Therefore, since $H = \{h_1, \ldots, h_n\}$ and each $\{h_i\}$ is closed, but notice that $H \setminus \{h_i\}$ is a union of a finite number of closed set, so is closed, therefore $\{h_i\}$ is also open. So unless H is trivial, i.e. $H = \{e\}$ there will be non-trivial clopen sets in H, and therefore H can not be connected (X space then X connected $\Leftrightarrow$ the only *clopen sets* are $X, \varnothing$). If $H = G'$ is trivial, i.e. $G' = 1 \Rightarrow G$ is commutative. Then by (I presume) 8.0.3 it follows that G is simultaneously triagonalizable. $\square$

We want to prove that $X^*(\mathrm{Diag}(n)) = \mathbb{Z}^n$, where we think of $\mathrm{Diag}(n)$ as an algebraic group over F, where F is *algebraically closed* in the sense of varieties, and $X^*(\mathrm{Diag}(n)) = \mathrm{Hom}_{\text{alg. groups}}(\mathrm{Diag}(n), \mathbb{G}_m)$, morphism of varieties that are also group homomorphisms.

10.0.1 Linear independence of characters

Let Γ be a group (not algebraic group), and let F be a field (which need not be algebraically closed), so that $X^*(\Gamma) = \{\mathrm{Hom}_{\text{group.hom.}}(\Gamma, F^\times)\} \subset \mathrm{Fun}(\Gamma, F)$, and note that $\mathrm{Fun}(\Gamma, F) = \Gamma^\vee$ is a vector-space over F.

Theorem 10.0.3. *$X^*(\Gamma)$ is a linearly independent set.*

Proof. Assume that

$$\sum_{\chi \in X^*(\Gamma)} a_\chi \chi = 0$$

is a linearly dependent relation, where only *finitely many* $a_\chi \neq 0$. Let

$$a_1\chi_1 + \ldots + a_n\chi_n$$

be the minimal such relation (works since $\mathbb{N}$ is well-ordered), and the χ_i are *distinct*.

Therefore, we have that

$$a_1\chi_1(g) + \ldots + a_n\chi_n(g) = 0, \forall g \in \Gamma \tag{10.0.1}$$

and

$$a_1\chi_1(gh) + \ldots + a_n\chi_n(gh) = 0, \forall g, h \in \Gamma.$$

Since all χ_i are characters (so homomorphisms), it follows that

$$a_1\chi_1(g)\chi_1(h) + \ldots + a_n\chi_n(g)\chi_n(h). \tag{10.0.2}$$

If we multiply 10.0.1 with $\chi_1(h)$ we get

$$a_1\chi_1(g)\chi_1(h) + a_2\chi_2(g)\chi_1(h) + \ldots + a_n\chi_n(g)\chi_1(h). \tag{10.0.3}$$

If we subtract 10.0.3 from 10.0.2 we get

$$a_2(\chi_2(h) - \chi_1(h))\chi_2(g) + \ldots + a_n(\chi_n(h) - \chi_1(h))\chi_n(g) = 0. \tag{10.0.4}$$

Since e.g. $\chi_1 \neq \chi_2$ there exists h such that $\chi_1(h) \neq \chi_2(h) \Rightarrow \chi_2(h) - \chi_1(h) \neq 0$.

Therefore $a_2(\chi_2(h) - \chi_1(h))\chi + \ldots + a_n(\chi_n(h) - \chi_1(h))\chi_n = 0$, with not all coefficients zero. This contradicts the minimality of n. $\square$

$X^*(\mathbb{G}_m) = X^*(\mathrm{Diag}(1))$.

recall: $\mathsf{GL}(n, F) = \mathcal{Z}(\det(a_{ij}) \cdot t - 1)$, which we can view as a subset of F^{n^2+1}, and that $M_n(F) = F^{n^2}$. Note here that have that $\det(a_{ij}) \cdot t - 1$ is an equation in $F[a_{11}, a_{12}, \ldots, a_{(n-1)n}, a_{nn}, t]$, from which $n^2 + 1$ in F^{n^2+1} is derived.

We have $\mathsf{GL}(1) = \mathcal{Z}(xy - 1) \subset F^2 = \mathbb{A}^2(F)$.

Remark 10.0.4. $\mathbb{A}^n$ = "affine n-space" $= \mathcal{Z}(0)$, where, roughly "$\mathbb{A}^n = F^n$" (but where $\mathbb{A}^n$ is endowed with a topology, the Zariski-topology). Perhaps functorially, we then have $\mathbb{A}^n(R) = R^n$.

We have $A(\mathcal{V}) = F[x_1, \ldots, x_n]/I_{\mathcal{V}}$ and $A(\mathsf{GL}(1)) = F[x, y]/(xy - 1) \cong F[x, x^{-1}]$, which are Laurent-polynomials. We have $X^*(\mathbb{G}_m) \subset A(\mathsf{GL}(1)) = F[x, x^{-1}]$ and $\chi_n(x) = x^n \in X^*(\mathsf{GL}(1))$ for $n \in \mathbb{Z}$.

Proof that $X^*(\mathsf{GL}(1)) = \mathbb{Z} = \{\chi_i \mid i \in \mathbb{Z}\}$:

Proof. Assume that $\chi \in X^*(\mathsf{GL}(1)) \Rightarrow \chi = \displaystyle\sum_{i=m}^{i=n} a_i \chi_i$ for $m, n \in \mathbb{Z}$ and $m \geqslant n$. If $\chi \neq \chi_j$ for some j, then

$$\chi - \sum_{i=m}^{i=n} a_i \chi_i = 0$$

is a linearly dependent relation among the characters $\chi, (\chi_i)_{i=m}^{i=n}$ contradicting 10.0.3. Since χ_n for $n \in \mathbb{Z}$ are characters, we already have the reverse inclusion $\mathbb{Z} \subseteq X^*(\mathsf{GL}(1))$ so this shows that $\mathbb{Z} = X^*(\mathsf{GL}(1))$. ☐

WARNING: More advanced material: Let $F = \mathbb{C}$ and consider group homomorphisms $\mathbb{C} \longrightarrow \mathbb{C}$, and in particular $z \xrightarrow{\varphi_{ab}} z^a \overline{z}^b$, where $z = x + iy$ so that $\overline{z} = x - iy$ denotes complex conjugation. Then φ_{ab} does not arise as $\psi(\mathbb{C})$ for $\psi \in X^*(\mathsf{GL}(1))$ if $b \neq 0$, but $\varphi_{a,b} = \psi_{a,b}(\mathbb{R})$ where $\psi_{a,b} : \mathbb{S} \to \mathbb{S}$ and $\mathbb{S} = \mathrm{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{G}_{m,\mathbb{C}}$. It is easiest to think of $\mathbb{S}$ as a **group functor**:

$$\begin{aligned} \mathbb{S}(\mathbb{R}) &= \mathbb{G}_{m,\mathbb{C}}(\mathbb{C}) \\ &= \mathbb{C}^\times \\ \mathbb{S}(A) &= \mathbb{G}_{m,\mathbb{C}}(A \otimes_{\mathbb{R}} \mathbb{C}), \end{aligned}$$

in the latter case for A an $\mathbb{R}$-algebra.

Remark 10.0.5. the characters $z^a \overline{z}^b$ of $\mathbb{S}$ arise naturally in hodge-theory.

Remark 10.0.6. (Res)

We have that Res = "restriction of scalars", and this works for all finite field extensions K/F and for all algebraic groups G. If G is an algebraic group over K then $(\mathrm{Res}_{K/F} G)(A) = G(A \otimes_F K)$, where A is an F-algebra.

$X^*(\mathrm{Diag}(1)) = \mathbb{Z}$, and

$$\begin{aligned} \mathrm{Diag}(n) &= \mathrm{Diag}(1)^n \\ &= \underbrace{\mathrm{Diag}(1) \times \cdots \times \mathrm{Diag}(1)}_{n \text{ times}}. \end{aligned}$$

We have $X^*(G \times H) = X^*(G) \times X^*(H)$ where in the right-hand side we have elements (χ, ψ) such that $(\chi, \psi)(g, h) = \chi(g)\psi(h)$, and this corresponds to $\gamma \in X^*(G \times H)$ such that $\gamma_1(g) := \gamma(g, 1)$ is a character of G. Hence $X^*(\mathrm{Diag}(n)) = \mathbb{Z}^n$. Let F be algebraically closed.

Theorem 10.0.7 (Additive Jordan Decomposition)**.** *Assume* $A \in M_n(F) \Rightarrow \exists! A_s, A_n \in M_n(F)$ *such that*

(1) $A = A_s + A_n$*;*

(2) A_s *is semisimple, and* A_n *is nilpotent;*

(3) $A_s A_n = A_n A_s$*.*

Theorem 10.0.8 (Multiplicative Jordan Decomposition)**.** *Assume* $A \in \mathsf{GL}(n, F) \Rightarrow \exists! A_n, A_u \in \mathsf{GL}(n, F)$ *such that*

(1) $A = A_s A_u$*;*

(2) A_s *semisimple,* A_u *unipotent;*

(3) $A_s A_u = A_u A_s$*.*

Remark 10.0.9. Note that A_s is the same in both the multiplicative and additive version, for fixed $A \in \mathsf{GL}(n, F)$.

Theorem 10.0.10 (Jordan Decomposition for algebraic groups)**.** *Let* G *be an algebraic group. Assume* $g \in G \Rightarrow \exists! g_s, g_u$ *such that*

(1) $g = g_s g_u$*;*

(2) g_s *semisimple, and* g_u *unipotent;*

(3) $g_s g_u = g_u g_s$*;*

(4) For all homomorphisms $\varphi : G \to \mathsf{GL}(n)$ *of algebraic groups, we have that* $\varphi(g) = \varphi(g)_s \varphi(g)_u$ *(coming from the multiplicative jordan decomposition).*

Theorem 10.0.11 (Jordan for semisimple Lie algebras)**.** *Let* $\mathfrak{g}$ *be a semisimple Lie algebra (7.0.13). Assume* $A \in \mathfrak{g} \Rightarrow \exists A_s, A_n$ *such that*

(1) $A = A_s + A_n$*;*

(2) A_s *is semisimple, and* A_n *is nilpotent;*

(3) $A_s A_n = A_n A_s$*;*

(4) For all homomorphisms of Lie algebras φ*, we have* $\varphi(A) = \varphi(A)_s + \varphi(A)_n$*.*

Remark 10.0.12. If F is not algebraically closed $\rightsquigarrow G(F) \subset G(\overline{F})$ so $g \in G(F)$ will have a jordan decomposition $g = g_s g_u$ with $g_s, g_u \in G(\overline{F})$.

Question: Does $g \in G(F) \Rightarrow g_s, g_u \in G(F)$?

Answer: "Mostly yes, *exotically no*". In particular, in characteristic 0, yes.

Definition

Definition 10.0.13. In characteristic $p > 0$, a field F is called **perfect** if

$$\begin{aligned} F &= F^p \\ &= \{a^p \mid a \in F\}, \end{aligned}$$

i.e. each element of F is a p-root.

Theorem 10.0.14. *F is perfect $\Leftrightarrow \forall g \in F[x]$ that are irreducible, g is separable (has no multiple roots). In particular, finite fields, and algebraically closed fields, are perfect fields.*

Example 10.0.15 (Imperfect field)**.** Take $\mathbb{F}_p(t)$, i.e. we adjoin the indeterminate t to $\mathbb{F}_p$ (so this is a transcendental extension). Assume that $t \in (\mathbb{F}_p(t))^p$. Since $x^p - t \in \mathbb{F}_p[t]$ is irreducible (apply Eisensteins criterion since (t) is a prime-ideal in $\mathbb{F}_p[t]$), it is irreducible in $\mathbb{F}_p(t)[x]$ by generalized Gauss Lemma (note here that $\mathbb{F}_p(t)$ is the field of fractions of $\mathbb{F}_p[t]$). But $x^p - t$ splits completely into linear factors, hence can not be irreducible (note that $s \in \mathbb{F}_p(t)$).

We have that $g_s, g_u \in G(F)$ if F is perfect. This can fail if F is imperfect. Recall that $R_u G$ is the unipotent radical of G (8.0.24). G is reductive if $R_u G = 0$ (where F is algebraically closed). If F is not algebraically closed, then G/F is reductive if $G/\overline{F}$ is reductive.

- ${}_F R_u G =$ maximal connected normal unipotent subgroup $/F$,
- $R_u G =$ maximal connected normal unipotent subgroup $/\overline{F}$.

If F is perfect and ${}_F R_u G = 0$ then $R_u G = 0$, and G is reductive. But if F is not perfect then there exists G such that ${}_F R_u G = 0$ but $R_u G \neq 0$ (over $\overline{F}$), so G is not reductive. Such G are called **pseudo-reductive**.

Going back to our theorems about Jordan Decomposition, notice that

$$\begin{aligned} A &= A_s + A_u \\ \Rightarrow A &= A_s(1 + A_s^{-1} A_u) \end{aligned}$$

(given $A_s \in \mathsf{GL}(n, F)$, atleast).

Remark 10.0.16 (About Jordan Decomposition)*.* A_s, A_n are polynomials in $A = (a_{ij})$.

10.0.2 Generalized e-spaces

Let $A \in M_n(F)$ and F algebraically closed, such that $(A - \lambda I)v = 0$, and let $F^n_\lambda = \{v \in F^n \mid Av = \lambda v\}$ be an e-space. Then A is a direct sum ($\oplus$) of its e-spaces $\Leftrightarrow$ A is diagonalizable.

We have the **generalized eigenspace**

$$F^n_{\text{gen-}\lambda} := \{v \in F^n \mid (A - \lambda I)^m = 0, \text{ for some } m \geqslant 1\} \tag{10.0.5}$$

i.e. so that $(A - \lambda I)^m$ acts *nilpotently* on $v \in F^n$. For all A (diagonalizable or not)

$$F^n = \bigoplus_{\lambda \in \Lambda} F^n_{\text{gen-}\lambda}$$

where Λ is the set of eigenvalues of A.

In terms of Jordan Normal Form we have that the jordan block of dimension $n \times n$

$$\begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ 0 & 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 0 & 0 & 0 & 0 & \lambda \end{bmatrix}$$

has λ as its only eigenvalue so in light of 10.0.5 we have that $F^n = F^n_{\text{gen-}\lambda}$, and also note that

$$A - \lambda I = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

is nilpotent on all of F^n.

Chapter 11

Dimension and Root space revisited, and Lie Groups connection

Plan:

- Dimension (was used in Lie-Kolchin).
- Jordan Decomposition - proof.
- Consequences of theorems on unipotent + solvable groups $\rightsquigarrow$ unipotent radical.

If we go back to the correspondence between connected reductive groups over algebraically closed fields and root data, we now know more. We have seen the "root Weyl-group"

$$\mathcal{W} = \langle S_\alpha \mid \alpha \in \Phi \rangle.$$

We want to see "normalizer of maximal torus weyl group" (the two are isomorphic with good hypothesis). We have **Flag varieties** which provides a link between (*affine*) algebraic groups and flag varieties (which are *projective*). Connected to this is also *representations* (2.0.11) of reductive groups.

11.0.1 Dimension

Definition

Definition 11.0.1. Let X be a topological space. The **dimension** of X, $\dim X$, is the maximal lenght n of a chain

$$X_0 \subsetneqq X_1 \subsetneqq \ldots \subsetneqq X_n \subset X$$

of *closed*, *irreducible* subsets of X, if such an n exists; otherwise $\dim X = \infty$.

Remark 11.0.2. A subset $Y \subset X$ of a space X is **irreducible** if there are no proper subsets $Y_1, Y_2 \subset Y$ such that $Y = Y_1 \cup Y_2$ and Y_1, Y_2 are closed in Y. Let

- k algebraically closed.
- Let $Y \subset \mathbb{A}^n(k) = k^n$ be algebraic (= Zariski-closed/defined by polynomial equations).

Then Y irreducible $\Leftrightarrow$ $\mathcal{I}(Y)$ is a prime ideal.

Definition

Definition 11.0.3. Let R be a commutative ring with 1. Then the **Krull-Dimension** of R is the maximal lenght n of a chain

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_n \subsetneqq R$$

of prime-ideals $\mathfrak{p}_i \subset R$, if such n exists; otherwise $\dim R = \infty$ (compare with the dimension of a topological space X).

Example 11.0.4. $\dim \mathbb{Z} = 1$, and more generally $\dim R = 1$ if R is a principal ideal domain (PID) since

1. R is then a domain, so that (0) is a prime-ideal (there are no zero-divisors);
2. Every non-zero prime ideal is maximal.

Hence $(0) \subset (p)$ are the maximal chains in $\mathbb{Z}$; or more generally $(0) \subset P$ maximal chain in R when R is a PID.

Example 11.0.5 (Dimension of a field)**.** Recall that $(0), (1)$ are the only ideals in a field, hence $\dim(F) = 0$ for a field F with maximal chain $(0) \subsetneqq F$.

Non-trivial fact: $\dim k[x_1, \ldots, x_n] = n$ with chain

$$(0) \subsetneqq (x_1) \subsetneqq (x_1, x_2) \subsetneqq \ldots \subsetneqq (x_1, \ldots, x_n) \subsetneqq k[x_1, \ldots, x_n]$$

is the maximal chain.

Definition

Definition 11.0.6. If $\mathfrak{p}$ is a prime ideal, the **height** of $\mathfrak{p}$, $\operatorname{ht} \mathfrak{p}$, is the length n of a maximal chain of prime ideals

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_n = \mathfrak{p},$$

and $\operatorname{ht} \mathfrak{p} = \infty$ otherwise.

Example 11.0.7 (Height in PID/Domain)**.** In a PID, every non-zero prime ideal is a height 1 prime. In a domain, the height 1 primes are the *minimal* non-zero prime ideals.

Fact: If $\mathfrak{p}$ is a prime and $Y = \mathcal{Z}(\mathfrak{p}) \subset \mathbb{A}^n(k)$ then

$$\dim Y = \dim(\mathbb{A}^n) - \operatorname{ht} \mathfrak{p}.$$

In general, $\dim A(Y) = \dim Y, \forall$ algebraic sets Y (where $A(Y)$ is the *coordinate ring*). Furthermore, we have that

$$\begin{aligned} \dim \mathbb{A}^n(k) &= \dim k[x_1, \ldots, x_n] \\ &= n \end{aligned}$$

Since $\dim \mathbb{A}^n = n$ and $\dim Y = \dim \mathbb{A}^n - \operatorname{ht} \mathfrak{p}$ for some prime $\mathfrak{p}$ (under the assumption that $Y = \mathcal{Z}(\mathfrak{p})$) it follows that $\dim Y \leqslant n$.

Example 11.0.8. $\dim k[x,1 \ldots, x_n, \ldots] = \infty$.

This gives us the dimension of an algebraic group. Recall that a connected algebraic group is irreducible. So if G is connected and $H \subsetneqq G$ is connected, then $\dim H < \dim G$. Let

$$X_0 \subsetneqq X_1 \subsetneqq \ldots \subsetneqq H \subsetneqq G,$$

where all X_i are closed and irreducible, then the chain including H will always be longer. One can do induction on the dimension of G, as in the proof of Lie-Kolchin.

If $Y \subset \mathbb{A}^n$ is algebraic, we can define algebraically the **tangent space** T_xY at $x \in Y$, which is a k-vector space. We have that $\dim T_xY = \dim Y$ if Y is *smooth*. In connection with this, we have that $\mathsf{Lie}(G) = T_1G$, i.e. the tangent space at the group-identity $1 \in G$. Then

$$\begin{aligned}\dim G &= \dim \mathsf{Lie}(G) \\ &= \dim T_1G,\end{aligned}$$

where $\dim T_1G = \dim_k T_1G$ is the dimension of T_1G as a vector-space over k. This can be helpful to compute dimensions.

Example 11.0.9 (Symplectic/Orthogonal)**.** Let $\mathcal{J}$ be symmetric ($\mathcal{J} = {}^t\mathcal{J}$) or anti-symmetric (${}^t\mathcal{J} = -\mathcal{J}$) in $\mathsf{GL}(n, k)$.

We have

$$G^{\mathcal{J}} = \{A \in \mathsf{GL}(n, \Bbbk) \mid {}^tA\mathcal{J}A = \mathcal{J}\}$$

which is *orthogonal* if $\mathcal{J}$ is symmetric and *symplectic* if $\mathcal{J}$ is anti-symmetric. Then it follows that

$$\mathsf{Lie}(G^{\mathcal{J}}) = \{A \in M_n(\Bbbk) \mid {}^tA\mathcal{J} + \mathcal{J}A = 0\}.$$

Example 11.0.10 ($\mathcal{J} = I$)**.** Let $\mathcal{J} = I$. Then

$$\begin{aligned}G^I(\Bbbk) &= \{A \in \mathsf{GL}(n, \Bbbk) \mid {}^tAA = I\} \\ &= \mathrm{SO}^I(n).\end{aligned}$$

We have

$$\begin{aligned}\mathsf{Lie}(\mathsf{SO}^I(n)) &= \mathfrak{so}(n) \\ &= \{A \in M_n(\Bbbk) \mid {}^tA + A = 0\} \\ &= \{A \in M_n(\Bbbk) \mid {}^tA = -A\} \\ &= \text{Antisymmetric matrices in } M_n(\Bbbk).\end{aligned}$$

We may ask how many such matrices there are. Notice that we are looking for such matrices in $M_n(\Bbbk)$ and not neccessarily $\mathsf{GL}(n, \Bbbk)$, which gives fewer restrictions. In fact, we note that if we let $A = (a_{ij})$, then since we have ${}^tA + A = 0$, this implies that $2a_{ii} = 0$ for all $1 \leqslant i \leqslant n$. Since $a_{ii} \in \Bbbk$, and $\Bbbk$ is a *field*, it follows that $a_{ii} = 0$ for $1 \leqslant i \leqslant n$.

Then notice that by definition of the transpose, we have that $a_{ji} = -a_{ij} \Leftrightarrow -a_{ji} = a_{ij}$ for $i > j$. We see that for $i = 1$, there is no such element. For $i = 2$ there is one such element, a_{21}, and generally, for column m where $1 \leqslant m \leqslant n$, there are $m - 1$ such elements. These elements above the main diagonal completely determines the elements below the diagonal.

Lemma

Lemma 11.0.11.

$$1 + 2 + \ldots + (n-1) = \frac{n(n-1)}{2}, \qquad n \geqslant 2, n \in \mathbb{N}.$$

Proof. We proceed by induction. Base case $n = 2$: We have

$$\frac{2(2-1)}{2} = 1.$$

Inductive assumption and inductive step: Assume it holds for $n = k$. We want to show that it holds for $n = k + 1$. We have

$$\begin{aligned} 1 + 2 + \ldots + (k-1) + (k+1-1) &= \frac{k(k-1)}{2} + k \\ &= \frac{k(k-1) + 2k}{2} \\ &= \frac{k(k-1+2)}{2} \\ &= \frac{k(k+1)}{2} \\ &= \frac{(k+1)(k)}{2} \\ &= \frac{(k+1)((k+1)-1)}{2}, \end{aligned}$$

which is what we wanted to show. □

Therefore, by 11.0.11 we get that

$$\begin{aligned} \dim \big(\mathsf{Lie}(SO^I(n)\big) &= \sum_{m=1}^{n} (m-1) \\ &= 1 + 2 + \ldots + (n-1) \\ &= \frac{n(n-1)}{2}. \end{aligned}$$

Example 11.0.12. By the above calculations, and recalling that $\dim G = \dim \mathsf{Lie}(G)$ (as a vector space over $\Bbbk$), we have that

$$\begin{aligned} \dim(\mathsf{SO}(3)) &= \dim(\mathsf{SO}^I(3)) \\ &= \dim(\mathsf{Lie}(\mathsf{SO}^I(3)) \\ &= \frac{3 \cdot 2}{2} \\ &= 3. \end{aligned}$$

Example 11.0.13 ($\mathsf{SO}(4)/\{\pm I\}$)**.** We have

$$\mathsf{SO}(4)/\{\pm I\} \cong \mathsf{SO}(3) \times \mathsf{SO}(3),$$

where the left-hand side is of type D_2, and the right-hand side is of type $\mathsf{A}_1 \times \mathsf{A}_1$, which we claim are isomorphic as root systems. Furthermore, we claim that $Z(\mathsf{SO}(4)) = \{\pm I\}$.

Remark 11.0.14. Notice that

$$\begin{aligned} \det(-I_{2n+1})) &= (-1)^{2n+1} \\ &= -1, \\ \Rightarrow -I_{2n+1} \notin \mathsf{SO}(2n+1) &= \mathsf{SL}(2n+1) \cap \mathsf{O}(2n+1), \end{aligned}$$

but

$$\begin{aligned}\det(-I_{2n}) &= (-1)^{2n} \\ &= 1, \\ \Rightarrow -I_{2n} &\in \mathsf{SL}(2n).\end{aligned}$$

Example 11.0.15.

$$\begin{aligned}\dim \mathsf{SO}(3) &= \frac{3 \cdot 2}{2} \\ &= 3.\end{aligned}$$

$$\mathsf{SU}(2) \twoheadrightarrow \mathsf{SO}(3)$$

and

$$\mathsf{SO}(4)/\{\pm I\} \cong \mathsf{SO}(3) \times \mathsf{SO}(3).$$

We have

$$\frac{4 \cdot 3}{2} = 3 + 3 = 6.$$

Furthermore, we claim that $\mathsf{SO}(6) \cong \mathsf{SL}(4)/\{\pm I\}$. We have

$$\frac{6 \cdot 5}{2} = 15.$$

Generally, $\dim \mathsf{SL}(n)$ = dimension of traceless-matrices $= n^2 - 1$.

We have that $\mathsf{SO}(4)/\{\pm I\} \cong \underbrace{\mathsf{SO}(3) \times \mathsf{SO}(3)}_{\text{adjoint group}}$ (6.0.23), so that its center is trivial. We have that $Z(\mathsf{SO}(4)) = \{\pm I\}$ so that

$$\mathsf{SO}(4)/\{\pm I\} = \mathsf{SO}(4)/Z(\mathsf{SO}(4)). \tag{11.0.1}$$

Furthermore, recall that $\mathsf{D}_2 \cong \mathsf{A}_1 \times \mathsf{A}_1$.

We have

$$\begin{tikzcd} \underbrace{\mathsf{SL}(4)/\{\pm I\}}_{\mathsf{A}_3} \arrow[r, shift left, "\sim"] \arrow[r, shift right, "\cong"'] & \underbrace{\mathsf{SO}(6)}_{\mathsf{D}_3} \end{tikzcd}$$

Simply connected

Remark 11.0.16. It seems like we want $\mathsf{SL}(n, F)$ with $n \geqslant 2$ and F algebraically closed for $\mathsf{SL}(n, F)$ to be simply connected. Recall 6.0.20 which says that a root datum is adjoint if $\mathbb{Z}\Phi^\vee = X_*(\mathsf{Diag}^\circ(n))$. We claim that $Z(\mathsf{SL}(4)) = \mu_4$, the 4^{th} roots of unity and that $Z(\mathsf{SO}(6)) = \{\pm I\}$.

<u>Another way</u>: Let $\mathsf{GL}(4) \to \mathsf{GL}(4)$ (I presume we want the identity representation here), and then form $\Lambda^2 \,\mathrm{id} : \mathsf{GL}(4) \to \mathsf{GL}(\Lambda^2 V)$. Now we have that

$$\dim \Lambda^2 V = \binom{n}{2}$$

where $n = \dim V$, therefore it follows that

$$\begin{aligned} \dim \Lambda^2 V &= \binom{4}{2} \\ &= 6. \end{aligned}$$

This is because looking at $\mathrm{id} : \mathsf{GL}(4) \to \mathsf{GL}(4) \cong \mathsf{GL}(V)$ with $V \cong \mathbb{F}^4$. Notice that $\mathsf{SL}(4) \subset \mathsf{GL}(4)$ and $\mathsf{SO}(6) \subset \mathsf{GL}(6)$. Λ^2 is the self-dual representation of $\mathsf{GL}(4)$, which means that it is orthogonal or symplectic (this seem to follow from the fact that we can define a non-degenerate bilinear form that is either symmetric or alternating, if the representation is self-dual). Then we have

$$(1,1,0,0) \rightsquigarrow (0,0,1,1) \in \mathbb{Z}^4 \qquad ((a_1,a_2,a_3,a_4) \leftrightarrow (a_4,a_3,a_2,a_1)) \tag{11.0.2}$$
$$\rightsquigarrow^{(-1)} (0,0,-1,-1) \tag{11.0.3}$$
$$(1,1,0,0) = (0,0,-1,-1) + (2,2,2,2) \tag{11.0.4}$$

Remark 11.0.17. Unclear from the notes in which way $(1,1,0,0) = (0,0,-1,-1) + (2,2,2,2)$ should be interpreted. Perhaps the author meant $(0,0,-1,-1) + (1,1,1,1)$ on the right-hand side of the equation.

Recall: For F algebraically closed, the irreducible algebraic representations of $\mathsf{GL}(n,F)$ are in one-to-one correspondence with Φ^+-dominant weights.

Group level: We have a maximal torus $\mathrm{Diag}(n,F)$ (in $\mathsf{GL}(n,F)$) acting on $M_n(F)$ by conjugation. This induces the eigenvalue-decomposition $M_n(F) = \mathrm{Diag}(n,F) \oplus \bigoplus_{i \neq j} \mathrm{span}(E_{ij})$ that we have seen earlier, where $\mathrm{Diag}(n,F)$ corresponds to the 0-weight space and E_{ij} are simultaneous eigenvectors.

$\mathfrak{diag}(n) \to \mathrm{End}(M_n(F))$. More generally, we have an action of $\mathfrak{diag}(n,F)$ on $M_n(F)$ by the bracket

$$\begin{aligned} H \cdot A &= [H,A] \\ &= HA - AH \end{aligned}$$

where we note that $\mathfrak{diag}(n,F) = \mathsf{Lie}(\mathrm{Diag}(n,F))$, and that $\mathfrak{diag}(n,F)$ is the maximal commutative Lie-subalgebra of $M_n(F) \cong \mathfrak{gl}(n,F) = \mathsf{Lie}(\mathsf{GL}(n,F))$.

Definition

Definition 11.0.18 (Lie Group)**.** A **Lie group** G is a *smooth manifold* (second countable, Hausdorff locally euclidean space with a smooth structure) such that the maps $m : G \times G \to G$ and $i : G \to G$ defined by $(g,h) \mapsto gh$ and $g \mapsto g^{-1}$ are smooth operations.

Remark 11.0.19. Cf. the above with a *topological group*, which does not require that G is second countable, locally euclidean or has a smooth structure, only that G is a group and a topological space such that the operations m, i above are *continuous*.

If G is an algebraic group over $\mathbb{R}$ then $G(\mathbb{R})$ is a Lie group (11.0.18). Similarly, we have that if G is an algebraic group over $\mathbb{C}$ then $G(\mathbb{C})$ is a complex Lie group.

Generally, we have

$$\begin{aligned} \textsf{algebraic sets/varieties} &\leftrightarrow \textsf{algebraic groups} \\ \textsf{smooth manifolds} &\leftrightarrow \textsf{Lie groups} \\ \textsf{complex manifolds} &\leftrightarrow \textsf{complex Lie groups} \end{aligned}$$

That a Lie group G is complex means that m, i are **holomorphic** operations. There are many complex manifolds M that are nog algebraic, e.g. $M \neq \mathcal{V}(\mathbb{C})$ for V variety.

We have that $G \mapsto G(\mathbb{C})$ is an **equivalence of categories**. To be more specific, the equivalence is

$$\begin{array}{ccc} \textsf{Connected reductive groups over } \mathbb{C} & \simeq & \textsf{Connected complex reductive Lie algebras} \\ \cap & & \cap \\ \textsf{Algebraic groups over } \mathbb{C} & \longleftrightarrow & \textsf{Complex Lie groups} \\ \mathbb{G}_m & \longmapsto & \mathbb{C}^\times \end{array}$$

We define a *connected, real* Lie group G to be **semisimple** if $\mathsf{Lie}(G)$ is semisimple. C.f. $\mathsf{Lie}(G) \otimes_{\mathbb{R}} \mathbb{C}$ is semisimple.

For $G/\mathbb{C}$, we have that G is Zariski-connected $\Leftrightarrow$ $G(\mathbb{C})$ is classically connected euclidean.

Example 11.0.20. $\mathsf{GL}(n)$ is Zariski-connected since open set of $M_n = \mathbb{A}^{n^2} \hookleftarrow$ irreducible, but $\mathsf{GL}(n, \mathbb{R})$ is disconnected since it has 2 components, depending on the sign of the determinant, i.e. $\mathsf{GL}(n, \mathbb{R}) = \mathsf{GL}(n, \mathbb{R})_+ \cup \mathsf{GL}(n, \mathbb{R})_-$ where $\mathsf{GL}(n, \mathbb{R})_+ = \{A \in \mathsf{GL}(n, \mathbb{R}) \mid \det(A) > 0\}$ and $\mathsf{GL}(n, \mathbb{R})_- = \{A \in \mathsf{GL}(n, \mathbb{R}) \mid \det(A) < 0\}$.

Furthermore, we define $\mathsf{GL}(n, \mathbb{R})_+ =$ identity component, which is a Lie group but not an algebraic group. I guess the reason we called this the identity component is that $I \in \mathsf{GL}(n, \mathbb{R})_+$, which is the multiplicative identity of $\mathsf{GL}(n, \mathbb{R})$ as a group.

For $G/\mathbb{C}$, we have that
G is simply connected in the sense of (6.0.19) $\Leftrightarrow$ G is simply connected in the sense that G is connected and for all $\varphi : H \to G$ surjective with finite kernel, and H connected then φ is an isomorphism $\Leftrightarrow$ $G(\mathbb{C})$ is simply connected in the sense that *every loop* in $G(\mathbb{C})$ (as a topological space) is *contractible*.

For Lie groups, we have **maximal compact subgroups**.

Theorem

Theorem 11.0.21.

1. *If G is a semisimple Lie group, all maximal compact subgroups of G are conjugate in G (also true if $G = \mathbb{G}(\mathbb{R})$ with $\mathbb{G}$ reductive over $\mathbb{R}$).*
2. *If K is a maximal compact subgroup, then G is* diffeomorphic *to $K \times C$ where C is a contractible. So essentially G is the same as the product manifold of K times C when viewed as* smooth manifolds.
   This implies that
   (a) *G connected $\Leftrightarrow$ K connected.*
   (b) *# of components of G = # number of components of K.*
   (c) *G simply connected $\Leftrightarrow$ K simply connected.*
   (d) *$\pi_1(G) \cong \pi_1(K)$.*

Example 11.0.22. Let $G = \mathsf{SL}(2, \mathbb{R})$, which we assume is an (algebraic) Lie group which is *semisimple* over $\mathbb{R}$

$$\begin{aligned} \rightsquigarrow K &= \mathsf{SO}(2, \mathbb{R}) \\ &\cong \mathsf{SO}^I(2, \mathbb{R}) \\ &\cong S^1. \end{aligned}$$

Since S^1 is connected, we claim that if ollows from above that G is connected (I presume this is the motivation for this example).

As an aside, recall that

$$\mathsf{SO}(2, \mathbb{R}) = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \,\middle|\, \theta \in [0, 2\pi) \right\}$$

is the set of rotation matrices. Therefore if we parametrize $S^1 = \{e^{i\theta} \quad 0 \leqslant \theta < 2\pi\}$ then $\phi : S^1 \to \mathsf{SO}(2, \mathbb{R})$ defined explicitly by $e^{i\theta} \mapsto \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$ is a group-isomorphism. One way to see this is to note that

$$\begin{aligned} \phi\left(e^{\theta_1 i}\right) \cdot \phi\left(e^{\theta_2 i}\right) &= \phi\left(e^{(\theta_1+\theta_2)i}\right) \\ &= \begin{pmatrix} \cos(\theta_1+\theta_2) & -\sin(\theta_1+\theta_2) \\ \sin(\theta_1+\theta_2) & \cos(\theta_1+\theta_2) \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2) & -(\sin(\theta_1)\cos(\theta_2) + \sin(\theta_2)\cos(\theta_1)) \\ \sin(\theta_1)\cos(\theta_2) + \sin(\theta_2)\cos(\theta_1) & \cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2) \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta_1) & -\sin(\theta_1) \\ \sin(\theta_1) & \cos(\theta_1) \end{pmatrix} \begin{pmatrix} \cos(\theta_2) & -\sin(\theta_2) \\ \sin(\theta_1) & \cos(\theta_2) \end{pmatrix} \\ &= \phi\left(e^{\theta_1 i}\right)\phi(e^{\theta_2 i}). \end{aligned}$$

Also, we then have (assuming now that $G \cong K \times C$ where C contractible and G, K as above)

$$\begin{aligned} \pi_1(\mathsf{SO}(2, \mathbb{R})) &= \pi_1(S^1) \\ &= \mathbb{Z} \end{aligned}$$

and recall that $\mathbb{R}/\mathbb{Z} \cong S^1$ and that $\mathbb{R}$ is the *universal cover* of S^1, so we have $\mathbb{R} \twoheadrightarrow \mathbb{R}/\mathbb{Z} \cong S^1$ and in full $0 \to \mathbb{Z} \hookrightarrow \mathbb{R} \twoheadrightarrow \mathbb{R}/\mathbb{Z} \to 0$. The associated cover from $\mathbb{R}$ to S^1 is the covering map $\omega : \mathbb{R} \to S^1$ defined by $r \overset{\omega}{\longmapsto} e^{2\pi i r}$.

If G is a Lie group (11.0.18) $\Rightarrow$ every cover of G has *the structure of a Lie group*, such that the covering map is a homomorphism *of Lie groups*.

If $\tilde{G}$ is the *universal cover* of G, then we have

$$1 \to \pi_1(G) \to \tilde{G} \twoheadrightarrow G \to 1.$$

Going back to our example, it follows that $\pi_1(\mathsf{SL}(2, \mathbb{R})) = \mathbb{Z}$.

$$0 \to \mathbb{Z}/n \to \mathbb{Z} \to \mathbb{Z}/n \to 0$$

$\Rightarrow$ that for all n there exists a covering $1 \to \mathbb{Z}/n \to \mathsf{SL}(2, \mathbb{R})_n \twoheadrightarrow \mathsf{SL}(2, \mathbb{R}) \to 1$ where $\mathsf{SL}(2, \mathbb{R})_n$ is a *maximal compact subgroup* of $\mathsf{SL}(2, \mathbb{R})$ (I presume, the notes seem to say of $\mathsf{SL}(2, \mathbb{C})$ here).

Remark 11.0.23. I believe each $\mathsf{SL}(2,\mathbb{R})_n$ corresponds to $[\omega]^n \in \pi_1(S^1)$, which in turn corresponds to $n \in \mathbb{Z}$.

Furthermore, we claim that a maximal compact subgroup of $\mathsf{SL}(2,\mathbb{C})$ is $\mathsf{SU}(2,\mathbb{C})$ and that

$$\mathsf{SU}(2) \cong S^3$$

but $\pi_1(S^3) = 1$ so that $\mathsf{SL}(2,\mathbb{C})$ is simply connected by (11.0.21).

Remark 11.0.24. Notice that if $A \in \mathsf{SU}(2,\mathbb{C})$ then $\det(A) = 1 \Rightarrow A \in \mathsf{SL}(2,\mathbb{C})$ so that $\mathsf{SU}(2,\mathbb{C}) \subset \mathsf{SL}(2,\mathbb{C})$.

We have $\mathsf{SO}(n) = \{A \in \mathsf{GL}(n,\mathbb{C}) \mid {}^tAA = I \text{ and } \det(A) = 1\}$. $\mathsf{SL}(2,\mathbb{R})$ are *non-algebraic* Lie groups. $\mathsf{SL}(\tilde{2},\mathbb{R})$ is the universal cover (Lie group, but not algebraic, it seems).

We have (equivalence it says in the notes)

$$\text{Connected reductive groups over } \mathbb{C} \longleftrightarrow \text{Connected compact Lie groups/Maximal compact subgroup}$$

$$G \longmapsto G(\mathbb{C})$$

$$\mathbb{K}(\mathbb{C}) \longmapsto K = \mathbb{K}(\mathbb{R})$$

Chapter 12

Borel, Parabolic subgroups, positive and simple roots

Recall:

Definition

Definition 12.0.1. Let G be an algebraic group over an algebraically closed field F. A **Borel subgroup** of G is a maximal $\underbrace{\text{connected}}_{\text{Due to Lie-Kolchin}}$ solvable subgroup.

Theorem

Theorem 12.0.2. *All Borel subgroups are conjugate in G.*

Remark 12.0.3.

1. For 12.0.2, we don't need G to be neither reductive, nor connected.
2. Definition 12.0.1 only works well when F is algebraically closed. Over more general F, replace "Borel" with "minimal parabolic" (definition over F).
3. Recall that $R_G =$"radical of G" (9.0.5), which is the maximal, connected normal solvable subgroup (cf. 8.0.24). So Borel (12.0.1) is like radical but without the *normality* hypothesis.

Observe: For $\mathsf{GL}(n)$, Lie-Kolchin $\Rightarrow$

Theorem

Theorem 12.0.4. *All Borel subgroups of $\mathsf{GL}(n)$ are conjugate to Triag$^+(n)$ (and to Triag$^-(n)$).*

Proof. Exercise: $\text{Triag}^+(n)$ is connected.

Homework: $\text{Triag}^+(n)$ is solvable.

Recall: Lie-Kolchin: If $G \subset \mathsf{GL}(n)$ is a connected, solvable algebraic group then there exists $x \in \mathsf{GL}(n)$ such that $xGx^{-1} \subset \text{Triag}^+(n)$.

Let G be maximal connected solvable in $\mathsf{GL}(n)$. Since G is connected and solvable there exists $x \in \mathsf{GL}(n)$ such that $xGx^{-1} \subset \mathrm{Triag}^+(n)$. Since G is maximal $\rightsquigarrow xGx^{-1}$ is maximal. We have that $\mathrm{Triag}^+(n)$ is connected and solvable $\rightsquigarrow xGx^{-1} = \mathrm{Triag}^+(n)$. $\square$

Remark 12.0.5. Notice here that maximality does not imply a *total* order with respect to inclusion $\subset$; i.e. when we say that G is maximal solvable connected subgroup we just mean that if H is also a maximal connected solvable subgroup of the same algebraic group and H contains G then $G = H$.

Remark 12.0.6. That xGx^{-1} is still solvable, might follow from the fact that I think $G \xmapsto{\mathrm{int(x)}} xGx^{-1}$ is a homeomorphism with respect to the Zariski-topology, and so take connected sets to connected sets, so that xGx^{-1} is connected. For solvability, we claim that $(xGx^{-1})' = xG'x^{-1}$ and so by induction $(xGx^{-1})^{(n)} = xG^{(n)}x^{-1}$ and since there is an $n \geqslant 1$ for G so that $G^{(n)} = e$ it follows that

$$\begin{aligned}(xGx^{-1})^{(n)} &= xG^{(n)}x^{-1} \\ &= xex^{-1} \\ &= e.\end{aligned}$$

We want to show that it holds that $(xGx^{-1})' = xG'x^{-1}$ and more generally that $(xGx^{-1})^{(n)} = xG^{(n)}x^{-1}$.

Let $H = xGx^{-1}$, then we want to show that $H' = xG'x^{-1}$.

$\underline{H' \subseteq xG'x^{-1}}$: Let $h_1, h_2 \in H$. Then there exists $g_1, g_2 \in G$ such that $h_1 = xg_1x^{-1}$ and $h_2 = xg_2x^{-1}$. Then we have that the *commutator* of h_1, h_2 is

$$\begin{aligned}[h_1, h_2] &= h_1h_2h_1^{-1}h_2^{-1} \\ &= xg_1x^{-1}xg_2x^{-1}(xg_1x^{-1})^{-1}(xg_2x^{-1})^{-1} \\ &= xg_1x^{-1}xg_2x^{-1}xg_1^{-1}x^{-1}xg_2^{-1}x^{-1} \\ &= xg_1g_2g_1^{-1}g_2^{-1}x^{-1} \\ &= x[g_1, g_2]x^{-1} \in xG'x^{-1}.\end{aligned}$$

This shows that $[h_1, h_2] \in xG'x^{-1}$ and hence products of commutators of elements of H are in $xG'x^{-1}$ (by applying the same idea as in the equalities above). But every element of H' is a product of such commutators of elements of H, therefore this shows that $H' \subseteq xG'x^{-1}$.

Remark 12.0.7. One definition of $\langle S\rangle$ for $S \subseteq G$ where G is a group, is as all the finite products $s_1 \cdots s_m$ for $s_i \in S$ (possibly inverses as well).

$\underline{xG'x^{-1} \subseteq H'}$: Let $g_1, g_2 \in G$ be arbitrary and consider $x[g_1, g_2]x^{-1} \in xG'x^{-1}$. Then we have

$$\begin{aligned}x[g_1, g_2]x^{-1} &= xg_1g_2g_1^{-1}g_2^{-1}x^{-1} \\ &= xg_1x^{-1}xg_2x^{-1}xg_1^{-1}x^{-1}xg_2^{-1}x^{-1} \\ &= [xg_1x^1, xg_2x^{-1}] \in H'.\end{aligned}$$

This shows that $[xg_1x^{-1}, xg_2x^{-1}] \in H'$ (since $xg_1x^{-1}, xg_2x^{-1} \in H$ so that also finite products of such elements [and their inverses] are in H).

Remark 12.0.8. Notice that

$$\begin{aligned}[h_1, h_2]^{-1} &= (h_1h_2h_1^{-1}h_2^{-1})^{-1} \\ &= h_2h_1h_2^{-1}h_1^{-1} \\ &= [h_2, h_1].\end{aligned}$$

Now assume that for $n-1$ we have that $(xGx^{-1})^{(n-1)} = xG^{(n-1)}x^{-1}$. Then

$$\begin{aligned}(xGx^{-1})^{(n)} &= (xG^{(n-1)}x^{-1})' \\ &= xG^{(n)}x^{-1}.\end{aligned}$$

The last step used the idea we showed above, i.e. that for any subgroup H it holds that $(xHx^{-1})' = xH'x^{-1}$, and the first equality above is just the inductive definition of the n^{th} step in a derived series.

Going back, this shows that xGx^{-1} is solvable if G is. Therefore, we have that xGx^{-1} is connected and solvable. Assume that xGx^{-1} was not maximal, so that xGx^{-1} was contained in some larger connected solvable subgroup H. Then conjugation by x^{-1} gives us that $G \subsetneq xHx^{-1}$, and by the above argument xHx^{-1} is still connected and solvable. This contradicts the maximality of G. We conclude that xGx^{-1} must be maximal, and since $\text{Triag}^+(n)$ was (assuming result of homework and exercise) connected and solvable we see that $xGx^{-1} = \text{Triag}^+(n)$.

Lie-Kolchin motivates the definition of Borel subgroups.

Recall that if $S \subset \mathsf{GL}(n)$ is commutative and every element is diagonalizable (semisimple?) then there exists x such that $xSx^{-1} \subset \text{Diag}(n)$.

All maximal tori in $\mathsf{GL}(n)$ are conjugate to $\text{Diag}(n)$.

The definition below I think is intended (if I am reading the notes right) to be in the context of an algebraically closed field.

Definition

Definition 12.0.9 (Maximal torus)**.** A **maximal torus** is an (algebraic) subgroup that is maximal with respect to the following properties:

1. Connected.
2. Commutative.
3. Diagonalizable.

In a connected, reductive group a maximal torus is *self-centralizing*, i.e. it is maximal commutative.

Example 12.0.10. $\mathbb{G}_a$ is connected unipotent.

If G is connected and reductive, T a maximal torus in G and α a root of T in G then there exists a root group $U_\alpha \subset G$, such that $U_\alpha \cong \mathbb{G}_a$ such that U_α is unipotent + commutative.

Example 12.0.11. For $G = \mathsf{GL}(n)$, $T = \text{Diag}(n)$ (this is a maximal torus in $\mathsf{GL}(n)$) we have seen that the set Φ of roots is $\{e_i - e_j \mid i \neq j\}$. For $\alpha = e_i - e_j$, we have that

$$\begin{aligned}U_\alpha(F) &= \{I + aE_{ij} \mid a \in F\} \\ &\cong F, \qquad (i \neq j)\end{aligned}$$

where the isomorphism is defined as taking $I + a_{ij}$ to $a \in F$.

Definition

Definition 12.0.12 (Parabolic subgroup)**.** A subgroup $P \subset G$ is **parabolic** if G/P is *projective.*

If H is an algebraic subgroup of G then G/H has a natural structure as a variety (If H is not normal, then G/H is not an *algebraic* group).

Theorem

Theorem 12.0.13. *A Borel subgroup (12.0.1) is a minimal parabolic subgroup (12.0.12). In particular, B Borel $\Rightarrow G/B$ projective.*

Remark 12.0.14. The last sentence in the theorem above follows directly from the first part, i.e. if B is a borel subgroup then by the theorem it is parabolic, and by definition of a parabolic subgroup we have that G/B is projective.

Remark 12.0.15. The quotient variety G/H is not always the functor $A \mapsto G(A)/H(A)$. It seems like $G(A)/H(A)$ might not always be a variety. So $G(A)/H(A)$ is the "naive quotient". $G(F)/H(F)$ might be smaller than $(G/H)(F)$. If H is not normal, then $A \mapsto G(A)/H(A)$ is not a group functor but a set-functor (from F-algebras to **Set**).

If G is a (non-commutative) connected reductive group, then a Borel subgroup (12.0.1) is never normal. For $H \triangleleft G$ with H, G algebraic groups, then G/H is an algebraic group (i.e. G/H affine), and if G is connected then G/H is connected.

Assume that G is connected and that $B \subset G$ is a Borel subgroup. Then $B \triangleleft G \Leftrightarrow B = G$.

Reason: If Y is an irreducible projective and affine variety, than Y is a point.

12.0.1 Categorical Quotient

Definition

Definition 12.0.16 (Categorical quotient)**.** Assume H acts on a variety X (e.g. a group G containing H as a subgroup; I presume we mean that H acts on G). A quotient of X by H is a pair (Y, π) such that

1. Y is a variety.
2. $$\begin{tikzcd} X \arrow[d, "\pi"] \\ Y \end{tikzcd}$$
   is constant on H-orbits (i.e. $\pi(x_1) = \pi(x_i)$ if x_1, x_2 are in the same H-orbit).
3. Satisfying the universal property that if $\pi' : X \to Y'$ is a *morphism* constant on H-orbits (i.e. it makes the same identifications as π; cf. quotient topology) then there exists a unique $f : Y \to Y'$ such that the following diagram commutes
   $$\begin{tikzcd} X \arrow[d, "\pi"'] \arrow[dr, "\pi'"] & \\ Y \arrow[r, dashed, "f"'] & Y' \end{tikzcd}$$

Furthermore, if (Y, π) exists, it is unique up to (unique) isomorphism.

In general, if H acts on X there might not exist a quotient variety. If $X = G$ and $H \subset G$ is a subgroup then there exists a variety G/H ("the categorical quotient").

Remark 12.0.17. G/H means that $G \curvearrowleft H$ acts on the right by right multiplication, i.e. $G \times H \to G$

defined by $(g,h) \mapsto g \cdot h$. If instead H acts on the left by left multiplication $H \curvearrowright G$, then write $H \backslash G$.

Example 12.0.18. $\mathsf{GL}(n,F) \curvearrowright F^n$ by matrix-multiplication which fixes $0 \rightsquigarrow \curvearrowright F^n \setminus \{0\} \rightsquigarrow \curvearrowright F^n \setminus \{0\} / (v \sim \lambda v \quad \forall \lambda \in F^\times) = \mathbb{P}^{n-1}(F)$. Hence we have an action $\mathsf{GL}(n) \curvearrowright \mathbb{P}^{n-1}$.

<u>Exercise</u>: The action above by $\mathsf{GL}(n)$ on $\mathbb{P}^{n-1}$ is transitive.

Example 12.0.19. Let $e = (1, 0, \ldots, 0)$. Then

$$\mathrm{Stab}(e) = \left\{ \left(\begin{array}{c|ccc} * & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \end{array} \right) \right\}$$

we claim is a parabolic subgroup (12.0.12) of $\mathsf{GL}(n)$, and that $\mathsf{GL}(n)/\mathrm{Stab}_{\mathsf{GL}(n)}(e) \cong \mathrm{Orb}(e)$, where

$$\begin{aligned} \mathrm{Orb}(e) &= \mathsf{GL}(n) \cdot e \\ &= \{g \cdot e \mid g \in \mathsf{GL}(n)\}. \end{aligned}$$

Now let this map above be defined by $g\mathrm{Stab}(e) \mapsto [g \cdot e]$.

Remark 12.0.20. Notice how we define the stabilizer above; such that if $h \cdot e = \lambda e$ then h is in the stabilizer of e.

<u>Well-defined</u>: If $g\mathrm{Stab} = g'\mathrm{Stab}(e)$ then there is a $h \in \mathrm{Stab}(e)$ such that $gh = g'$. But notice that then by definition $h \cdot e = \lambda \cdot e$.

Then we have that

$$\begin{aligned} (g \cdot h) \cdot e &= g\lambda e \\ &= \lambda(g \cdot e) \\ &= g' \cdot e, \end{aligned}$$

Let $v = g \cdot e$ and $w = g' \cdot e$. Then we have that $\lambda v = w$ so that $[v] = [w]$, i.e. $g\mathrm{Stab}(e) = g'\mathrm{Stab}(e)$ means that g, g' are sent to the same element $[v] = [w] \in \mathbb{P}^{n-1}$.

<u>Injective</u>: Assume that $[g \cdot e] = [g' \cdot e]$. Then there is some $\lambda \neq 0$ such that

$$g \cdot e = \lambda(g' \cdot e). \tag{12.0.1}$$

Consider the fact that g, g' are linear maps so commute with scalar multiplication, and that g' is invertible. Therefore from 12.0.1 we have

$$\begin{aligned} (g'^{-1} \cdot g) \cdot e &= \lambda e \\ \Leftrightarrow g'^{-1} g &\in \mathrm{Stab}(e) \\ \Leftrightarrow g\mathrm{Stab}(e) &= g'\mathrm{Stab}(e), \end{aligned}$$

which shows that the map is injective.

<u>Surjective</u>: Let $[v] \in \mathbb{P}^{n-1}$. We can then complete a representative $v \neq 0 \in \mathbf{F}^n \setminus \{0\}$ to a basis for $\mathbf{F}^n$, say $\{v := v_1, \ldots, v_n\}$, and take g as the matrix with columns $v_1, \ldots, v_n$. This is then invertible and its action on e gives back $[v]$.

$$\begin{array}{ccccccc} \text{Reductive Lie Algebras} & \longleftrightarrow & \text{Connected Reductive Groups} & \longleftrightarrow & \underbrace{\underline{\text{Finite Weyl groups}}}_{\text{Crystallographic}} & \subset & \text{Finite Coxeter groups} \\ \cap & & & & \cap & & \\ \text{Kac-Moody Lie Algebras} & \longleftrightarrow & \text{Kac-Moody groups} & \longleftrightarrow & \text{Crystallographic Coxeter groups} = \text{Weyl Groups} & \subset & \text{Coxeter Groups} \end{array}$$

Let $n = n_1 + \ldots + n_r$ be a *partition* of n. Then

1. $$P_{(n_1,\ldots,n_r)} = \begin{pmatrix} n_1 & * & * & * \\ & n_2 & * & * \\ & & \ddots & * \\ & & & n_r \end{pmatrix}$$
   where n_i are *block*-matrices. We claim this is a parabolic subgroup (12.0.12) of $\mathsf{GL}(n)$ contained in $\mathrm{Triag}^+(n)$.

2. Every parabolic subgroup (12.0.12) of $\mathsf{GL}(n)$ containing $\mathrm{Triag}^+(n)$ is $P_{(n_1,\ldots,n_r)}$ for some unique partition $n = n_1 + \ldots + n_r$.

3. Every parabolic subgroup of $\mathsf{GL}(n)$ is conjugate to $P_{(n_1,\ldots,n_r)}$ for a unique $(n_1, \ldots, n_r)$.

In particular, if $P_{(n_1,\ldots,n_r)}$ is conjugate to $P_{(m_1,\ldots,m_r)}$ then $n_1 = m_1, \ldots, n_r = m_r$.

Definition

Definition 12.0.21 (Standard parabolic subgroups)**.** The $P_{(n_1,\ldots,n_r)}$ above are called **Standard parabolic subgroups** relative the Borel subgroup $\mathrm{Triag}^+(n)$.

We have a bijection between *conjugacy classes* of parabolic subgroups of $\mathsf{GL}(n) \longleftrightarrow$ partitions $(n_1, \ldots, n_r)$ of n, corresponding to Weyl-groups S_n (of $\mathsf{GL}(n)$) $S_{n_1} \times \cdots \times S_{n_r} \subset S_n$.

12.0.2 System of positive roots, simple roots

Recall: We have root systems (V, Φ) with

1) $\mathrm{span}_{\mathbb{Q}} \Phi = V$.
2) Reflections $S_\alpha(\Phi) \subset \Phi$ for $\alpha \in \Phi$.
3) $\frac{2(\alpha,\beta)}{(\alpha,\alpha)} \in \mathbb{Z}$ for all $\alpha, \beta \in \Phi$.

From 2) we see that since $S_\alpha(\alpha) = -\alpha$ we have that $-\alpha \in \Phi$, and $S_\alpha(-\alpha) = \alpha$ so that

$$\alpha \in \Phi \Leftrightarrow -\alpha \in \Phi.$$

Motivation of *system of positive roots*: We want to choose one element from the sets $\{\pm\alpha\}$ for all $\alpha \in \Phi$.

Example 12.0.22. $\Phi_{\mathsf{A}}^{n-1} = \{e_i - e_j \mid i \neq j\} \rightsquigarrow \Phi_{\mathsf{A}}^{n-1,+} = \{e_i - e_j \mid i < j\}$. Notice that $e_i - e_j \in \Phi_{\mathsf{A}}^{n-1,+}$ but $e_j - e_i \notin \Phi_{\mathsf{A}}^{n-1,+}$. Notice that if we have $\alpha = e_i - e_j$ and $\beta = e_j - e_k$ with $i < j < k$ then we get $\alpha + \beta = e_i - e_k \in \Phi$, but then we have that $i < k$ so that $\alpha + \beta \in \Phi_{\mathsf{A}}^+$.

Definition

Definition 12.0.23 (System of positive roots)**.** A **system of positive roots** is a subset $\Phi^+ \subset \Phi$ such that

1. $$|\{\pm\alpha\} \cap \Phi^+| = 1, \qquad (\forall \alpha \in \Phi)$$
2. If $\alpha, \beta, \alpha + \beta \in \Phi$ and $\alpha, \beta \in \Phi^+$ then $\alpha + \beta \in \Phi^+$, i.e. Φ^+ is closed under addition.

Example 12.0.24. $\Phi_{\mathsf{D}} = \{\pm(e_i \pm e_j) \mid i < j\} \rightsquigarrow \Phi_{\mathsf{D}}^+ = \{(e_i \pm e_j) \mid i < j\}$. Notice here that if $e_i - e_j \in \Phi_{\mathsf{D}}^+$ then $e_j - e_i \notin \Phi_{\mathsf{D}}^+$ since we need $i < j$ to hold. On the other hand, if we have $e_i + e_j$, then we get that $-(e_i + e_j) = -e_i - e_j \notin \Phi_{\mathsf{D}}^+$. For the case when we have $\alpha = e_i - e_j, \beta = e_j - e_k$ with $i < j < k$ the reasoning is the same as in example 12.0.22. Assume we have $\alpha = e_i + e_j$ and $\beta = e_\ell - e_j$ with $i < \ell < j$, then $\alpha + \beta = e_i + e_\ell$ with $i < \ell$ so that $\alpha + \beta \in \Phi_{\mathsf{D}}^+$.

We claim this covers all cases, I think this follows from the fact that $e_i + e_j = e_k$ for $i \neq j \neq k$ can not happen since $\{e_i\}_{1 \leqslant i \leqslant n}$ are linearly independent (so we should think of them analogously to basis vectors of e.g. $\mathbb{Q}^n$ or $\mathbb{R}^n$).

Question I: Does a system of positive roots (12.0.23) always exist?

Question II: How many are there?

The third issue: positive roots $\rightsquigarrow$ simple roots. We have that $\operatorname{span}_{\mathbb{Q}}\Phi = V$. If Φ^+ is a positive system $\Rightarrow \operatorname{span}_{\mathbb{Q}}\Phi^+ = V$.

Example 12.0.25. $\mathsf{A}_2 : e_1 - e_2, e_2 - e_3 \rightsquigarrow (e_1 - e_2) + (e_2 - e_3) = (e_1 - e_3)$.

Definition

Definition 12.0.26 (Simple root)**.** Given a positive system Φ^+, $\alpha \in \Phi^+$ is **simple** if α is not a sum $\alpha = \beta + \gamma$ with $\beta, \gamma \in \Phi^+$.

Remark 12.0.27. If $\alpha \in \Phi^+$ is not simple, then there exists a *simple* root $\beta \in \Phi^+$ and $\gamma \in \Phi^+$ such that $\alpha = \beta + \gamma$.

Theorem

Theorem 12.0.28. *Let $\Delta \subset \Phi^+$ be the subset of simple roots (12.0.26).*

a) Every $\alpha \in \Phi$ is a $\mathbb{Z}$-linear combination of simple roots with all coefficients having the same *sign ($+$ if $\alpha \in \Phi^+$ and $-$ if $\alpha \in \Phi^- = -\Phi^+$).*

b) Δ is a basis for $\operatorname{span}_{\mathbb{Q}}\Phi = V$.

c) The Weyl group $\mathcal{W}$ (2.0.9) acts on $(+) := \{\Phi^+ \subset \Phi \mid \Phi^+$ positive root system$\}$. This action is simply transitive, *i.e.*

$$\forall \Phi_1^+, \Phi_2^+ \in (+) \exists! w \in \mathcal{W}(w\Phi_1^+ = \Phi_2^+).$$

In particular,

$$\#\text{ of positive root systems} = |\mathcal{W}|.$$

We want to connect this to Borel subgroups & maximal tori.

Theorem

Theorem 12.0.29. *Let G be a connected, reductive group over an algebraically closed field F. Fix a maximal torus T in G. Then*

$$\begin{aligned} N_G(T)/T &\cong \mathcal{W} \\ &= \langle S_\alpha \mid \alpha \in \Phi \rangle. \end{aligned}$$

There is a bijection between Borel subgroups in G that contains T ($\{B$ Borel $\mid B \supset T\}$) and $(+) = \{\Phi^+ \subset \Phi \mid \Phi^+$ positive root system$\}$. The correspondence above is given by sending Φ^+ to the subgroup of G generated by T and U_α such that $\alpha \in \Phi^+$ where U_α is a root group *(that is unipotent and commutative).*

Remark 12.0.30. We have an action $N_G T \curvearrowright X = \{B \text{ Borel} \mid B \supset T\}$. This action induces a homomorphism $\varphi : N_G(T) \to \mathrm{Sym}(X)$ and since the action is by conjugation and we have that $tBt^{-1} = B$ we get that φ factors through $\tilde{\varphi} \circ \pi = \varphi$ where $\tilde{\varphi} : N_G(T)/T \to \mathrm{Sym}(X)$ induces an action $[g] \cdot x = \tilde{\varphi}(x)$ for all $[g] \in N_G(T)/T$ and $x \in X$, and where Φ^+ is the *stabilizer* of a point in T.

Definition

Definition 12.0.31 (Adjoint representation)**.** Let T be a maximal torus in G. Then we have a representation $\mathsf{Ad} : G \to \mathsf{GL}(\mathsf{Lie}(G))$ called the **adjoint representation**. We can restrict the representation to T and get a representation $\mathsf{Ad}_T \to \mathsf{GL}(\mathsf{Lie}(G))$.

We claim there is a root-space decomposition

$$\mathsf{Lie}(G) = \underbrace{\mathsf{Lie}(T)}_{\mathsf{Lie}(G)_0} \oplus \bigoplus_{\chi \in X^*(T)} \mathsf{Lie}(G)_\chi$$

where

$$\mathsf{Lie}(G)_\chi = \{y \in \mathsf{Lie}(G) \mid tyt^{-1} = \chi(t)y, \forall t \in T\}$$

and

$$\begin{aligned} \Phi &= \text{root of } T \text{ in } G \\ &= \{\chi \mid \chi \neq 0 \text{ and } \mathsf{Lie}(G)_\chi \neq 0\}. \end{aligned}$$

Partition $(n_1, \ldots, n_r) \longleftrightarrow (e_1 - e_2, e_2 - e_3, \ldots, e_{n_1 - 1} - e_{n_1}) \coprod (e_{n_1+1} - e_{n_1+2}, \ldots, e_{n_1+n_2-1} - e_{n_1+n_2}) \coprod \ldots$.

Example 12.0.32 ($\mathsf{GL}(n)$)**.** Let $\Phi = \{e_i - e_j \mid i < j\} \rightsquigarrow \Delta = \{e_1 - e_2, e_2 - e_3, \ldots, e_{n-1}, e_n\}$.

Chapter 13

Jordan, Unipotent Radical, Highest root

We want to prove Jordan Decomposition for $M_n(F)$, where F is algebraically closed; Recall that for $A \in M_n(F)$ there exists A_s, A_n such that

1. $A = A_s + A_n$.
2. $A_n A_s = A_s A_n$.
3. A_s semisimple (diagonalizable) and A_n nilpotent (exists $m \geqslant 1$ such that $A_n^m = 0$).

We discussed that

a) The Jordan Decomposition for $\mathsf{GL}(n, F)$ (i.e. $(g = g_s g_u)$) follows easily from the case for $M_n(F)$: We know that if $g \in \mathsf{GL}(n, F) \subset M_n(F)$ then (assuming the Jordan Decomposition for $M_n(F)$) we have a [Jordan] decomposition $g = g_s + g_n$ and so $g = g_s(I_n + g_s^{-1} g_n)$. We claim that $I + g_s^{-1} g_n$ commute with g_s. First note that by assumption we have that $g_s g_n = g_n g_s \Leftrightarrow g_n = g_s^{-1} g_n g_s \rightsquigarrow (I + g_s^{-1} g_n) g_s = g_s + g_n$ and $g_s(I + g_s^{-1} g_n) = g_s + g_n$.

b) There exists a Jordan Decomposition in a general algebraic group $G \subset \mathsf{GL}(n)$. Furthermore, we claim that $I + g_s^{-1} g_n$ is *unipotent*. To see this first note that

$$\begin{aligned} g_s g_n &= g_n g_s \\ \Leftrightarrow g_n &= g_s^{-1} g_n g_s \\ \Leftrightarrow g_n g_s^{-1} &= g_s^{-1} g_n \end{aligned}$$

so that

$$\begin{aligned} (g_s^{-1} g_n)^m &= \underbrace{(g_s^{-1} g_n)(g_s^{-1} g_n) \cdots (g_s^{-1} g_n)}_{m \text{ times}} \\ &= g_s^{-m} \underbrace{g_n^m}_{=0} \\ &= 0. \end{aligned}$$

Therefore, $g_s^{-1} g_n$ is *nilpotent*, so all its eigenvalues are 0. Therefore, if we have an eigenvector v associated with $I + g_s^{-1} g_s$ so that $(I + g_s^{-1} g_n) v = \lambda v$ we get that $g_s^{-1} g_n v = \lambda v - v$ so that $g_s^{-1} g_n v = (\lambda - 1) v$ so that $\lambda - 1$ is an eigenvalue of $g_s^{-1} g_n$. Since $g_s^{-1} g_n$ is nilpotent, we must have that $\lambda - 1 = 0 \Leftrightarrow \lambda = 1$. Therefore the eigenvalues of $I + g_s^{-1} g_n$ are all 1, so that $I + g_s^{-1} g_n$ is unipotent (this seems to be, atleast for an algebraically closed field, a *definition*).

c) If $\varphi : G \to H$ is a homomorphism of algebraic groups and $g = g_s g_u$ is a Jordan Decomposition for $g \in G$ (where now g_u is *unipotent*) then

$$\begin{aligned}\varphi(g) &= \varphi(g_s g_u)\\ &= \varphi(g_s)\varphi(g_u)\\ &= \varphi(g)_s \varphi(g)_u.\end{aligned}$$

Remark 13.0.1. Compare 10.0.10 and 10.0.11.

Proof. We prove the Jordan Decomposition for $M_n(F)$. Let $A \in M_n(F)$.

Existence:

We have $F^n = \bigoplus_{\lambda \in F} F^n_\lambda$ where $F^n_\lambda = \{v \in F^n \mid (A - \lambda I)^m v = 0 \text{ for some } m \geqslant 1\}$, called the generalised λ-eigenspace. Notice that $(A - \lambda I)|_{F^n_\lambda}$ is nilpotent.

The generalized eigenspace decomposition of F^n can be seen from Jordan Normal form but can also be proved without it. One can use the Chinese Remainder Theorem (CRT) on the polynomial ring $F[x]$. Recall that if $\gcd(m, n) = 1$ for $m, n \in \mathbb{Z}$ then

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

For the more general CRT, we recall the following definition.

Definition

Definition 13.0.2 (Comaximal ideals)**.** Let A, B be ideals of a ring R. Then A, B are said to be **comaximal** if $A + B = R$, where

$$A + B := \{a + b \mid a \in A, b \in B\}.$$

Lemma

Lemma 13.0.3 (Chinese Remainder Theorem)**.** *Let $A_1, \ldots, A_k$ be ideals in a ring R. The map*

$$R \to R/A_1 \times R/A_2 \times \cdots \times R/A_k$$

defined by

$$r \mapsto (r + A_1, r + A_2, \ldots, r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap \cdots \cap A_k$. If for each $i, j \in \{1, 2, \ldots, k\}$ with $i \neq j$ the ideals A_i and A_j are comaximal, *then this map is surjective and $A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k$, so*

$$\begin{aligned}R/(A_1 A_2 \cdots A_k) &= R/(A_1 \cap A_2 \cap \cdots \cap A_k)\\ &\cong R/A_1 \times R/A_2 \times \cdots \times R/A_k.\end{aligned}$$

Now take $R = F[x]$. By 13.0.3 there exists $f(x) \in F[x]$ such that $f(x) = \lambda_i \mod (x - \lambda_i)^{m_i}$ for all i, where the λ_i are the eigenvalues of A and $m_i = \dim F^n_{\lambda_i}$ is the generalized eigenspace, or equivalently $m_i =$ is the algebraic multiplicity of λ_i (i.e. how many repetitions of $(\lambda - \lambda_i)$ there are in a splitting field for the polynomial $\det(A - \lambda I) \in F[\lambda]$).

Remark 13.0.4. To say more about how 13.0.3 gives us the existence of $f(x) \in F[x]$ such that $f(x) = \lambda_i$ mod $(x-\lambda_i)^m_i$, notice that $(x-\lambda_i)$ and $(x-\lambda_j)$ for $\lambda_i \neq \lambda_j$ are comaximal since

$$\begin{aligned}\frac{1}{\lambda_j-\lambda_i}(x-\lambda_i) - \frac{1}{\lambda_j-\lambda_i}(x-\lambda_j) &= \frac{\lambda_j-\lambda_i}{\lambda_j-\lambda_i} \\ &= 1,\end{aligned}$$

where we used that $\lambda_i \neq \lambda_j$. For $(x-\lambda_i)^{m_i}$ and $(x-\lambda_j)^{m_j}$ we see that if they shared a common factor $d(x) \in F[x]$ so that $d(x)$ divided both $(x-\lambda_i)^{m_i}$ and $(x-\lambda_j)^{m_i}$ and $d(x)$ was not trivial, then $d(x)$ would have to include factors $(x-\lambda_i)(x-\lambda_j)$, but this is impossible since we would then have e.g. $(x-\lambda_i)^{m_i} = q(x)d(x)$ where the right-hand side would be zero for λ_j but the left-hand side would be non-zero. Therefore we claim it follows that $\gcd((x-\lambda_i)^{m_i}, (x-\lambda_j)^{m_j}) = 1$, and so since $F[x]$ is a Bezout-domain, it follows that there are $a(x), b(x) \in F[x]$ such that $a(x)(x-\lambda_i)^{m_i} + b(x)(x-\lambda_j)^{m_j} = 1 \rightsquigarrow (x-\lambda_i)^{m_i}, (x-\lambda_j)^{m_j}$ are comaximal. Since λ_i, λ_j were arbitrary eigenvalues of A, we can apply 13.0.3 and get a *surjective* map

$$\varphi : F[x] \twoheadrightarrow \prod_i F[x]/(x-\lambda_i)^{m_i}$$

defined by $f(x) \mapsto (f(x) \mod (x-\lambda_1)^{m_1}, f(x) \mod (x-\lambda_2)^{m_2}, \dots, f(x) \mod (x-\lambda_n)^{m_n})$ (given that A has n distinct eigenvalues). Therefore, by surjectivity of φ we know that there exists a $f(x) \in F[x]$

$$\begin{aligned}\varphi(f(x)) &= (f(x) \mod (x-\lambda_1)^{m_1}, f(x) \mod (x-\lambda_2)^{m_2}, \dots, f(x) \mod (x-\lambda_n)^{m_n}) \\ &= (\lambda_1 \mod (x-\lambda_1)^{m_1}, \lambda_2 \mod (x-\lambda_2)^{m_2}, \dots, \lambda_n \mod (x-\lambda_n)^{m_n}).\end{aligned}$$

This gives existence. To show uniqueness $\mod \prod_i (x-\lambda_i)^{m_i}$, assume that there was $g(x) \in F[x]$ where $f(x) \neq g(x)$ such that the same holds for $g(x)$. Then $f(x) - g(x) \equiv 0 \mod (x-\lambda_i)^{m_i}$ for $i = 1, \dots, n$ so that $f(x) \equiv g(x) \mod (x-\lambda_i)^{m_i}$ for each $i = 1, \dots, n$.

We want to prove that there is a decomposition $F^n = \bigoplus_{\lambda \in \Lambda} F^n_\lambda$ where Λ is the set of eigenvalues for $A \in M_n(F)$ and F is algebraically closed.

Proof. Assume $A \in M_n(F)$ for F algebraically closed and that Λ is the set of eigenvalues for A. Since F is algebraically closed, the minimal polynomial (which if I recall correctly we have shown exists) $m_A(x) \in F[x]$ splits completely due. Therefore we have

$$m_A(x) = \prod_{i=1}^{k} (x-\lambda_i)^{e_i}$$

where $n = |\Lambda|$. We want to prove that $F^n = \mathcal{N}((A-\lambda_1 I)^{e_1}) \oplus \cdots \oplus \mathcal{N}((A-\lambda_k I)^{e_k})$ where $\mathcal{N}((A-\lambda_i I)^{e_i})$ is the *null-space* of $(A-\lambda_i I)^{e_i}$ in F^n. Notice that then $q(t) = (t-\lambda_i)^m$ is an *annihilating* polynomial for v. On the other hand, $m_A(t)$ restricted to $F^n_{\lambda_i}$ is $p(t) = (t-\lambda_i)^{e_i}$. Furthermore we have that $p(A)v = 0$ for all $v \in F^n_{\lambda_i}$.

Proposition 13.0.5. *If f_1, f_2 are two polynomials that are relatively prime and are not identically zero and $f(A) = f_1(A) f_2(A)$ is an annihilating polynomial, then $F^n = \mathcal{N}(f_1(A)) \oplus \mathcal{N}(f_2(A))$ and $\mathcal{N}(f_1(A))$ and $\mathcal{N}(f_2(A))$ are invariant under the linear transformation defined by A (by invariant we mean that if v is in some subspace then Av is also in the same subspace).*

Proof. Since f_1, f_2 are not identically zero and $F[x]$ is a Bezout domain, there are polynomials $p_1, p_2 \in F[x]$ sucht that $p_1 f_1 + p_2 f_2 = 1$. Therefore, using the ring-homomorphism to $F[A]$ we get that

$$p_1(A) f_1(A) + p_2(A) f_2(A) = I. \tag{13.0.1}$$

By multiplying both sides of the equation 13.0.1 by $v \in F^n$ we get that

$$\begin{aligned} v &= \underbrace{p_1(A)f_1(A)v}_{v_1} + \underbrace{p_2(A)f_2(A)v}_{v_2} && (13.0.2)\\ &= v_1 + v_2. && (13.0.3) \end{aligned}$$

If we multiply v_1 by $f_2(A)$ and v_2 by $f_1(A)$, we get that

$$\begin{aligned} f_2(A)v_1 &= f_1(A)p_1(A)f_2(A)v \\ &= p_1(f_1(A)f_2(A))v, \qquad \text{since } F[A] \text{ is a commutative ring} \\ &= p_1 f(A)v \\ &= 0 \end{aligned}$$

and

$$\begin{aligned} f_1(A)v_2 &= f_1(A)(p_2(A)f_2(A))v \\ &= p_2(A)f_1(A)f_2(A)v \\ &= p_2 f(A)v \\ &= 0, \end{aligned}$$

so that $v_1 \in \mathcal{N}(f_2(A))$ and $v_2 \in \mathcal{N}(f_1(A))$. Since $v \in F^n$ was arbitrary, we have that $F^n = \mathcal{N}(f_1(A)) + \mathcal{N}(f_2(A))$.

We want to show that the sum is *direct* by showing that for each $v \in F^n$ there are *unique* $v_1 \in \mathcal{N}(f_1(A))$ and $v_2 \in \mathcal{N}(f_2(A))$ such that $v = v_1 + v_2$. To see that this implies that it is a direct sum notice that if then $\mathcal{N}(f_1(A)) \cap \mathcal{N}(f_2(A)) \neq 1$ so there is some $a = b = v$ in the intersection then we can write v non-uniquely contradicting that we could write v uniquely. So to see that we can write any v uniquely:

Assume to the contrary that $v = v_1 + v_2$ and $v = w_1 + w_2$ with $w_1 \in \mathcal{N}(f_1(A))$ and $w_2 \in (f_2(A))$. Then we have

$$\begin{aligned} v_1 + v_2 &= w_1 + w_2 \\ \Leftrightarrow v_1 - w_1 &= w_2 - v_2 && (13.0.4) \end{aligned}$$

and if we then multiply equation 13.0.1 on both sides by $v_1 - w_1$ we get

$$\begin{aligned} v_1 - w_1 &= p_1(A)f_1(A)(v_1 - w_1) + p_2(A)f_2(A)(v_1 - w_1) \\ &= p_2(A)f_2(A)(v_1 - w_1), \qquad \text{since } v_1, w_1 \in \mathcal{N}(f_1(A)) \\ &= p_2(A)f_2(A)(w_2 - v_2), \qquad \text{by equation 13.0.4} \\ &= 0, \qquad \text{since } w_2, v_2 \in \mathcal{N}(f_2(A)) \\ \Rightarrow v_1 &= w_1. \end{aligned}$$

Therefore, from $v_1 + v_2 = w_1 + w_2$ by subtracting $v_1 = w_1$ from both sides we get that $v_2 = w_2$, which shows uniqueness. We conclude that $F^n = \mathcal{N}(f_1(A)) \oplus \mathcal{N}(f_2(A))$.

Lastly, if $v \in \mathcal{N}(f_i(A))$ then $f_i(A)v = 0$. But then

$$\begin{aligned} f_i(A)(Av) &= Af_i(A)v \\ &= 0, \end{aligned}$$

so that $Av \in \mathcal{N}(f_i(A))$. Therefore $\mathcal{N}(f_i(A))$ is an A-invariant subspace of F^n. $\square$

We now go on to prove the main theorem:

Let $m_A(t) = \prod_i (t-\lambda_i)^{e_i}$ be the minimal polynomial of A in $F[x]$. Since the minimal polynomial must divide any other polynomial $q(x)$ for which $q(A) = 0$, it follows that $m_A(t)$ must divide the characteristic polynomial of A, therefore the roots of $m_A(t)$ are the eigenvalues of A, i.e. λ_i are eigenvalues associated with A. In fact, since we have that $m_A(t) = (t-\lambda)f(t) + m_A(\lambda)$ we see that

$$\begin{aligned}
m_A(A) &= (A-\lambda_i)f(A) + m_A(\lambda_i) \\
\Leftrightarrow 0 &= (A-\lambda_i I)f(A) + m_A(\lambda_i) \\
\Leftrightarrow 0 &= (A-\lambda_i I)p(\lambda_i)v + m_A(\lambda_i) \\
\Leftrightarrow 0 &= q(\lambda_i)\underbrace{(A-\lambda_i I)v}_{=0} + m_A(\lambda_i) \\
\Leftrightarrow 0 &= m_A(\lambda_i).
\end{aligned}$$

which we claims shows that any eigenvalue λ_i is a root of $m_A(t)$.

Moving on, we start with $f_1(t) = (t-\lambda_1)^{e_1}$ and $g_1(t) = \prod_{i=2}^k (t-\lambda_i)^{e_i}$. These polynomials are relatively prime and non-zero, and their product is an annihilating polynomial of A since the product is equal to the minimal polynomial of A, $m_A(t)$. Therefore by the previous lemma we have that

$$F^n = \mathcal{N}(f_1(A)) \oplus \mathcal{N}(g_1(A)).$$

Now consider $\mathcal{N}(g_1(A))$ and define $f_2(t) = (t-\lambda_2)^{e_2}$ and $g_2(t) = \prod_{i=3}^k (t-\lambda_i)^{e_i}$. These polynomials are again relatively prime, non-zero and their product is an annihilating polynomial for the space $\mathcal{N}(g_1(A))$ in the sense that restricting to $v \in \mathcal{N}(g_1(A))$ we have that $f_2(A)g_2(A)|_{\mathcal{N}(g_1(A)} \equiv 0$. But notice that $\mathcal{N}(g_1(A)) \cong F^m$ for some $m \geqslant 1$. Therefore, we can apply the same lemma again, to get that $\mathcal{N}(g_1(A)) = \mathcal{N}(f_2(A)) \oplus \mathcal{N}(g_2(A))$.

Therefore, we have that

$$\begin{aligned}
\mathcal{N}(m_A(t)) &= \mathcal{N}(f_1(A)) \oplus \mathcal{N}(g_1(A)) \\
&= \mathcal{N}(f_1(A)) \oplus (\mathcal{N}(g_2(A)) \oplus \mathcal{N}(f_2(A)))
\end{aligned}$$

where we notice that $\mathcal{N}(f_i(A)) = \{v \in F^n \mid (A-\lambda_i)^{e_i}v = 0\}$. By repeatedly (in a finite number of steps) performing the same operation, we see that we get

$$\begin{aligned}
\mathcal{N}(m_A(t)) &= \mathcal{N}(f_1(A)) \oplus \cdots \oplus \mathcal{N}(f_k(A)) \\
&= \mathcal{N}((A-\lambda_1 I)^{e_1}) \oplus \cdots \oplus \mathcal{N}((A-\lambda_k I)^{e_k}).
\end{aligned}$$

This shows that we have a decomposition

$$F^n = \bigoplus_{\lambda \in \Lambda} \mathcal{N}((A-\lambda_i)^{e_i}).$$

It remains to show that

$$F^n = \bigoplus_{\lambda \in \Lambda} F^n_\lambda$$

where $F^n_\lambda = \{v \in F^n \mid (A-\lambda)^m v = 0 \text{ for some } m \geqslant 1\}$.

We aim to show that $\mathcal{N}((A-\lambda_i I)^{e_i}) = F^n_{\lambda_i}$.

$\underline{\mathcal{N}((A-\lambda_i)^{e_i}) \subseteq F^n_{\lambda_i}}$: If v is such that $(A-\lambda_i)^{e_i}v = 0$ then since $e_i \geqslant 1$ it follows that $v \in F^n_{\lambda_i}$ so that $\mathcal{N}((A-\lambda_i)^{e_i}) \subseteq F^n_{\lambda_i}$.

$\underline{F^n_{\lambda_i} \subseteq \mathcal{N}((A-\lambda_i I)^{e_i})}$: Assume that $v \in F^n$ is such that there is some $m \geqslant 1$ such that $(A-\lambda_i I)^m v = 0$. If $m \leqslant e_i$ then

$$\begin{aligned}
(A-\lambda_i I)^m v &= 0 \\
\Rightarrow (A-\lambda_i I)^{e_i} v &= (A-\lambda_i I)^{e_i-m}(A-\lambda_i I)^m v \\
&= (A-\lambda_i I)^{e_i-m} 0 \\
&= 0.
\end{aligned}$$

On the other hand, if $m > e_i$ is such that $(A-\lambda_i)^m v = 0$. We then have that $m = e_i + r$. Then we see that

$$\begin{aligned}
(A-\lambda_i I)^m v &= (A-\lambda_i I)^{e_i+r} \\
&= (A-\lambda_i I)^{e_i}(A-\lambda_i I)^r v \\
&= (A-\lambda_i I)^{e_i} w, \qquad \text{where } w = (A-\lambda_i I)^r v \\
\Rightarrow (A-\lambda_i I)^{e_i} w &= 0
\end{aligned}$$

so that $w \in \mathcal{N}((A-\lambda_i I)^{e_i})$.

Define $d = \min\{k \geqslant 1 \mid (A-\lambda_i I)^d v = 0\}$ so that $(A-\lambda_i I)^d v = 0$ and $(A-\lambda_i I)^{d-1} v \neq 0$. We have that $m_A(t) = (t-\lambda_i)^{e_i} q(t)$ where $q(\lambda_i) \neq 0$. We know that $m_A(A)v = 0$ so that

$$\left[(A-\lambda_i I)^{e_i} q(A)\right] v = 0.$$

By the division algorithm we have that $m_A(t) = (t-\lambda_i)^d g(t) + h(t)$ where $\deg(h(t)) = 0$ or $\deg(h(t)) < d$. First we substitute A for t and then multiply by v. Then we get

$$\begin{aligned}
m_A(A)v &= (A-\lambda_i)^d g(A)v + h(A)v \\
\Leftrightarrow 0 &= \underbrace{g(A)(A-\lambda_i I)^d v}_{=0} + h(A)v, \qquad \text{since } (A-\lambda_i I)^d, g(A) \in F[A] \text{ which is a commutative ring} \\
\Leftrightarrow 0 &= h(A)v.
\end{aligned}$$

If $h(A) \neq 0$ then since

$$\begin{aligned}
m_A(\lambda_i) &= (\lambda_i - \lambda_i)^d g(\lambda_i) + h(\lambda_i) \\
\Leftrightarrow 0 &= h(\lambda_i).
\end{aligned}$$

We aim to show that any polynomial $p(t) \in F[t]$ can be written on the form $p(t) = c_0 + c_1(t-\lambda_i) + c_2(t-\lambda_i)^2 + \ldots + c_k(t-\lambda_i)^k$.

Notice that $\{1, t, t^2, \ldots\}$ is a basis for $F[t]$. Define $\mu = t - \lambda_i$ so that $t = \mu + \lambda_i$. Then we have that $p(t) = p(\mu + \lambda_i)$ (and pay attention to the fact that this is a polynomial of the same degree in $F[\mu]$), and any polynomial in $F[\mu]$ can be written as a F-linear combination of the elements $\{1, \mu, \mu^2, \ldots\}$. Since λ_i is a scalar, we have that $p(\mu+\lambda_i) \in F[\mu]$, therefore $p(\mu + \lambda_i) = c_0 + c_1\mu + \ldots + c_k\mu^k$. But $\mu = t - \lambda_i$ gives us that

$$\begin{aligned}
p(t) &= p(\mu + \lambda_i) \\
&= c_0 + c_1(t-\lambda_i) + \ldots + c_k(t-\lambda_i)^k.
\end{aligned}$$

Since $\deg(h(t)) = k < d$ we can write $h(t) = c_0 + c_1(t-\lambda_i) + \ldots + c_k(t-\lambda_i)^k$ where $k < d$. Then we have that

$$\begin{aligned}
h(A) &= c_0 + c_1(A-\lambda_i I) + \ldots + c_k(A-\lambda_i I)^k \\
\Rightarrow h(A)v &= c_0 v + c_1(A-\lambda_i I)v + \ldots + c_k(A-\lambda_i I)^k v \\
\Leftrightarrow 0 &= c_0 v + c_1(A-\lambda_i I)v + \ldots + c_k(A-\lambda_i I)^k v.
\end{aligned}$$

We claim that this is impossible, since $\{v, (A-\lambda_i I)v, \ldots, (A-\lambda_i I)^k v\}$ is a linearly independent set of vectors, unless $h(t) \equiv 0$. But if $h(t) = 0$ then $m_A(t) = (t-\lambda_i)^d g(t)$ so that $(t-\lambda_i)^d$ divides the minimal polynomial. We see that it follows that $d \leqslant e_i$. Since $d \leqslant e_i$ we have that

$$\begin{aligned}(A-\lambda_i I)^{e_i} v &= (A-\lambda_i I)^{e_i - d}[(A-\lambda_i I)^d v] \\ &= 0,\end{aligned}$$

since d was minimal such that this holds. Therefore, we conclude that $v \in \mathcal{N}((A-\lambda_i I)^{e_i})$. Notice that the most important thing was that we showed that $d \leqslant e_i$, since the last step above then followed easily from how we defined d. $\square$

Example 13.0.6. Let

$$B = \begin{pmatrix} 2 & 1 & \\ & 2 & \\ & & 3 \end{pmatrix}.$$

First observe that much more generally, for upper triangular matrices it holds that the eigenvalues of a matrix are those on the main diagonal, so that $\lambda_1 = 2, \lambda_2 = 3$ are the eigenvalues of B. Then we have two Jordan Blocks, the first one being

$$B_{\lambda_1} = \begin{pmatrix} 2 & 1 \\ & 2 \end{pmatrix}$$

and the second being just $B_{\lambda_2} = 3$.

We then have

$$\begin{aligned}(B-\lambda_2)^2 &= \begin{pmatrix} & 1 & \\ & & \\ & & 1 \end{pmatrix}^2 \\ &= \begin{pmatrix} & & \\ & & \\ & & 1 \end{pmatrix}\end{aligned}$$

so that $F^3_{\lambda_1} = \operatorname{span}(e_1, e_2)$ where $e_1 = (1,0,0)$ and $e_2 = (0,1,0)$. For $\lambda_2 = 3$, we have that

$$B - I\lambda_2 = \begin{pmatrix} -1 & 1 & \\ & -1 & \\ & & \end{pmatrix}$$

So if $(B - I\lambda_2)v = 0$ then we see that if $v = (v_1, v_2, v_3)$ then we have

$$\begin{cases} -v_1 + v_2 = 0 \\ -v_2 = 0 \end{cases}$$

so that $v_2 = 0 \Rightarrow v_1 = 0$. There are no restrictions imposed on $v_3 \rightsquigarrow F^3_{\lambda_3} = \operatorname{span}(e_3)$.

We can then write $B = B_s + B_n$ where

$$B_s = \begin{pmatrix} 2 & & \\ & 2 & \\ & & 3 \end{pmatrix}$$

is semisimple (diagonalizable) and where

$$B_n = \begin{pmatrix} & 1 & \\ & & \\ & & \end{pmatrix}$$

which is nilpotent, since $B_n^2 = 0$.

Going back to the proof, we want $A = A_s + A_n$. Let $A_s := f(A)$ and

$$\begin{aligned} A_n &= A - f(A) \\ &= A - A_s. \end{aligned}$$

We claim that $A_s|_{F^n_{\lambda_i}}$ is a scalar multiple of λ_i.

Proof. Since $f(x) = \lambda_i \mod (x - \lambda_i)^{m_i}$ we have that $f(x) = \lambda_i + g_i(x)(x - \lambda_i)^{m_i}$ where $g_i(x) \in F[x]$.

Here we use that $F[A] = \{f(A) \mid f \in F[x]\}$ is a (commutative) subalgebra of $M_n(F)$. We let

$$\begin{aligned} f(A) + g(A) &= (f + g)(A) \\ &= (g + f)(A) \\ &= g(A) + f(A) \end{aligned}$$

$$\begin{aligned} f(A)g(A) &= (f \cdot g)(A) \\ &= (g \cdot f)(A) \\ &= g(A)f(A) \end{aligned}$$

and

$$f(A) = kI$$

when $f(x) = k \in F$, or just generally $f(A) = b_0A^0 + b_1A^1 + + \ldots + b_{n-1}A^{n-1} + b_nA^n$ when $f(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1} + b_nx^n$ where $A^0 = I$. I.e. $F[A]$ is basically the image under the evaluation-map that takes $f(x) \in F[x]$ to $f(A)$, which we showed earlier was a ring-homomorphism.

Then we have that if $f(x) = \lambda_i + g_i(x)(x - \lambda_i)^{m_i}$ then

$$f(A) = \lambda_i I + g_i(A)(A - \lambda_i)^{m_i}$$

and so that

$$\begin{aligned} f(A)v &= (\lambda_i I + g_i(A)(A - \lambda_i)^{m_i})v \\ &= \lambda_i v + g_i(A) \underbrace{(A - \lambda_i)^{m_i} v}_{=0} \\ &= \lambda_i v \end{aligned}$$

for $v \in F^n_{\lambda_i}$. □

Notice that $i = 1, \ldots, n$ was arbitrary in the proof above. What conclusion can we draw from the fact that $A_s|_{F^n_{\lambda_i}}$. Well, this means that $f(A)$ acts by scalar multiplication on each $F^n_{\lambda_i}$ for each eigenvalue λ_i, i.e. the jordan block of A_s corresponding to its action on $F^n_{\lambda_i}$ is by scalar multiplication, therefore its block is diagonal, so $A|_s$ can be written as a diagonal matrix in Jordan block form where each block is of dimension 1×1, I believe.

Uniqueness: Assume that $A := A'_s + A'_n$ is another Jordan decomposition such that $A'_s + A'_n = A_s + A_n$. Then we have that $A_s - A'_s = A'_n - A_n$.

Furthermore, consider the fact that A'_s, A'_n commute under multiplication, and that we have that $A = A'_s + A'_n$ so that $A'_s = A - A'_n$. Furthermore, we have that

$$\begin{aligned}
A'_sA &= (A - A'_n)A \\
&= A^2 - A'_n(A) \\
&= A^2 - A'_n(A'_s + A'_n) \\
&= (A'_s + A'_n)^2 - A'_n(A'_s + A'_n) \\
&= (A'_s)^2 + 2A'_sA'_n + (A'_n)^2 - A'_nA'_s - (A'_n)^2 \\
&= (A'_s)^2 + A'_sA'_n \\
&= (A'_s)^2 + A'_sA'_n \\
&= (A'_s + A'_n)A'_s \\
&= AA'_s
\end{aligned}$$

so that A, A'_s commutes.

Furthermore, we have that

$$\begin{aligned}
A'_n(A) &= (A - A'_s)A \\
&= A^2 - A'_sA \\
&= (A'_s + A'_n)^2 - A'_s(A'_s + A'_n) \\
&= \cancel{(A'_s)^2} + \cancel{2}A'_sA'_n + (A'_n)^2 - \cancel{(A'_s)^2} - \cancel{A'_sA'_n} \\
&= A'_sA'_n + (A'_n)^2 \\
&= (A'_s + A'_n)A'_n \\
&= AA'_n
\end{aligned}$$

so that A, A'_n also commutes.

From this, it is clear that A'_s, A'_n commutes with any $h(A)$ with $h \in F[x]$ arbitrary, so in particular it follows that A'_s commute with $f(A) := A_s$, and that A'_n commutes with

$$\begin{aligned}
A_n &= A - A_s \\
&= A - f(A)
\end{aligned}$$

since A'_n commutes with both $f(A)$ and A.

Lemma

Lemma 13.0.7. *If $A, B \in M_n(F)$ are diagonalizable matrices such that $AB = BA$ then, $A - B$ is diagonalizable.*

Proof. By theorem 8.0.1 there is some $g \in \mathsf{GL}(V)$ such that $gAg^{-1} = D_1$ and $gBg^{-1} = D_2$. Then we have that

$$\begin{aligned}
g(A - B)g^{-1} &= gAg^{-1} - gBg^{-1} \\
&= D_1 - D_2 \\
&= D_3
\end{aligned}$$

which is diagonal, since the subtraction of one diagonal matrix from another is diagonal itself. $\square$

It follows from lemma 13.0.7 that $A_s - A'_s$ is diagonalizable, i.e. semisimple.

Lemma

Lemma 13.0.8. *If $A, B \in M_n(F)$ (assume F is algebraically closed) are nilpotent and $AB = BA$ then it follows that $A - B$ is nilpotent.*

Proof. Commuting matrices over an algebraically closed field are simultaneously trigonalizable by 8.0.1, so there is some P such that $P^{-1}AP = T_A$ and $P^{-1}BP = T_B$ where T_A, T_B are on upper-triangular form. Then $P(A-B)P^{-1} = T_A - T_B$ which is also on upper triangular form. But notice that similar matrices have the same characteristic equation so the same eigenvalues and A, B have all eigenvalues 0 so so must T_A, T_B and the diagonal elements of T_A, T_B are zero, hence so are $T_A - T_B$. $\square$

Since A'_n, A_n are commuting nilpotent matrices, by lemma 13.0.8 we have that $A'_n - A_n$ is nilpotent.

Therefore, we see that $A_s - A'_s = A'_n - A_n$ is both nilpotent and semisimple.

Lemma

Lemma 13.0.9. *If $A \in M_n(F)$ for F algebraically closed is both semisimple and nilpotent, then $A = 0$.*

Proof. That A is semisimple means that there is some invertible matrix $P \in \mathsf{GL}(n)$ such that $P^{-1}AP = D$.

Consider that

$$\begin{aligned}\det(D - \lambda I) &= \det(P^{-1}AP - \lambda I)\\ &= \det(P^{-1}AP - P^{-1}\lambda IP)\\ &= \det(P^{-1}(A - \lambda I)P)\\ &= \det(P^{-1})\det(A-\lambda I)\det(P)\\ &= \det(P)^{-1}\det(A-\lambda I)\det(P)\\ &= \det(A - \lambda I)\end{aligned}$$

But since A is nilpotent all of its eigenvalues are 0, hence all of D:s eigenvalues are 0. But $\det(D-\lambda I) = \prod_i (d_i - \lambda)$ and so if some $d_i \neq 0$ then we will have some eigenvalue $\lambda_i = d_i$ different from zero. Therefore $d_i = 0$ for all $i = 1, \ldots, n$ and so $D = \mathbf{0}$ is the zero matrix of dimension $n \times n$. $\square$

It follows from 13.0.9 that

$$\begin{aligned} A_s - A'_s &= 0\\ A'_n - A_n &= 0\\ \Leftrightarrow A_s = A'_s &\text{ and } A'_n = A_n.\end{aligned}$$

$\square$

Notice that if $f'(x) = f(x) + g(x)\prod(x-\lambda_i)^{m_i} \rightsquigarrow f'(A) = f(A) + \underbrace{g(A)\det(A - \lambda_i I)}_{=0}$.

13.0.1 Analogue in a group G (not necessarily algebraic group, not necessarily finite)

Definition

Definition 13.0.10.
- Let $x \in G$ have finite order n.
- Let p be a prime.
  - x is **p-regular** if $\gcd(n, p) = 1$.
  - x is **p-singular** if $n = p^a$ for some $a \geqslant 0$.

We saw in HW3 that there exists a *unique* decomposition $x = yz$ with y p-regular and z p-singular such that $yz = zy$. This is simpler than algebraic group Jordan Decomposition since y is a power of x, not just a polynomial in x.

Recall that $R(G) =$ the maximal normal connected solvable subgroup of G (9.0.5), called the **radical of** G, and that

$$G \text{ semisimple} \Leftrightarrow R(G) = 1.$$

Furthermore we had that $R_u(G) =$ maximal connected unipotent normal subgroup of G (8.0.24), where it held that

$$G \text{ reducitve} \Leftrightarrow R_u(G) = 1.$$

Theorem

Theorem 13.0.11.
- *N_1, N_2 normal $\Rightarrow N_1N_2$ normal.*
- *N_1, N_2 connected $\Rightarrow N_1N_2$ connected.*
- *N_1, N_2 solvable $\Rightarrow N_1N_2$ solvable.*

The product of two unipotent matrices need not be unipotent, but the product of two unipotent upper-triangular matrices is unipotent! Since upper-triangluar $\Rightarrow$ eigenvalues are on the diagonal and if unipotent then all diagonal entries are 1.

If N_1, N_2 unipotent and $N_1, N_2 \subset \mathsf{Triag}^+(n) \Rightarrow N_1N_2 \subset \mathsf{Uniag}^+(n)$, i.e. N_1N_2 is unipotent $\Rightarrow \exists!$ maximal connected normal unipotent subgroup, i.e. $R_u(G)$ is well-defined.

We also have that

$$\begin{aligned} R_uG &= (RG)_u \\ &= \text{all unipotent elements in } RG. \end{aligned}$$

Theorem

Theorem 13.0.12. *For all algebraic groups G, we have a short exact sequence*

$$1 \to R_uG \to G \xrightarrow{\pi} G/R_uG \to 1$$

and G/R_uG is reductive.

Remark 13.0.13. To prove something for all algebraic groups G, it is enough to prove it for reductive G, unipotent G and show that it is closed under extensions.

Proof. □

13.0.2 Positive systems

Basic fact: Every positive root $\alpha \in \Phi^+$ is a nonnegative $\mathbb{Z}$-linear combination of *simple* roots. If (V, Φ) is a root system, then Δ is a *basis* of V.

$$\beta, \gamma \in \Phi^+ \Rightarrow \beta = \sum_{\alpha \in \Delta} m_\alpha(\beta)\alpha \text{ and } \gamma = \sum_{\alpha \in \Delta} m_\alpha(\gamma)\alpha$$

where $m_\alpha(\beta), m_\alpha(\gamma) \geqslant 0$ for all $\alpha \in \Delta$.

Partial order: $\beta \geqslant \gamma$ if $m_\alpha(\beta) \geqslant m_\alpha(\gamma)$ for all $\alpha \in \Delta$.

Theorem

Theorem 13.0.14. *Assume that (V, Φ) is an reduced + irreducible root system. Then there exists a unique highest root α^h, i.e. a unique maximal element with respect to "$\geqslant$".*

$$\alpha^h = \sum_{\alpha \in \Delta} m(\alpha)\alpha$$

where $m(\alpha) \geqslant 1$ for all $\alpha \in \Delta$.

Example 13.0.15. Let Φ be of type A_{n-1} so that $\Phi = \{e_i - e_j \quad 1 \leqslant i \neq j \leqslant n\}$ and $\Delta = \{e_1 - e_2, e_2 - e_3, \ldots, e_{n-1} - e_n\}$. Then

$$\alpha^h = (e_1 - e_2) + (e_2 - e_3) + \ldots + (e_{n-1} - e_n),$$

so that $m(\alpha) \geqslant 1$ for all $\alpha \in \Delta$. Furthermore, for all $e_i - e_j$ with $i < j$ we have that

$$\begin{aligned} e_i - e_j &= (e_i - e_{i+1}) + (e_{i+1} - e_{i+2}) + \ldots + (e_{j-1} - e_j) \\ &\leqslant e_1 - e_n. \end{aligned}$$

Existence of $\Phi^+ \subset \Phi$: Let $e_1, \ldots, e_n$ be a basis of V. Choose a *lexicographical ordering*:

$$\sum a_i e_i > \sum b_i e_i$$

if for the smallest j such that a_j, b_j are not both zero we have that $a_j > b_j$. Define

$$\Phi^+ = \{\alpha \in \Phi \mid \alpha > 0\}$$

, by which we mean $\alpha \in \Phi$ such that the first non-zero coefficient of α in the basis $e_1, \ldots, e_n$ is positive. Then Φ^+ is a system of positive roots.

Theorem

Theorem 13.0.16. *Let Δ be a base of simple roots. The order of $\prod_{\alpha \in \Delta} s_\alpha$ does not depend on the ordering of Δ. It's the Coxeter number h of (V, Φ). If $\alpha^h = \sum_{\alpha \in \Delta} m(\alpha)\alpha \Rightarrow h = 1 + \sum_{\alpha \in \Delta} m(\alpha)$.*

Remark 13.0.17. The element $\prod_{\alpha \in \Delta} s_\alpha$ is known as the **Coxeter element**, I believe.

Example 13.0.18. $\Delta = \{e_1 - e_2, e_2 - e_3, \ldots, e_{n-1} - e_n\}$ and $s_{e_i - e_{i+1}} = (i\ i+1)$ so that

$$\begin{aligned} \prod_{\alpha \in \Delta} s_\alpha &= (12)(23) \cdots (n-1\ n) \\ &= (1 \cdots n), \end{aligned}$$

with order n. $h = n$ of type A_{n-1}.

$$\sum_{\alpha \in \Delta} m(\alpha) = \underbrace{1 + 1 + \ldots + 1}_{n-1}.$$

Chapter 14

Classification and irreducible representations via root data

14.0.1 Conclusions?

Reductive groups:

1. Classification by root data.
2. Representations.

Let G be a connected, reductive algebraic group over an algebraically closed field F. Here we mean connecte with respect to the $\mathfrak{Z}$ariski-topology, and by reductive we mean that $R(G) = 1$. Let $T \subset G$ be a maximal torus. Recall that all maximal tori of G are G-conjugate.

Let $\mathfrak{g} = \mathsf{Lie}(G)$, the Lie-algebra of G, and let $\mathcal{J} \in \mathsf{GL}(n, F)$. Then we have the following examples.

$$\begin{aligned}
\mathsf{Lie}(G^{\mathcal{J}}) &= \{A \in M_n(F) \mid {}^tA\mathcal{J} + \mathcal{J}A = 0\} \\
\mathsf{Lie}(\mathsf{SL}(n)) &= \{A \mid \mathrm{tr}A = 0\} \\
\mathsf{Lie}(\mathsf{GL}(n)) &= M_n.
\end{aligned}$$

Remark 14.0.1. We have G act on $\mathsf{Lie}(G)$ by conjugation.

Adjoint representation:

$$\begin{tikzcd}
\mathsf{Ad}: & G \arrow[r] \arrow[d, leftrightarrow] & \mathsf{GL}(\mathfrak{g}) \\
& T \arrow[ur] &
\end{tikzcd}$$

The adjoint action is the action by conjugation of G on its Lie algebra $\mathsf{Lie}(G) = \mathfrak{g}$, i.e. $\mathsf{Ad}(g)(X) = gXg^{-1}$ for $g \in G$ and $X \in \mathfrak{g}$.

Let $r : T \to \mathsf{GL}(V)$ be a representation of a torus T. Given a basis $e_1, \ldots, e_n$ of V, $\mathsf{GL}(V) = \mathsf{GL}(n)$. We have seen that $r(T)$ is conjugate to a subgroup of $\mathrm{Diag}(n)$ (where?). This implies (why?) that every irreducible representation of T is one-dimensional.

Stronger. r is a direct sum of 1-dimensional representations (I believe this is in the context of *any* (not necessarily irreducible) representation of T).

Up to isomorphism, we may assume that $r(t)$ is diagonal, i.e.

$$r(t) = \begin{pmatrix} \chi_1(t) & & & \\ & \chi_2(t) & & \\ & & \ddots & \\ & & & \chi_n(t) \end{pmatrix}$$

where $\chi_i(t) = i^{\text{th}}$ diagonal entry of $r(t)$ and $\chi_i \in X^*(T) = \mathrm{Hom}(T, \mathbb{G}_m)$ where we can think of $\mathbb{G}_m = \mathsf{GL}(1)$. Then we have that $r = \bigoplus_{i=1}^{n} \chi_i$.

Example 14.0.2. Let $A = \{i \mid \chi_i = \chi_1\}$, then $V_{\chi_1} = \mathrm{span}(e_i \mid \in A)$. For all $\lambda \in X^*(T)$ the λ-weight space of V (relative to r) is

$$V_\lambda = \{v \in V \mid r(t)v = \lambda(t)v, \forall t \in T\}.$$

"λ-eigenspace": $v \in V_\lambda$ is a simultaneous eigenvector for all $r(t)$ with varying λ-value $\lambda(t)$.

T torus $\Rightarrow V = \bigoplus_{\lambda \in X^*(T)} V_\lambda$. This is the **weight-space decomposition of V relative to** (T, r).

Going back to the adjoint action, to give one example we have

$$\begin{tikzcd} \mathsf{Ad}: & \mathsf{GL}(n) \arrow[r] \arrow[d, leftrightarrow] & \mathsf{GL}(M_n) \\ & \mathrm{Diag}(n) \arrow[ur] & \end{tikzcd}$$

since with $G = \mathsf{GL}(n)$ we have that $\mathsf{Lie}(\mathsf{GL}(n)) = M_n$ and so $\mathsf{GL}(\mathfrak{g}) = \mathsf{GL}(M_n)$ since $\mathsf{Lie}(\mathsf{GL}(n)) = M_n$, and furthermore $T = \mathrm{Diag}(n)$ is the prototypical torus for $\mathsf{GL}(n)$.

Definition

Definition 14.0.3. The set of roots $\Phi := \Phi(G, T)$ of T in G is the set of non-zer weights of $\mathsf{Ad}|_T : T \to \mathsf{GL}(\mathfrak{g})$.

$$0 \in X^*(T) \longleftrightarrow 0 : T \to 1$$

and root-space decomposition

$$\begin{aligned} \mathfrak{g} &= \mathfrak{t} \oplus \bigoplus_{\lambda \in X^*(T) \setminus \{0\}} \mathfrak{g}_\lambda \\ &= \mathfrak{t} \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha, \end{aligned}$$

with the weight-space $\mathfrak{g}_\alpha$ called the root space of the root $\alpha \in \Phi$.

Theorem

Theorem 14.0.4. *Let $\mathbb{Q}\Phi = span_{\mathbb{Q}}\Phi$ in $X^*(T) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then $(\mathbb{Q}\Phi, \Phi)$ is a root system.*

$$\begin{array}{ccc} \text{Connected reductive groups} & \longrightarrow & \text{root systems} \\ \\ (G,T) & \longmapsto & (\mathbb{Q}\Phi, \Phi(G,T)) \end{array}$$

Problem: The above root system does not determine G up to isomorphism.

Example 14.0.5.

$$\begin{tikzcd} (\mathsf{GL}(n), \mathrm{Diag}(n)) \arrow[dr] & \\ (\mathsf{SL}(n), \mathrm{Diag}^1(n)) \arrow[r] & \text{Root system of type } \mathsf{A}_{n-1} = (\mathbb{Q}_0^n, \{e_i - e_j \mid i \neq j\}) \\ (\mathsf{PGL}(n), \mathsf{PDiag}(n)) \arrow[ur] & \end{tikzcd}$$

where

- $\mathsf{Diag}^1(n) = \mathsf{Diag}(n) \cap \mathsf{SL}(n)$.
- $\mathsf{PDiag}(n) = \pi(\mathrm{Diag}(n))$ where $\pi : \mathsf{GL}(n) \to \mathsf{GL}(n)/Z(\mathsf{GL}(n)) = \mathsf{PGL}(n)$.

Solution to the problem above: Coroots (2.0.3). Recall that $X_*(T) = \mathrm{Hom}(\mathbb{G}_m, T)$ are the *cocharacters* (4.1.5). Furthermore, there is perhaps a pairing $\langle -, - \rangle : X^*(T) \times X_*(T) \to \mathbb{Z}$.

We have

$$\mathbb{G}_m \xrightarrow{\mu} T \xrightarrow{\chi} \mathbb{G}_m$$

where μ is a cocharacter and χ is a character. This gives us $\langle \chi, \mu \rangle \in \mathbb{Z}$, such that $\chi \circ \mu = (z \mapsto z^m)$.

Let $\alpha \in \Phi$ such that $\alpha : T \to \mathbb{G}_m$, i.e. such that α is a character, so that then $\ker \alpha \subset T$, and define $\mathrm{Cent}(\ker \alpha) := G_\alpha$. Since T is a (maximal, right) torus, we have that $\mathrm{Cent}_G(T) = T$.

Theorem

Theorem 14.0.6. *G_α is connected and reductive. $G_\alpha^{der} = [G_\alpha, G_\alpha]$ is of type A_1, i.e.*

$$G_\alpha^{der} \cong \mathsf{SL}(2) \text{ or } \mathsf{PGL}(2).$$

So we get

$$\begin{tikzcd} \mathsf{SL}(2) \arrow[r] \arrow[rrr, bend right, "\varphi_\alpha"'] & G_\alpha^{\mathrm{der}} \arrow[r, hook] & G_\alpha \arrow[r, hook] & G \end{tikzcd}$$

where φ_α is called the α-$\mathsf{SL}(2)$ of G.

In Char 2, $1 = -1$, but we still claim that $\mathsf{SL}(2) \neq \mathsf{PGL}(2)$. $\{\pm 1\}$ is a non-smooth, non-reduced contrived (?) group scheme in characteristic 2. We claim that (in some cases, e.g. $\mathbb{C}$) we have

$$\begin{aligned}\mathsf{SL}(2)/Z(\mathsf{SL}(2)) &= \mathsf{SL}(2)/\{\pm 1\}\\ &\cong \mathsf{PGL}(2).\end{aligned}$$

One would imagine that since $-1 = 1$ so that $\{\pm 1\} = \{1\}$ we would have an isomorphism, but we claim that this "intuitive picture" is false.

Definition

Definition 14.0.7 (Special type of coroot)**.** The **coroot** $\alpha^\vee : \mathbb{G}_m \to T$ is given by

$$\alpha^\vee(a) = \varphi_a\left(\begin{pmatrix} a & \\ & a^{-1}\end{pmatrix}\right).$$

Example 14.0.8. Let $G = \mathsf{GL}(n)$,and let

$$\alpha^\vee = e_i - e_j : a \mapsto \varphi_a\left(\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & \underbrace{a}_{i^{\text{th}}\text{ place}} & & & & \\ & & & \ddots & & & \\ & & & & \underbrace{a^{-1}}_{j^{\text{th}}\text{ place}} & & \\ & & & & & \ddots & \\ & & & & & & 1\end{pmatrix}\right)$$

Remark 14.0.9. The notes says z and z^{-1} in the matrix above, without φ_a, so this is my guess.

Definition

Definition 14.0.10. Let $\Phi^+ \subset \Phi$ be a system of positive roots, and let $\chi \in \Phi^+$. The **root homomorphism** $\chi_\alpha : \mathbb{G}_a \to G$ is

$$\chi_\alpha(b) = \varphi_\alpha\left(\begin{pmatrix} 1 & b \\ & 1\end{pmatrix}\right)$$

where recall that $\mathbb{G}_a(F) = (F, +)$.

Example 14.0.11 (Root homomorphisms (14.0.10))**.** $\chi_{e_i - e_j}(b) = I + bE_{ij}$ with 1 in the (i, j)-entry and zeroes everywhere else.

Remark 14.0.12. The notes say $\chi_{e_i - e - j}(b) = I + E_{ij}$ but I believe the former, written above, is more in line with the example above.

If we take $-(e_i - e_j) = e_j - e_i$ we instead get

$$\chi_{-\alpha}(b) = \varphi_\alpha\left(\begin{pmatrix} 1 & \\ b & 1\end{pmatrix}\right)$$

Lemma

Lemma 14.0.13. *Let* $\Phi^\vee = \{\alpha^\vee \mid \alpha \in \Phi\}$ *be the set of coroots of* T *in* G. *Then*

$$(\mathbb{Q}\Phi, \Phi^\vee)$$

is also a root system.

Remark 14.0.14. $\mathbb{Q}\Phi^\vee = \operatorname{span}_{\mathbb{Q}}\Phi^\vee$ in $X_*(T) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proposition 14.0.15. $(X^*(T), \Phi; X_*(T), \Phi^\vee)$ *is a root datum, called the root datum* $\mathsf{RD}(G,T)$ *of* (G,T).

Definition

Definition 14.0.16 (Isogeny)**.** Given $(X_i^*, \Phi_i, X_*^i, \Phi_i^\vee)$ for $i = 1, 2$, an **isogeny** is a group homomorphism $f : X_2^* \to X_1^*$ such that

- f is injective.
- $\operatorname{im}(f)$ has finite index in X_1^*.
- $f|_{\Phi_2}$ is a bijection onto Φ_1.

Remark 14.0.17. We have a morphism (I suppose the "transpose" of f) ${}^t f : X_*^1 \to X_*^2$ that restricts to a bijection $\Phi_1^\vee \xrightarrow{\sim} \Phi_2^\vee$.

Definition

Definition 14.0.18 (Central isogeny)**.** A homomorphism of algebraic groups $\psi : G \to H$ is a **central isogeny** if

1. ψ is surjective.
2. $\ker \psi$ is finite.
3. $\ker \psi \subset Z(G)$, i.e. the kernel of ψ is a subset of the center of G.

Theorem

Theorem 14.0.19 (Uniqueness and existence of isogeny of connected reductive groups)**.** *Uniqueness: If $\psi : G \to H$ is an isogeny of connected reductive groups G, H, $T_G \subset G$ is a maximal torus and $T_H \subset H$ is a maximal torus of H contained in $\psi(T_G)$, then we have an associated isogeny of root data*

$$\overline{\psi} : \mathsf{RD}(H, T_H) \to \mathsf{RD}(G, T_G)$$

given by

$$(\psi|_{T_G})^* : X^*(T_H) \xrightarrow{\overline{\psi}} X^*(T_G)$$

with associated transpose

$${}^t\overline{\psi} : X_*(T_G) \to X_*(T_H).$$

$\psi : G \xrightarrow{\sim} H$ is an isomorphism of algebraic groups $\Leftrightarrow$ $\overline{\psi}$ is an isomorphism of root data. More generally, if $\psi_i : G \to H$ is an isogeny for $i = 1, 2$ with equal *induced isogenies $\overline{\psi}_1 = \overline{\psi}_2$ of root data, then there exists $t \in T_G$ such that $\psi_2 = \psi_1 \circ \mathsf{Int}(t)$, i.e. such that*

$$\psi_2(g) = \psi_1(tgt^{-1}).$$

Existence: Given an isogeny $f : (X_2^*, \Phi_2, X_*^2, \Phi_2^\vee) \to (X_1^*, \Phi_1, X_*^1, \Phi_1^\vee)$ there exists connected reductive groups G, H with maximal tori $T_G \subset G, T_H \subset H$ and isogeny $\psi : G \to H$ such that $\psi(T_G) \subset T_H$ and $\overline{\psi} = f$.

Moral: We understand connected reductive groups up to isomorphism and isogenies between them in terms of root data.

Open Problem: How to understand arbitrary morphisms between connected reductive groups in terms of root data or generalizations?

There exists an isogeny called the canonical isogeny. This can be defined entirely in terms of root data for all $(X^*, \Phi, X_*, \Phi^\vee)$ (don't need to talk about groups, briefly (?)).

By existence, it gives an isogeny of groups (if we have an isgeny of root data). Let me tell you what it is! Given (G, T), there exists

$$\varphi_{\text{can}} : G^{\text{der}} \times R(G) \overset{\text{isogeny}}{\twoheadrightarrow} G$$

where $\ker \varphi_{\text{can}} \simeq Z(G^{\text{der}})$. Note here that $R(G)$ is the radical of G (9.0.5) which we claim is torus if G is reductive and where G^{der} is a commutative, semisimple subgroup of G.

Example 14.0.20. $G = \mathsf{GL}(n)$. We claim that $G^{\text{der}} = \mathsf{SL}(n)$ and that

$$\begin{aligned} R(G) &= Z(\mathsf{GL}(n)) \\ &= \mathbb{G}_m \\ &= \mathsf{GL}(1) \end{aligned}$$

i.e. the set of non-zero scalars. By the previous reasoning we then get an isogeny $\varphi_{\text{can}} : \mathsf{SL}(n) \times \mathsf{GL}(1) \to \mathsf{GL}(n)$, explicitly defined by

$$\mathsf{SL}(n) \times \mathsf{GL}(1) \ni (A, \lambda) \xmapsto{\varphi_{\text{can}}} A\lambda$$

and furthermore that

$$\ker \varphi_{\text{can}} = \{(\zeta I, \zeta^{-1}) \mid \zeta \in \mu_n\}.$$

If G is semisimple and simply-connected then $G = G_1 \times \cdots \times G_d$ is a product of semisimple, simply connected groups.

So every connected reductive group G admits an isogeny

$$\tilde{G} \times R(G) \xrightarrow[\psi]{\text{isogeny}} G^{\text{der}} \times R(G) \xrightarrow{\varphi_{\text{can}}} G$$

where $\tilde{G}$ is a simply connected cover of G^{der} (so is the *universal cover*, up to isomorphism). We then claim that $\varphi_{\text{can}} \circ \psi$ is an isogeny such that $\tilde{G} \times R(G)$ is a product of simple, simply-connected groups ($= G_i$) times a torus ($= R(G)$).

G is generated by $\{\varphi_\alpha(\mathsf{SL}(2)) \mid \alpha \in \Phi\}$ and T. A reductive group is built by gluing a torus with copies of $\mathsf{SL}(2)$ and/or $\mathsf{PGL}(2)$. The root datum *gives the instruction how to glue.*

Let $\Phi^+ \subset \Phi$ be a system of positive roots. Then

$$\langle T, \chi_\alpha(\mathbb{G}_a) \mid \alpha \in \Phi^+ \rangle := B$$

is a Borel subgroup (12.0.1).

Example 14.0.21. Let $G = \mathsf{GL}(n)$ and $\Phi = \{e_i - e_j \mid i \neq j\}$, then $B = \mathsf{Triag}^-(n)$.

The conjugacy classes of parabolic subgroups (12.0.12) of G are in bijection with $\mathcal{P}(\Delta)$, where $\Delta \subset \Phi^+$ is the base of simple roots, and $\mathcal{P}(-)$ denotes the power-set.

Given $I \subset \Delta$, let

$$\mathcal{P}_I = \langle T, \chi_{-\alpha}(\mathbb{G}_m) \text{ such that } \alpha \in \Phi^+ \text{ and } \chi_\alpha(\mathbb{G}_m) \text{ such that } \alpha \in \mathbb{Z}I \cap \Phi \rangle.$$

Then $\mathcal{P}_I$ we claim is a parabolic subgroup of G and that every parabolic subgroup of G is conjugate to $\mathcal{P}_I$ for precisely one $I \subset \Delta$.

Definition

Definition 14.0.22 (Standard Levi subgroup of $\mathcal{P}_I$)**.** Let $\mathcal{L}_I = \langle T, \chi_\alpha(\mathbb{G}_m), \chi_{-\alpha}(\mathbb{G}_m) \mid \alpha \in \mathbb{Z}I \cap \Phi \rangle$. Then $\mathcal{L}_I$ is a connected reductive group called the **standard Levi subgroup of** $\mathcal{P}_I$.

We have that $\mathcal{P}_I = \mathcal{L}_I R_u(\mathcal{P}_I)$ where $R_u(\mathcal{P}_I)$ denotes the unipotent radical of $\mathcal{P}_I$ (8.0.24).

Furthermore, in connection with $\mathcal{L}_I$ (14.0.22) we have

$$\mathcal{W}(\mathcal{L}_I, T) = \langle s_\alpha \mid \alpha \in I \rangle$$

is a parabolic subgroup of $\mathcal{W}(G, T)$ in the sense of Coxeter groups (3.0.6).

$(G, T) \mapsto \mathsf{RD}(G, T)$. Choose $\Phi^+ \subset \Phi$ which gives us a base $\Delta \subset \Phi^+$ of simple roots $\rightsquigarrow$ Dynkin Diagram:

- Vertices Δ.
- α, β are connected by $\langle \alpha, \beta^\vee \rangle \langle \beta, \alpha^\vee \rangle$ edges.
- α, β are connected by an edge $\Leftrightarrow$ $\langle \alpha, \beta^\vee \neq 0 \Leftrightarrow \langle \beta, \alpha^\vee \rangle \neq 0$.

Remark 14.0.23. Advanced material: That two Dynkin Diagrams are isomorphic does not imply that groups are isomorphic.

Definition

Definition 14.0.24. Let $X^*_+(T) = \{\lambda \in X^*(T) \mid \langle \lambda, \alpha^\vee \rangle \geqslant 0, \forall \alpha \in \Delta\}$ is the set of **dominant characters** relative choice of $\Phi^+ \subset \Phi$.

We claim that $\langle \lambda, \alpha^\vee \rangle \geqslant 0$ for all $\alpha \in \Delta \Leftrightarrow \langle \lambda, \alpha^\vee \rangle \geqslant 0$ for all $\alpha \in \Phi^+$ and that this is a straightforward application of the fact that we can write every element of Φ^+ as a non-negative $\mathbb{Z}$-linear combination of the base Δ together with the bilinearity of $\langle -, - \rangle$ (also recall that $\alpha^\vee = \frac{2\alpha}{(\alpha,\alpha)}$), and also assuming that $(\alpha, \alpha) > 0$ (2.0.1).

Example 14.0.25. Take $G = \mathsf{GL}(n)$ and $\Phi^+ = \{e_i - e_j \mid i < j\}$ with $\Delta = \{e_1 - e_2, \ldots, e_{n-1} - e_n\}$ and let $\lambda = (a_1, \ldots, a_n)$. Then

$$\begin{aligned} \langle \lambda, e_i - e_{i+1} \rangle &= a_i - a_{i+1} \geq 0 \\ &\Leftrightarrow a_i \geq a_{i+1}. \end{aligned}$$

We then claim that $X^*_+(T) = \{a \in \mathbb{Z}^n \mid a_1 \geqslant \ldots \geqslant a_n\}$.

Remark 14.0.26. I believe the idea is that $T = \mathrm{Diag}(n)$, and we are using that $X^*(T) \cong \mathbb{Z}^n$. Furthermore, since the base is $\Delta = \{e_1 - e_2, \ldots, e_{n-1} - e_n\}$ we see from the above that $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n$ since this must hold *for all* $\alpha^\vee \in \Delta$. Also note that

$$\begin{aligned} (e_i - e_j)^\vee &= \frac{2(e_i - e_j)}{(e_i - e_j, e_i - e_j)} \\ &= \frac{2(e_i - e_j)}{2} \\ &= e_i - e_j \end{aligned}$$

so it is enough to look at $e_i - e_{i+1} \in \Delta$ for $i = 1, \ldots, n-1$.

Theorem

Theorem 14.0.27. *There exists a* 1-1 *correspondence between isomorphism classes of irreducible representations* (2.0.14) *ofa connected reductive group G and $X^*_+(T)$.*
For all $\lambda \in X^*_+(T)$ there exists an irreducible representation $L(\lambda)$ of G of highest weight λ, meaning that $L(\lambda)|_T$ admits λ as a weight with multiplicity 1*, i.e.* $\dim L(\lambda)|_\lambda = 1$*. Furthermore, for all weights μ of $L(\lambda)$, i.e. $L(\lambda)_\mu \neq 0$, we have that $\lambda - \mu$ is a nonnegative $\mathbb{Z}$-linear combination of simple roots, i.e.*

$$\lambda - \mu = \sum_{\alpha \in \Delta} m_\alpha(\mu)\alpha, \qquad m_\alpha(\mu) \geqslant 0, \forall \alpha \in \Delta.$$

In characteristic 0,

$$\dim L(\lambda) = \prod_{\alpha \in \Phi^+} \frac{\langle \lambda + \rho, \alpha^\vee \rangle}{\langle \rho, \alpha^\vee \rangle}, \qquad \rho = \frac{1}{2} \sum_{\alpha \in \Phi^+} \alpha,$$

called the **Weyl dimension formula**.

In characteristic p, $\dim L(\lambda)$ is a mystery!

The Weyl group $\mathcal{W}$ acts on the set of weights of $L(\lambda)$. In characteristic 0, $L(\lambda)$ is minuscule (?) $\Leftrightarrow \mathcal{W}$ acts transitively. [In general, $L(\lambda)$ is determined by $L(\lambda)|_T$].

$X^*_+(T)$ *classifies* irreducible representations of G. We look at $G(F)$ for F an interesting field, e.g. $\mathbb{R}$ or $\mathbb{C} \rightsquigarrow$ interesting ∞-dimensional representations of $G(\mathbb{C})$ or $G(\mathbb{R})$, again classified by roots, but more complicated.

Look at $G(\mathbb{A})$ where $\mathbb{A}$ is a subring of $\mathbb{R}\times\prod_p \mathbb{Q}_p$, with classification not known $\rightsquigarrow$ Langlands programme.

Appendix A

Yonedas lemma & representable functors

To prove our next proposition, we need a lemma.

Lemma A.0.1. *Assume that $\alpha : F \Rightarrow G$ and $\beta : G \Rightarrow H$ are natural transformations between parallel functors $F, G, H : \mathcal{C} \rightrightarrows \mathcal{D}$. Then there is a natural transformation $\beta \circ \alpha : F \Rightarrow H$ so that*

$$(\beta \circ \alpha)_A := \beta_A \circ \alpha_A$$

.

Proof. For $f : A \to B$, we contemplate the following rectangle

$$\begin{tikzcd}
F(A) \arrow[r, "\alpha_A"] \arrow[d, "F(f)"] & G(A) \arrow[r, "\beta_A"] \arrow[d, "G(f)"] & H(A) \arrow[d, "H(f)"] \\
F(B) \arrow[r, "\alpha_B"] & G(B) \arrow[r, "\beta_B"] & H(B)
\end{tikzcd}$$

Let $x \in F(A)$. Then we have that

$$\begin{aligned}
(H(f) \circ \beta_A \circ \alpha_A)(x) &= (\beta_B \circ G(f) \circ \alpha_A)(x) \\
&= (\beta_B \circ \alpha_B \circ F(f))(x)
\end{aligned}$$

so that the larger square commutes, for an arbitrary morphism $f \in \mathrm{Mor}(\mathcal{C})$. $\square$

Lemma A.0.2. *Let $F : \mathcal{C} \to \mathbf{Set}$ be a any (covariant) functor from a* locally small *category $\mathcal{C}$, and let X be an object of $\mathcal{C}$. Then there is a bijection*

$$\mathbf{Nat}(\mathrm{Hom}_{\mathcal{C}}(X, -), F) \cong F(X).$$

Furthermore, natural transformations $\alpha : \mathrm{Hom}_{\mathcal{C}}(X, -) \to F$ correspond to $\alpha_X(1_X) \in F(X)$, and this correspondence is natural *in X and F.*

Proof. We start by proving the bijective property.

Bijection: Let $\phi : \mathrm{Hom}(\mathrm{Hom}_{\mathcal{C}}(A, -), F) \to F(A)$, where $\mathrm{Hom}(\mathrm{Hom}_{\mathcal{C}}(A, -), F)$ is the class of (*natural transformations*) from $\mathrm{Hom}_{\mathcal{C}}(A, -)$ to F.

ϕ is defined explicitly by taking a natural transformation $\alpha : \mathrm{Hom}(A, -) \Rightarrow F$ to $\alpha_A(1_A) \in F(A)$, i.e.

$$\alpha \xmapsto{\phi} \alpha_A(1_A).$$

This map is clearly right unique and left total, hence a function.

We want to find an inverse function $\Psi : F(A) \to \mathrm{Hom}(\mathrm{Hom}_{\mathcal{C}}(A, -), F)$ such that for $x \in F(A)$, we get a natural transformation $\Psi(x) : \mathrm{Hom}(\mathrm{Hom}_{\mathcal{C}}(A, -)) \to F$.

It follows that we must define components $\Psi(x)_B : \mathrm{Hom}(\mathrm{Hom}(A, B)) \to F(B)$, so that for $f : A \to B \in \mathrm{Mor}(\mathcal{C})$, we get

$$\begin{tikzcd}
\mathrm{Hom}(A, A) \arrow[r, "\Psi(x)_A"] \arrow[d, "\mathrm{Hom}(A,f)=f_*"] & F(A) \arrow[d, "F(f)"] \\
\mathrm{Hom}(A, B) \arrow[r, "\Psi(x)_B"] & F(B)
\end{tikzcd}$$

We find that $1_A \in \mathrm{Hom}(A, A)$ get's taken to $(\Psi(x)_B)(f)$ by going downward left and then right, while 1_A get's taken to $F(f) \circ (\Psi(x)_A)(1_A)$ via the right-downward route.

We see that we need to define $\Psi(x)_A(1_A) = x$, since we want

$$\begin{aligned} \Phi(\Psi(x)) &= \Psi(x)_A(1_A) \\ &= x. \end{aligned}$$

It follows, since we need naturality, that

$$F(f)(x) = \Psi(x)_B(f) \tag{A.0.1}$$

We conclude by showing that for a generic morphism $g : B \to D \in \mathrm{Mor}(\mathcal{C})$, $\Psi(x)$ is a natural transformation. I.e. showing that the following diagram commutes

$$\begin{tikzcd}
\mathrm{Hom}(A, B) \arrow[r, "\Psi(x)_B"] \arrow[d, "\mathrm{Hom}(A,g)=g_*"] & F(B) \arrow[d, "F(g)"] \\
\mathrm{Hom}(A, D) \arrow[r, "\Psi(x)_D"] & F(D)
\end{tikzcd}$$

For that, let $f \in \mathrm{Hom}(A, B)$. Then along the right-downward path we get that f gets taken to

$$\begin{aligned}(F(g) \circ \Psi(x)_B)(f) &= F(g) \circ \Psi(x)_B(f) \\ &= F(g)(F(f)(x)).\end{aligned}$$

On the downward-right path, f gets taken to

$$\begin{aligned}(\Psi(x)_D \circ g)(f) &= \Psi(x)_D(gf) \\ &= F(gf)(x)\end{aligned}$$

using A.0.1

Since F is a functor, we have $F(gf) = F(g) \circ F(f)$, so that the paths gives the same element in $F(D)$, i.e. the diagram commutes, for arbitrary morphism $g \in \mathrm{Hom}(B, D)$, where $B, D \in \mathcal{C}$ are arbitrary.

We have already seen that Ψ is a right-inverse to ϕ, and we want to show that Ψ is a left-inverse to ϕ; that is, that

$$\begin{aligned}\Psi\phi(\alpha) &= \Psi\alpha_A(1_A) \\ &= \alpha\end{aligned}$$

for a natural transformation $\alpha : \mathrm{Hom}(A, -) \Rightarrow F$. From (A.0.1) (with $x = \alpha_A(1_A) \in F(A)$) have that

$$\Psi(\alpha_A(1_A))_B(f) = Ff(\alpha_A(1_A)) \tag{A.0.2}$$

Since α is a natural transformation, the square to the right below commutes (with respect to any morphism $f : A \to B$)

$$\begin{tikzcd} A \arrow[d, "f"] & \mathrm{Hom}(A,A) \arrow[r, "\alpha_A"] \arrow[d, "\mathrm{Hom}(A,f)=f_*"] & F(A) \arrow[d, "F(f)"] \\ B & \mathrm{Hom}(A,B) \arrow[r, "\alpha_B"] & F(B) \end{tikzcd} \tag{A.0.3}$$

from which it follows that

$$\begin{aligned}F(f)(\alpha_A(1_A)) &= \alpha_B(f)(1_A) \\ &= \alpha_B(f)\end{aligned}$$

so that $\Psi(\alpha_A(1_A))_B(f) = \alpha_B(f)$ by (A.0.2).

This concludes the proof of the bijection $\mathrm{Hom}(\mathrm{Hom}_{\mathcal{C}}(A, -), F) \cong F(A)$.

We prove *naturality*.

Naturality: The assertion about naturality in X and F corresponds to the following claims:

1. Naturality in F means that, given a natural transformation $\beta : F \to G$, the element of $G(A)$ representing the composite natural transformation $\beta\alpha : \mathrm{Hom}(A, -) \to F \to G$ is the image under $\beta_A : F(A) \to G(A)$ of the element of $F(A)$ representing $\alpha : \mathrm{Hom}(A, -) \to F$, that is, the following diagram commutes

$$\begin{tikzcd}
\mathrm{Hom}(\mathrm{Hom}(A,-),F) \arrow[r, "\phi_F", "\cong"'] \arrow[d, "\beta_*"] & F(A) \arrow[d, "\beta_A"] \\
\mathrm{Hom}(\mathrm{Hom}(A,-),G) \arrow[r, "\phi_G", "\cong"'] & G(A)
\end{tikzcd}$$

where we have $\phi_F : \mathrm{Hom}(A,-) \to F(A)$ and $\phi_G : \mathrm{Hom}(A,-) \to G(A)$ defined explicitly by

$$\phi_F(\alpha) = \alpha_A(1_A)$$

$$\phi_G(\beta \circ \alpha) = (\beta \circ \alpha)_A(1_A).$$

To show that $\beta_A(\phi_F(\alpha)) = \phi_G(\beta \circ \alpha)$ for $\alpha \in \mathrm{Hom}(\mathrm{Hom}(A,-),F)$, we will use

We note that we have parallel functors $\mathrm{Hom}(A,-), F, G : \mathcal{C} \rightrightarrows \mathbf{Set}$, and natural transformations $\alpha : \mathrm{Hom}(A,-) \to F$ and $\beta : F \to G$. This gives us that $(\beta \circ \alpha)_A(1_A) := (\beta_A \circ \alpha_A)(1_A)$ by A.0.1.

That is, we have

$$\begin{aligned}
\phi_G(\beta \circ \alpha) &= (\beta \circ \alpha)_A(1_A) \\
&= (\beta_A \circ \alpha_A)(1_A) \\
&= \beta_A(\phi_F(\alpha))
\end{aligned}$$

where the last equality follows from $\phi_F(\alpha) := \alpha_A(1_A)$ and associativity of morphisms.

2. "Naturality in X" amounts to the assertion that given $f : A \to B \in \mathrm{Mor}(\mathcal{C})$, the element of $F(B)$ representing the composite natural transformation $\alpha f^* : \mathrm{Hom}(B,-) \Rightarrow \mathrm{Hom}(A,-) \Rightarrow F$ is the image under $F(f) : F(A) \to F(B)$ of the element of $F(A)$ representing α, i.e. the following diagram commutes

$$\begin{tikzcd}
\mathrm{Hom}(\mathrm{Hom}(A,-),F) \arrow[r, "\phi_A", "\cong"'] \arrow[d, "(f^*)^*"] & F(A) \arrow[d, "F(f)"] \\
\mathrm{Hom}(\mathrm{Hom}(B,-),F) \arrow[r, "\phi_B", "\cong"'] & F(B)
\end{tikzcd} \tag{A.0.4}$$

We see that the image of α along the right-downward path is $F(f)\phi_A(\alpha) = F(f)(\alpha_A(1_A))$ and that the image of α along the downward-right path is

$$\begin{aligned}
\phi_B((f^*)^* \circ \alpha) &= \phi_B(\alpha \circ f^*) \\
&= (\alpha \circ f^*)_B(1_B).
\end{aligned}$$

We use the following lemma

Lemma A.0.3. *Let $\mathcal{C}$ be a category, and let $f : A \to B \in \mathrm{Mor}(\mathcal{C})$. Then the pullback $f^* : \mathrm{Hom}(B, -) \Rightarrow \mathrm{Hom}(A, -)$ is a natural transformation.*

Proof. We contemplate the following diagram

$$\begin{tikzcd} X \arrow[d, "g"] & \mathrm{Hom}(B,X) \arrow[r, "f_X^*"] \arrow[d, "\mathrm{Hom}(B,g)=g_*"] & \mathrm{Hom}(A,X) \arrow[d, "\mathrm{Hom}(A,g)=g_*"] \\ Y & \mathrm{Hom}(B,Y) \arrow[r, "f_Y^*"] & \mathrm{Hom}(A,Y) \end{tikzcd} \tag{A.0.5}$$

We want to show that for arbitrary $h \in \mathrm{Hom}(B, X)$ we have that $(g_* \circ f_X^*)(h) = (f_Y^* \circ g_*)(h)$. This should be clear by definition. □

It follows that αf^* as assumed, is a composition of natural transformations. We have parallel functors $\mathrm{Hom}(A, -), \mathrm{Hom}(B, -), F : \mathcal{C} \to \mathbf{Set}$, and natural transformations $f^* : \mathrm{Hom}(B, -) \to \mathrm{Hom}(A, -)$ and $\alpha : \mathrm{Hom}(A, -) \to F$. By A.0.1, we have that

$$\begin{aligned} (\alpha f^*)_B(1_B) &= (\alpha_B \circ f_B^*)(1_B) \\ &= \alpha_B(f). \end{aligned}$$

From diagram (A.0.3) we then see that $\alpha_B(f) = F(f)(\alpha_A(1_A))$. It follows that

$$\begin{aligned} F(f)\phi_A(\alpha) &= F(f)(\alpha_A(1_A)) \\ &= \alpha_B(f) \\ &= (\alpha f^*)_B(1_B) \\ &= \phi_B((f^*)^* \circ \alpha) \end{aligned}$$

so that diagram (A.0.4) commutes.

□

There is also a *contravariant* version of yonedas lemma, which we will not prove.

Lemma A.0.4. *Let $F : \mathcal{C} \to \mathbf{Set}$ be any (contravariant) functor from a* locally small category *$\mathcal{C}$, and let X be an object of $\mathcal{C}$. Then there is a bijection*

$$\mathbf{Nat}(\mathrm{Hom}_{\mathcal{C}}(-, X), F) \cong F(X).$$

Furthermore, natural transformations $\alpha : \mathrm{Hom}_{\mathcal{C}}(-, X) \Rightarrow F$ correspond to $\alpha_X(1_X) \in F(X)$, and this correspondence is natural *in X and F.* □

Definition

Definition A.0.5. We say that a *covariant* functor F is **corepresentable** if there is some object $c \in \mathcal{C}$ such that there is a natural isomorphism $\alpha : \mathrm{Hom}_{\mathcal{C}}(c, -) \Rightarrow F$. A specific choice of α, c for F gives us a **corepresentation** (c, α).

Definition

Definition A.0.6. If F is a *contravariant* functor, and there is some object $c \in \mathcal{C}$ such that there is a natural isomorphism $\alpha : \mathrm{Hom}(-, c) \Rightarrow F$, then we say that F is **representable**, and we call a pair (c, α) a **representation**.

Appendix B

Schemes

Let F be a ring, and let $\mathbf{Alg}_F$ be the *category* of F-algebras. Think of this as that we have a functor from **Fields** to **Set** defined by taking $F \mapsto$ a set of solutions to a set of equations over F.

Definition

Definition B.0.1. A functor category $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$ is a category where the *objects* are *functors* $F : \mathcal{C} \to \mathcal{D}$ and the *morphisms* are *natural transformations* $\alpha : F \Rightarrow G$ between functors $F, G : \mathcal{C} \rightrightarrows \mathcal{D}$. We can also denote this category as $\mathcal{D}^{\mathcal{C}}$ (cf. representing the set of all functions $f : A \to B$ as B^A).

Definition

Definition B.0.2. Contravariantly, we have that a functor $h : \mathbf{Alg}_F \to \mathbf{Set}$ is called an **Affine Scheme**, if it is *representable* (A.0.6) by some object $R \in \mathbf{Alg}_F$. We denote by $\mathbf{AffSch}_F$ = category of affine schemes over F. This is a subcategory of the *functor category* (B.0.1) $\mathrm{Fun}(\mathbf{Alg}_F, \mathbf{Set})$.

Example B.0.3. For any $S \in \mathbf{Alg}_F$ we have

$$\begin{aligned} h_{F[x]}(S) &= \mathrm{Hom}_F(F[x], S) \\ &\cong S, \end{aligned}$$

with isomorphism given by taking $\varphi : F[x] \to S$ to $\varphi(x) \in S$, i.e. so by the evaluation $\mathrm{ev}_x : \mathrm{Hom}_F(F[x], S) \to S$.

Theorem B.0.4. *The category* $\mathbf{AffSch}_F$ *is canonically isomorphic to* opposite *category of* $\mathbf{Alg}_F$.

Example B.0.5. Let $R = F[x_1, \ldots, x_n]$, i.e. the polynomial ring in n variables over F. Then we have

$$\begin{aligned} \mathbf{Alg}_F \ni S \mapsto h_R(S) &= \mathrm{Hom}(F[x_1, \ldots, x_n], S) \\ &\cong S^n, \end{aligned}$$

I believe this can be seen by taking $\mathrm{ev}_{x_1,\ldots,x_n} : \mathrm{Hom}(F[x_1, \ldots, x_n], S) \to S^n$ defined by $\mathrm{Hom}(F[x_1, \ldots, x_n], S) \ni \varphi \xmapsto{\mathrm{ev}_{x_1,\ldots,x_n}} (\varphi(x_1), \ldots, \varphi(x_n)) \in S^n$.

Example B.0.6. $R = F[x_1, \ldots, x_n]/(f_1, \ldots, f_k)$ for $f_i \in F[x_1, \ldots, x_n]$. Then

$$\begin{aligned} h_R(S) &= \operatorname{Hom}\left(F[x_1, \ldots, x_n]/(f_1, \ldots, f_k), S\right) \\ &= V(f_1, \ldots, f_k) \\ &= \{s \in S^n \mid f_1(s) = \ldots = f_k(s) = 0\}, \end{aligned}$$

i.e. the *vanishing locus* of $(f_1, \ldots, f_k)$.

We have that $h_{F[x]} = \mathbb{A}^1_F$, i.e. $\mathbb{A}^1_F$ seen as a functor is represented by $h_{F[x]}$.

B.0.1 Affine Group Schemes

Definition

Definition B.0.7. An **affine group scheme over** F, is a *functor* $h : \mathbf{Alg}_F \to \mathbf{Grp}$ such that

$$\mathbf{Alg}_F \xrightarrow{h} \mathbf{Grp} \xrightarrow{U} \mathbf{Set}$$

is an *affine scheme* (B.0.2), where U is the *forgetful functor* from the category of groups to **Set**.

Example B.0.8. $\mathbb{G}_a(R) = (R, +)$. We have

$$\begin{aligned} \mathbb{G}_{a,F} &\cong h_{F[x]} \\ &\cong \mathbb{A}^1_F. \end{aligned}$$

See also [7].

Example B.0.9. $\mathbb{G}_m(R) = (R^\times, \times)$. We have that

$$\begin{aligned} \mathbb{G}_{m,F} &= h_{F[x,y]}/(xy - 1) \\ &= h_{F[x,x^{-1}]} \end{aligned}$$

,

where $h_{F[x,y]/(xy-1)} = \operatorname{Hom}\left(F[x,y]/(xy-1), S\right)$ are morphisms φ sending $x \overset{\varphi}{\longmapsto} s$ and $y \overset{\varphi}{\longmapsto} t$ such that $st = 1$.

Example B.0.10. Let $\mu_{n,m} = \mathbb{A}^{m,n}_F$. Then $\mathsf{GL}_n \subset \mu_{n,n}$. We have that

$$\mathsf{GL}_n(R) = \{A \in M_{n,n}(R) \mid \det(A) \in R^\times\}.$$

$M_{n,n}$ is *represented* by $F[x_{11}, x_{12}, \ldots, x_{nn}]$. GL_n is represented by $F[x_{11}, x_{12}, \ldots, x_{nn}]/(t \cdot \det((x_{ij})) - 1)$, where (x_{ij}) is the matrix

$$(x_{ij}) = \begin{pmatrix} x_{11} & \ldots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \ldots & x_{nn} \end{pmatrix}.$$

B.0.2 Algebraic groups and general schemes

Definition

Definition B.0.11. An **algebraic group** over a ring F, is an *affine group scheme over F* (B.0.7) h_R such that R is finitely generated over F.

Definition

Definition B.0.12. A **general scheme over a ring** F is a functor $h : \mathbf{Alg}_F \to \mathbf{Set}$ that is "covered by affine schemes". For more details, see Jantzen ([4]).

B.0.3 $\mathbb{P}^n_F$

Definition

Definition B.0.13. If $\Bbbk$ is a field extension of F ($\Bbbk \supset F$ and $\Bbbk$ field), then we define

$$\begin{aligned}\mathbb{P}^n_F(\Bbbk) &= \{\text{lines } \mathcal{L} \text{ through origin } \subset \Bbbk^{n+1}\}\\ &= \{\{tv, t \in \Bbbk\} \mid v \in \Bbbk^{n+1} \setminus \{0\}\}/(\{v = \lambda v \mid \lambda \in \Bbbk^\times\})\\ &= \{[x_0, \ldots, x_n] \in \Bbbk^{n+1} \setminus \{0\}\}/([x_0, \ldots, x_n] \sim \lambda[x_0, \ldots, x_n]).\end{aligned}$$

Example B.0.14. $\mathbb{P}^1(\mathbb{C}) = \{[x_0, x_1] \mid \mathbb{C}^2 \setminus \{0\}\}/([x_0, x_1] \sim \lambda[x_0, x_1])$. There is an isomorphism from $\mathbb{P}^1(\mathbb{C})$ to the *one-point compactification* $\mathbb{C}^* = \mathbb{C} \cup \{\infty\}$ given by

$$[x_0, x_1] \mapsto \begin{cases} \frac{x_0}{x_1}, & \text{if } x_1 \neq 0 \\ \infty, & \text{if } x_1 = 0. \end{cases}$$

Bibliography

[1] David S. Dummit and Richard M. Foote. *Abstract algebra*. 3rd ed. New York: Wiley, 2004.

[2] Joe Harris. *Algebraic Geometry: A First Course*. Vol. 133. Graduate Texts in Mathematics. New York: Springer, 1992. ISBN: 978-0-387-97716-4. DOI: 10.1007/978-1-4757-2189-8. URL: https://doi.org/10.1007/978-1-4757-2189-8.

[3] Robin Hartshorne. *Algebraic Geometry*. Vol. 52. Graduate Texts in Mathematics. New York: Springer, 1977. ISBN: 978-0-387-90244-9. DOI: 10.1007/978-1-4757-3849-0. URL: https://doi.org/10.1007/978-1-4757-3849-0.

[4] Jens Carsten Jantzen. *Representations of Algebraic Groups I*. Preprint Series 9. Bonn, 1985. URL: https://archive.mpim-bonn.mpg.de/id/eprint/607/1/preprint_1985_9.pdf.

[5] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd. Vol. 106. Graduate Texts in Mathematics. New York: Springer, 2009. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6. URL: https://doi.org/10.1007/978-0-387-09494-6.

[6] T. A. Springer. *Linear Algebraic Groups*. 2nd. Modern Birkhäuser Classics. Boston: Springer, 1998. ISBN: 978-0-8176-4021-2. DOI: 10.1007/978-0-8176-4840-9. URL: https://doi.org/10.1007/978-0-8176-4840-9.

[7] The Stacks project authors. *The Stacks project, Additive Group Scheme*. https://stacks.math.columbia.edu/tag/022V. 2024.

[8] Eric Wofsey. *Commutator subgroup of connected group*. URL: https://math.stackexchange.com/q/4508616.