Linear Algebraic Groups

Fall 2015

These are notes for the graduate course Math 6690 (Linear Algebraic Groups) taught by Dr. Mahdi Asgari at the Oklahoma State University in Fall 2015. The notes are taken by Pan Yan (pyan@math.okstate.edu), who is responsible for any mistakes. If you notice any mistakes or have any comments, please let me know.

Contents

1 Root Systems (08/19)

Root Systems

Reference for this part is *Lie Groups and Lie Algebras, Chapters 4-6* by N. Bourbaki.

Let V be a finite dimensional vector space over $\mathbb{R}$. An endomorphism $s : V \to V$ is called a *reflection* if there exists $0 \neq a \in V$ such that $s(a) = -a$ and s fixes pointwise a hyperplane (i.e., a subspace of codimension 1) in V. Then

$$V = \ker(s-1) \oplus \ker(s+1)$$

and $s^2 = 1$. We denote $V_s^+ = \ker(s-1)$ which is a hyperplane in V, and $V_s^- = \ker(s+1)$ which is just $\mathbb{R}a$.

Let $D = \mathrm{im}(1-s)$, then $\dim(D) = 1$. This implies that given $0 \neq a \in D$, there exists a nonzero linear form $a^* : V \to \mathbb{R}$ such that

$$x - s(x) = \langle x, a^* \rangle a, \forall x \in V$$

where $\langle x, a^* \rangle = a^*(x)$. Conversely, given some $0 \neq a \in V$ and a linear form $a^* \neq 0$ on V, set

$$s_{a,a^*}(x) = x - \langle x, a^* \rangle a, \forall x \in V$$

this gives an endomorphism of V such that $1 - s_{a,a^*}$ is of rank 1. Note that

$$\begin{aligned} s_{a,a^*}^2(x) &= s_{a,a^*}(x - \langle x, a^* \rangle a) \\ &= x - \langle x, a^* \rangle a - \langle x - \langle x, a^* \rangle a, a^* \rangle a \\ &= x - 2\langle x, a^* \rangle a + \langle x, a^* \rangle \langle a, a^* \rangle a \\ &= x + (\langle a, a^* \rangle a - 2)\langle x, a^* \rangle a. \end{aligned}$$

So s_{a,a^*} is a reflection if and only if $\langle a, a^* \rangle = 2$, i.e., $s_{a,a^*}(a) = -a$.

WARNING: $\langle x, a^* \rangle$ is only linear in the first variable, but not the second.

Remark 1.1. *(i) When V is equipped with a scalar product (i.e., a non-degenerate symmetric bilinear form B), then we can consider the so called orthogonal reflections, i.e., the following equivalent conditions hold:*

$$V_s^+ \text{ and } V_s^- \text{ are perpendicular w.r.t. } B \Leftrightarrow B \text{ is invariant under } s.$$

In that case,

$$s(x) = x - \frac{2B(x,a)}{B(a,a)}a.$$

(ii) A reflection s determines the hyperplane uniquely, but not the choice of the nonzero a (but it does in a root system, which we will talk about later).

Definition 1.2. Let V be a finite dimensional vector space over $\mathbb{R}$, and let R be a subset of V. Then R is called a *root system* in V if
(i) R is finite, $0 \notin R$, and R spans V;
(ii) For any $\alpha \in R$, there is an $\alpha^\vee \in V^*$ where $V^* = \{f : V \to \mathbb{R} \text{ linear}\}$ is the dual of V;
(iii) For any $\alpha \in R$, $\alpha^\vee(R) \subset \mathbb{Z}$.

Lemma 1.3. *Let V be a vector space over $\mathbb{R}$ and let R be a finite subset of V generating V. For any $\alpha \in R$ such that $\alpha \neq 0$, there exists at most one reflection s of V such that $s(\alpha) = -\alpha$ and $s(R) = R$.*

Proof. Suppose there are two reflections s, s' such that $s(\alpha) = s'(\alpha) = -\alpha$ and $s(R) = s'(R) = R$. Then $s(x) = x - f(x)\alpha$, $s'(x) = x - g(x)\alpha$ for some linear functions $f(x), g(x)$. Since $s(\alpha) = s'(\alpha) = -\alpha$, we have $f(\alpha) = g(\alpha) = 2$. Then

$$\begin{aligned} s(s'(x)) &= x - g(x)\alpha - f\left(x - g(x)\alpha\right)\alpha \\ &= x - g(x)\alpha - f(x)\alpha + f(\alpha)g(x)\alpha \\ &= x - g(x)\alpha - f(x)\alpha + 2g(x)\alpha \\ &= x - (g(x) - f(x))\alpha \end{aligned}$$

is a linear function, and $s(s'(R)) = R$. Since R is finite, $s \circ s'$ is of finite order, i.e., $(s \circ s')^n = (s \circ s') \circ (s \circ s') \circ \cdots \circ (s \circ s')$ is identity for some $n \geq 1$. Moreover,

$$\begin{aligned} (s \circ s')^2(x) &= x - (g(x) - f(x))\alpha - (g(x - (g(x) - f(x))\alpha) - f(x - (g(x) - f(x))\alpha))\,\alpha \\ &= x - 2(g(x) - f(x))\alpha \end{aligned}$$

and by applying the composition repeatedly, we have

$$(s \circ s')^n(x) = x - n(g(x) - f(x))\alpha.$$

But $(s \circ s')^n(x) = x$ for all $x \in V$, therefore, $g(x) = f(x)$. Hence $s(x) = s'(x)$. □

Lemma 1.3 shows that given $\alpha \in R$, there is a unique reflection s of V such that $s(\alpha) = -\alpha$ and $s(R) = R$. That implies α determines $s_{\alpha,\alpha^\vee}$ and $\alpha^\vee$ uniquely, and hence (iii) in the definition makes sense.

We can write $s_{\alpha,\alpha^\vee} = s_\alpha$. Then

$$s_\alpha(x) = x - \left\langle x, \alpha^\vee \right\rangle \alpha, \forall x \in V.$$

The elements of R are called *roots* (of this system). The *rank* of the root system is the dimension of V. We define

$$A(R) = \text{ finite group of automorphisms of } V \text{ leaving } R \text{ stable}$$

and the *Weyl group* of the root system R to be

$$W = W(R) = \text{ the subgroup of } A(R) \text{ generated by the } s_\alpha, \alpha \in R.$$

Remark 1.4. *Let R be a root system in V. Let $(x|y)$ be a symmetric bilinear form on V, non-degenerate and invariant under $W(R)$. We can use this form to identify V with V^*. Now if $\alpha \in R$, then α is non-isotropic (i.e., $(\alpha|\alpha) \neq 0$) and*

$$\alpha^\vee = \frac{2\alpha}{(\alpha|\alpha)}.$$

This is because we saw that $(x|y)$ invariant under s_α implies

$$s_\alpha(x) = x - \frac{2(x|\alpha)}{(\alpha|\alpha)}\alpha.$$

Proposition 1.5. *$R^\vee = \{\alpha^\vee : \alpha \in R\}$ is a root system in V^* and $\alpha^{\vee\vee} = \alpha$, $\forall \alpha \in R$.*

Proof. (Sketch). For (i) in Definition 1.2, $R^\vee$ is finite and does not contain 0. To see that $R^\vee$ spans V^*, we need to use the canonical bilinear form on $V \times V^*$ to identify

$$V_{\mathbb{Q}} = \mathbb{Q} - \text{vector space of } V \text{ generated by the } \alpha$$

and

$$V^*_{\mathbb{Q}} = \mathbb{Q} - \text{vector space of } V^* \text{ generated by the } \alpha^\vee$$

with the dual of the other. This way, the $\alpha^\vee$ generate V^*.

For (ii) in Definition 1.2, $s_{\alpha,\alpha^\vee}$ is an automorphism of V equipped with the root system R and ${}^t(s_{\alpha,\alpha^\vee})^{-1}$ leaved $R^\vee$ stable, but one can check that ${}^t(s_{\alpha,\alpha^\vee})^{-1} = s_{\alpha,\alpha^\vee}$ and $\alpha^{\vee\vee} = \alpha$.

For (iii) in Definition 1.2, note that $\langle \beta, \alpha^\vee \rangle \in \mathbb{Z}\ \forall \beta \in R, \forall \alpha^\vee \in R^\vee$, so $R^\vee$ satisfies (iii). □

Remark 1.6. *$R^\vee$ is called the dual root system of R. The map $\alpha \mapsto \alpha^\vee$ is a bijection from R to $R^\vee$ and is called the canonical bijection from R to $R^\vee$.*

WARNING: If $\alpha, \beta \in R$ and $\alpha + \beta \in R$, then $(\alpha + \beta)^\vee \neq \alpha^\vee + \beta^\vee$ in general.

Remark 1.7. *(i) The facts $s_\alpha(\alpha) = -\alpha$ and $s_\alpha(R) \subset R$ imply $R = -R$.*

(ii) It is also clear that $(-\alpha)^\vee = -\alpha^\vee$. $-1 \in A(R)$, but -1 is not always an element of $W(R)$.

(iii) The equality ${}^t(s_{\alpha,\alpha^\vee})^{-1} = s_{\alpha^\vee,\alpha}$ implies the map $u \mapsto {}^t u^{-1}$ is an isomorphism from $W(R)$ to $W(R^\vee)$, so we can identify these two via this isomorphism, and simply consider $W(R)$ as acting on both V and V^*. It is similar for $A(R)$.

First Examples

Now we give a few examples of root systems.

Example 1.8. (A_1): $V = \mathbb{R}e$. The root system is

$$R = \{\alpha = e, -e\}.$$

The reflection is $s_\alpha(x) = -x$. $V_s^+ = 0$, $V_s^- = V$. $A(R) = W(R) = \mathbb{Z}/2\mathbb{Z}$. The usual scalar product $(x|y) = xy$ is $W(R)$-invariant. The dual space is $V^* = \mathbb{R}e^*$ where $e^* : V \to \mathbb{R}$ such that $e^*(e) = 1$. Then $\alpha^\vee = 2e^*$ and $\langle \alpha, \alpha^\vee \rangle = (2e^*)(e) = 2$. $R^\vee = \{\alpha^\vee = 2e^*, -2e^*\}$ is a root system in V^*, which is the dual root system of R. Observe that if we identify V and V^* via $e \leftrightarrow e^*$, then $\alpha^\vee = \frac{2\alpha}{(\alpha|\alpha)}$. See Figure 1.

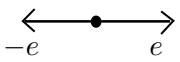


Figure 1: Root system for A_1, Example 1.8

Example 1.9. (A_1-non-reduced): $V = \mathbb{R}e$. The root system is

$$R = \{e, 2e, -e, -2e\}.$$

The dual space is $R^* = \mathbb{R}e^*$, and the dual root system is $R^\vee = \{\pm e^*, \pm 2e^*\}$. $E^\vee = 2e^*, (2e)^\vee = e^*$. See Figure 2

Remark 1.10. *Example 1.8 and Example 1.9 are the only dimension 1 root systems for* $V = \mathbb{R}$.

Example 1.11. ($A_1 \times A_1$): $V = \mathbb{R}^2 = \mathbb{R}e_1 \oplus \mathbb{R}e_2$. The root system is

$$R = \{\alpha = e_1, -\alpha, \beta = e_2, -\beta\}.$$

The dual space is $V^* = \mathbb{R}e_1^* \oplus \mathbb{R}e_2^*$. We have $\alpha^\vee = 2e_1^*$, $\beta^\vee = 2e_2^*$. The dual root system is $R^\vee = \{\pm 2e_1^*, \pm 2e_2^*\}$. This root system will be called reducible. See Figure 3.

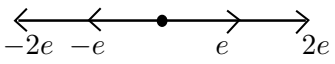


Figure 2: Root system for A_1-non-reduced, Example 1.9

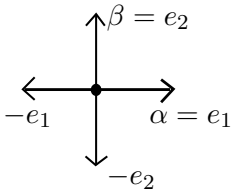


Figure 3: Root system for $A_1 \times A_1$, Example 1.11

Example 1.12. (A_2): $E = \mathbb{R}^3$, $V = \{(x_1, x_2, x_3) \in E : x_1 + x_2 + x_3 = 0\}$. The root system is

$$R = \{\pm(e_1 - e_2), \pm(e_1 - e_3), \pm(e_2 - e_3)\}.$$

Moreover,

$$W(R) = S_3 = \{\text{permutations on } e_1, e_2, e_3\},$$

$$A(R) = S_3 \times \{1, -1\}$$

where -1 maps e_i to $-e_i$. See Figure 4.

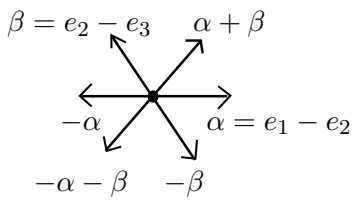


Figure 4: Root system for A_2, Example 1.12

Example 1.13. (B_2): $V = \mathbb{R}^2 = \mathbb{R}e_1 \oplus \mathbb{R}e_2$. The root system is

$$R = \{\pm e_1, \pm e_2, \pm e_1 \pm e_2\}.$$

Moreover,

$$A(R) = W(R) = (\mathbb{Z}/2\mathbb{Z})^2 \rtimes S_2.$$

See Figure 5.

Example 1.14. (C_2) – the dual of (B_2): The root system is

$$R = \{\pm 2e_1, \pm 2e_2, \pm e_1 \pm e_2\}$$

And

$$A(R) = W(R) = (\mathbb{Z}/2\mathbb{Z})^2 \rtimes S_2.$$

See Figure 6.

Example 1.15. (BC_2) – this is non-reduced (also the unique irreducible non-reduced root system of rank 2): $V = \mathbb{R}^2$. The root system is

$$R = \{\pm e_1, \pm e_2, \pm 2e_1, \pm 2e_2, \pm e_1 \pm e_2\}$$

and

$$A(R) = W(R) = (\mathbb{Z}/2\mathbb{Z})^2 \rtimes S_2.$$

See Figure 7.

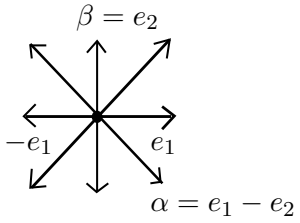


Figure 5: Root system for B_2, Example 1.13

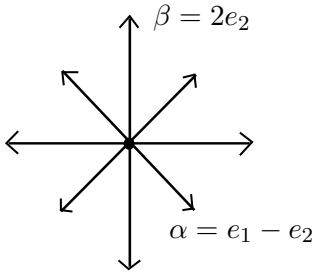


Figure 6: Root system for C_2, Example 1.14

Example 1.16. (G_2): $E = \mathbb{R}^3$, $V = \{(x_1, x_2, x_3) \in E : x_1 + x_2 + x_3 = 0\}$. The root system is

$$R = \{\pm(e_1 - e_2), \pm(e_1 - e_3), \pm(e_2 - e_3), \pm(2e_1 - e_2 - e_3), \pm(2e_2 - e_1 - e_3), \pm(2e_3 - e_1 - e_2)\}$$

and

$$A(R) = W(R) = \text{dihedral group of order 12.}$$

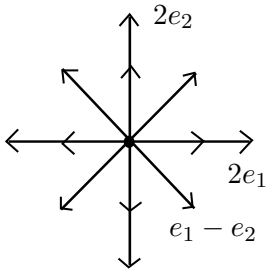


Figure 7: Non-reduced root system for BC_2, Example 1.15

See Figure 8.

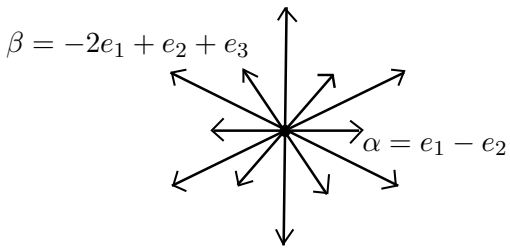


Figure 8: Root system for G_2, Example 1.16

Remark 1.17. *The above eight examples comprise of all rank 1 and rank 2 root systems (up to isomorphism). The rank 1 root systems are A_1, and non-reduced A_1. The rank 2 root systems are $A_1 \times A_1$, A_2, $B_2 \cong C_2$, G_2, BC_2.*

Irreducible Root Systems

Let V be the direct sum of $V_i, 1 \le i \le r$. Identify V^* with the direct sum of V_i^*, and for each i, let R_i be a root system in V_i. Then $R = \coprod_i R_i$ is a root system in V whose dual system is $R^\vee = \coprod_i R_i^\vee$. The canonical bijection $R \leftrightarrow R^\vee$ extends each canonical bijection $R_i \leftrightarrow R_i^\vee$ for each i. We say R is the *direct sum* of root systems R_i.

Let $\alpha \in R_i$. If $j \neq i$, then $\ker(\alpha^\vee) \supset V_j$. So s_α induces identity on $V_j, j \neq i$. On the other hand, $\mathbb{R}\alpha \subset V_i$, so s_α leaves V_i stable. Then $W(R)$ can be identified with $W(R_1) \times \cdots \times W(R_r)$.

Definition 1.18. A root system R is *irreducible* if $R \neq \emptyset$ and R is not the direct sum of two nonempty root systems.

It is easy to check that every root system R in V is the direct sum of a family of $(R_i)_{i\in I}$ of irreducible root systems. The direct sum is unique up to permutation of the index set I. The R_i are called *irreducible components* of R.

Definition 1.19. A root system R is *reduced* if $\alpha \in R$ implies $\frac{1}{2}\alpha \notin R$. α is called *indivisible root*.

Here is the complete list of irreducible, reduced root systems (up to isomorphism).

$$
\begin{aligned}
(I)\quad (A_l), l \ge 1 :& E = \mathbb{R}^{l+1}, V = \{(\alpha_1, \cdots, \alpha_{l+1}) : \sum_{i=1}^{l+1} \alpha_i = 0\},\\
& R = \{\pm(e_i - e_j) : 1 \le i < j \le l+1\}, \#R = l(l+1),\\
& W(R) = S_{l+1}, \quad A(R) = \begin{cases} W(R), \text{ if } l = 1,\\ W(R) \times \mathbb{Z}/2\mathbb{Z}, \text{ if } l \ge 2. \end{cases}\\
(II)\quad (B_l), l \ge 2 :& E = V = \mathbb{R}^l,\\
& R = \{\pm e_i, 1 \le i \le l; \pm e_i \pm e_j, 1 \le i < j \le l\}, \#R = 2l^2,\\
& A(R) = W(R) = (\mathbb{Z}/2\mathbb{Z})^l \rtimes S_l.\\
(III)\quad (C_l), l \ge 2 :& E = V = \mathbb{R}^l,\\
& R = \{\pm 2e_i, 1 \le i \le l; \pm e_i \pm e_j, 1 \le i < j \le l\}, \#R = 2l^2,\\
& A(R) = W(R) = (\mathbb{Z}/2\mathbb{Z})^l \rtimes S_l.\\
(IV)\quad (D_l), l \ge 3 :& E = V = \mathbb{R}^l,\\
& R = \{\pm e_i \pm e_j, 1 \le i < j \le l\}, \#R = 2l(l-1),\\
& W(R) = (\mathbb{Z}/2\mathbb{Z})^{l-1} \rtimes S_l,\\
& A(R)/W(R) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, \text{ if } l \neq 4,\\ S_3, \text{ if } l = 4, \end{cases}
\end{aligned}
$$

(V) Exceptional root systems: E_6, E_7, E_8, F_4, G_2.

Remark 1.20. *The above list will classify split, connected, semisimple linear algebraic groups over an algebraically closed field (up to isogeny).*

Angles between Roots

Let $\alpha, \beta \in R$. Put $\langle \alpha, \beta^\vee \rangle = n(\alpha, \beta)$. Then we have

$$\begin{aligned} &n(\alpha, \alpha) = 2, \\ &n(-\alpha, \beta) = n(\alpha, -\beta) = -n(\alpha, \beta), \\ &n(\alpha, \beta) \in \mathbb{Z}, \\ &s_\beta(\alpha) = \alpha - n(\alpha, \beta)\beta, \\ &n(\alpha, \beta) = n(\beta^\vee, \alpha^\vee). \end{aligned}$$

Let $(x|y)$ be a symmetric bilinear form on V, non-degenerate, invariant under $W(R)$. Then

$$n(\alpha, \beta) = \frac{2(\alpha|\beta)}{(\beta|\beta)}.$$

So

$$\begin{aligned} & n(\alpha, \beta) = 0 \\ \Leftrightarrow\ & n(\beta, \alpha) = 0 \\ \Leftrightarrow\ & (\alpha, \beta) = 0 \\ \Leftrightarrow\ & s_\alpha \text{ and } s_\beta \text{ commute }, \end{aligned}$$

and

$$(\alpha|\beta) \neq 0 \Rightarrow \frac{n(\beta, \alpha)}{n(\alpha, \beta)} = \frac{(\beta|\beta)}{(\alpha|\alpha)}.$$

We can determine possible angles between α and β. Let $(x|y)$ be scalar product, $W(R)$-invariant and $\alpha, \beta \in R$. Then

$$n(\alpha, \beta)n(\beta, \alpha) = \frac{2(\alpha|\beta)}{(\beta|\beta)} \cdot \frac{2(\beta|\alpha)}{(\alpha|\alpha)} = 4\cos^2(\widehat{\alpha, \beta}) \leq 4.$$

We list all the possibilities in Table 1.

Corollary 1.21. *Let $\alpha, \beta \in R$. If $\alpha = c\beta$, then $c \in \{\pm 1, \pm 2, \pm \frac{1}{2}\}$.*

Corollary 1.22. *Let α, β be non-proportional roots. If $(\alpha|\beta) > 0$ (i.e., if the angle between α and β is strictly acute), then $\alpha - \beta$ is a root. If $(\alpha|\beta) < 0$, then $\alpha + \beta$ is a root.*

Proof. Without loss of generality we may assume $||\alpha|| \leq ||\beta||$. If $(\alpha|\beta) > 0$, then $s_\beta(\alpha) = \alpha - n(\alpha, \beta)\beta \in R$ must be $\alpha - \beta$ by Table 1 (case 1 is the only possibility). Similarly, if $(\alpha|\beta) < 0$, then $s_\beta(\alpha) = \alpha - n(\alpha, \beta)\beta \in R$ must be $\alpha + \beta$ (case 2 is the only possibility). $\square$

case		angle between α and β	order of $s_\alpha s_\beta$
1	$n(\alpha,\beta)=n(\beta,\alpha)=0$	$\pi/2$	2
2	$n(\alpha,\beta)=n(\beta,\alpha)=1$	$\pi/3$ and $\|\|\alpha\|\|=\|\|\beta\|\|$	3
3	$n(\alpha,\beta)=n(\beta,\alpha)=-1$	$2\pi/3$ and $\|\|\alpha\|\|=\|\|\beta\|\|$	3
4	$n(\alpha,\beta)=1, n(\beta,\alpha)=2$	$\pi/4$ and $\|\|\alpha\|\|=\sqrt{2}\|\|\beta\|\|$	4
5	$n(\alpha,\beta)=-1, n(\beta,\alpha)=-2$	$3\pi/4$ and $\|\|\alpha\|\|=\sqrt{2}\|\|\beta\|\|$	4
6	$n(\alpha,\beta)=1, n(\beta,\alpha)=3$	$\pi/6$ and $\|\|\alpha\|\|=\sqrt{3}\|\|\beta\|\|$	6
7	$n(\alpha,\beta)=-1, n(\beta,\alpha)=-3$	$5\pi/6$ and $\|\|\alpha\|\|=\sqrt{3}\|\|\beta\|\|$	6
8	$n(\alpha,\beta)=2, n(\beta,\alpha)=2$	$\alpha=\beta$	
9	$n(\alpha,\beta)=-2, n(\beta,\alpha)=-2$	$\alpha=-\beta$	
10	$n(\alpha,\beta)=1, n(\beta,\alpha)=4$	$\beta=2\alpha$	
11	$n(\alpha,\beta)=-1, n(\beta,\alpha)=-4$	$\beta=-2\alpha$	

Table 1: Possible Angels Between Two Roots

2 Review of Algebraic Geometry I (08/26)

The Zariski Topology

Let k be an algebraically closed field (of any characteristic, occasionally $\text{char}(k) \neq 2, 3$). Let $V = k^n$, $S = k[T] := k[T_1, T_2, \cdots, T_n]$. $f \in S$ can be thought of as a function $f : V \to k$, via evaluation. We say $v \in V$ is a *zero* of $f \in k[T]$ if $f(v) = 0$. We say $v \in V$ is a zero of an ideal I of S if $f(v) = 0, \forall f \in I$. Given an ideal I, write $\nu(I) =$ set of zeros of I. In the opposite direction, if $X \subset V$, define $\mathcal{I}(X) \subset S = k[T]$ to be the ideal consisting of polynomials $f \in S$ with $f(v) = 0$, $\forall v \in X$.

Example 2.1. Let $S = k[T] = [T_1]$, consider $I = (T^2)$, then $\nu(I) = \{0\}$ and $\mathcal{I}(\{0\}) = (T)$.

Definition 2.2. The *radical* or *nilradical* $\sqrt{I}$ of an ideal I is

$$\sqrt{I} = \{f \in S : f^m \in I \text{ for some } m \geq 1\}.$$

Theorem 2.3 (Hilbert's Nullstellensatz)**.** *(i) If I is a proper ideal in S, then $\nu(I) \neq \emptyset$. (ii) For any ideal I of S we have $\mathcal{I}(\nu(I)) = \sqrt{I}$.*

Definition 2.4. Observe that
(i) $\nu(\{0\}) = V$, $\nu(S) = \emptyset$;
(ii) $I \subset J \Rightarrow \nu(J) \subset \nu(I)$;
(iii) $\nu(I \cap J) = \nu(I) \cup \nu(J)$;
(iv) If $(I_\alpha)_{\alpha \in A}$ is a family of ideals and $I = \sum_{\alpha \in A} I_\alpha$, then $\nu(I) = \bigcap_{\alpha \in A} \nu(I_\alpha)$.

Note that (i), (ii), (iv) imply that there is a topology on $V = k^n$ whose closed sets are the $\nu(I)$ where I is an ideal in S – we call it the *Zariski topology*. A closed subset in the Zariski topology is called an *algebraic set*. Also, for any $X \subset V$, we have a Zariski subspace topology on X.

Proposition 2.5. *Let $X \subset V$ be an algebraic set.*

(i) The Zariski topology on X is T_1, i.e., points are closed.

(ii) The topology space X is noetherian, i.e., it satisfies the following two equivalent properties: any family of closed subsets of X contains a minimal one , or equivalently if $X_1 \supset X_2 \supset X_3 \supset \cdots$ is a decreasing sequence of closed subsets of X, then there exists some index h such that $X_i = X_h$ for $i \geq h$.

(iii) X is quasi-compact, i.e., any open covering of X has a finite subcover.

Note that in algebraic geometry, compact means quasi-compact and Hausdorff.

Review of Reducibility of Topological Spaces

Definition 2.6. A non-empty topological space X is called *reducible* if it is the union of two proper, closed subsets. Otherwise, it is called *irreducible*.

Remark 2.7. *If X is irreducible, then any two non-empty open subsets of X have a non-empty intersection.*

This is mostly interesting only in non-Hausdorff space. In fact, any irreducible Hausdorff space is simply a point.

If X, Y are two topological spaces. Then

$$A \subset X \text{ irreducible } \Leftrightarrow \overline{A} \text{ is irreducible,}$$

$$f : X \to Y \text{ continuous and } X \text{ irreducible } \Rightarrow f(X) \text{ is irreducible.}$$

If X is noetherian topological space, then X has finitely many maximal irreducible subsets, called the (irreducible) components of X. The components are closed and they cover X.

Now, we consider the Zariski topology on $V = k^n$.

Proposition 2.8. *A closed subset X of V is irreducible if and only if $\mathcal{I}(X)$ is prime.*

Proof. Let $f, g \in S$ with $fg \in \mathcal{I}(X)$. Then

$$X = (X \cap \nu(fS)) \cup (X \cap \nu(gS))$$

where both $X \cap \nu(fS)$ and $X \cap \nu(gS)$ are closed subsets of V. Since X is irreducible, $X \subset \nu(fS)$ or $X \subset \nu(gS)$. Hence $f \in \mathcal{I}(X)$ or $g \in \mathcal{I}(X)$. So $\mathcal{I}(X)$ is prime.

Conversely, assume $\mathcal{I}(X)$ is a prime ideal. If $X = \nu(I_1) \cup \nu(I_2) = \nu(I_1 \cap I_2)$ and $X \neq \nu(I_1)$, then there exists $f \in I_1$ such that $f \notin \mathcal{I}(X)$. But $fg \in \mathcal{I}(X)$ for all $g \in I_2$. By primeness, $g \in \mathcal{I}(X)$ implies $I_2 \subset \mathcal{I}(X)$. Hence $X = \nu(I_2)$. So X is irreducible. □

Recall that a topological space is *connected* if it is not the union of two disjoint proper closed subsets. So if a topological space is irreducible, then it must be connected (but the inverse direction is not true, see Example 2.9).

A noetherian topological space X is a disjoint union of finitely many connected closed subsets – its connected components. A connected component is a union of irreducible components. A closed subset X of $V = k^n$ is not connected if and only if there exists two ideals I_1, I_2 of S with $I_1 + I_2 = S$ and $I_1 \cap I_2 = \mathcal{I}(X)$.

Example 2.9. $X = \{(x, y) \in k^2 : xy = 0\}$ is closed in k^2 which is connected, but not irreducible.

Here is a dictionary between algebraic objects and geometric objects.

Algebra	Geometry
$k[T_1, \cdots, T_n]$	$V = k^n$
radical ideals	closed subsets
maximal ideals	points
prime ideals	irreducible closed subsets

Review of Affine Algebras

A k-algebra is a vector space A over k together with a bilinear operation $A \times A \to A$ such that for all $f, g, h \in A$ and scalars $c_1, c_2 \in k$, we have $(f+g)h = fh+gh$, $f(g+h) = fg+fh$, $(c_1 f)(c_2 g) = (c_1 c_2)fg$. A k-algebra homomorphism $F : A \to B$ is a ring homomorphism which is k-linear.

Let $X \subset V = k^n$ be an algebraic set. Define

$$k[X] := \{f|_X : f \in S = k[T]\}.$$

Then $k[X] \cong k[T]/\mathcal{I}(X)$ (this is an isomorphism of k-algebra). $k[X]$ is called an *affine k-algebra*, i.e., it has the following two properties: (i) $k[X]$ is an algebra of finite type, i.e., there exists a finite subset $\{f_1, \cdots, f_r\}$ of $k[X]$ such that $k[X] = k[f_1, \cdots, f_r]$; (ii) $k[X]$ is reduced, i.e., 0 is the only nilpotent element of $k[X]$.

An affine k-algebra A also determines an algebraic subset X of some k^r such that $A \cong k[X]$. If $A \cong k[T_1, \cdots, T_r]/I$ where $I = \ker(T_i \xrightarrow{1 \le i \le r} f_i)$, then

$$A \text{ is reduced } \Leftrightarrow I \text{ is a radical ideal.}$$

The affine k-algebra $k[X]$ determines both the algebraic set X and its Zariski topology. We have the following one-to-one correspondence

$$\begin{aligned} \{\text{points of } X\} &\leftrightarrow \operatorname{Max}(k[X]) = \{\text{maximal ideals of } S \text{ containing } \mathcal{I}(X)\} \\ x &\mapsto M_x = \mathcal{I}_X(\{x\}), \end{aligned}$$

where for $Y \subset X$, $\mathcal{I}_X(Y) = \{f \in k[X] : f(y) = 0, \forall y \in Y\}$. Note that $k[X]/M_x \cong k$, so M_x is a maximal ideal. It is easy to check that
(i) $x \mapsto M_x$ is a bijection;
(ii) $x \in \nu_X(I) \Leftrightarrow I \subset M_x$;
(iii) The closed sets of X are the $\nu_X(I)$, where I is an ideal in $k[X]$;
Hence the algebra $k[X]$ determines X and its Zariski topology.

For $f \in k[X]$, set

$$D_X(f) = D(f) := \{x \in X : f(x) \neq 0\}.$$

This is an open set of X and we call it a *principal open subset* of X. It is easy to check that the principal opens form a basis for the Zariski topology.

Review of Field of Definitions and F-structures

Definition 2.10. Let F be a subfield of k. We say F is a *field of definition* of the closed subset X of $V = k^n$ if the ideal $\mathcal{I}(X)$ is generated by polynomials with coefficients in F.

Set

$$F[X] := F[T]/(\mathcal{I}(X) \cap F[T]).$$

Then $F[T] \hookrightarrow k[T] = S$ induces an isomorphism of F-algebras

$$F[X] \cong (\text{an } F - \text{subalgebra of } S)$$

and an isomorphism of k-algebras

$$k \otimes_F F[X] \cong k[X]$$

($F[X]$ will be called an F-structure on X). However, this definition of field of definition and F-structure is not intrinsic.

Definition 2.11. Let $A = k[X]$ be an affine algebra. An *F-structure on X* is an F-subalgebra A_0 of A which is of finite type over F such that the homomorphism

$$k \otimes_F A_0 \to A = k[X]$$

induced by multiplication is an isomorphism. We then write $A_0 = F[X]$ and $X(F) := \{F - \text{homomorphism} : F[X] \to F\}$ which is called the *F-rational points* for the given F-structure.

Example 2.12. Let $k = \mathbb{C}$ and $F = \mathbb{R}$. Let $X = \{(z, w) \in \mathbb{C}^2 : z^2 + w^2 = 1\}$, $A = k[X] = \mathbb{C}[T, U]/(T^2 + U^2 - 1)$. Let $a = T \mod (T^2 + U^2 - 1)$, $b = U \mod (T^2 + U^2 - 1)$. Here are two $\mathbb{R}$-structure on X:

$$A_1 = \mathbb{R}[a, b],$$

$$A_2 = \mathbb{R}[ia, ib].$$

These are two different $\mathbb{R}$-structures. To see this, consider the $\mathbb{R}$-rational points for A_1 and A_2. The $\mathbb{R}$-rational points for A_1 is

$$X(\mathbb{R}) = \{\mathbb{R} - \text{homomorphism } \mathbb{R}[a, b] \to \mathbb{R}\} = S^1$$

while the $\mathbb{R}$-rational points for A_2 is

$$X(\mathbb{R}) = \{\mathbb{R} - \text{homomorphism } \mathbb{R}[ia, ib] \to \mathbb{R}\} = \emptyset.$$

3 Review of Algebraic Geometry II, Introduction to Linear Algebraic Groups I (09/02)

Review of Regular Functions

Let $x \in X \subset V = k^n$.

Definition 3.1. A function $f : U \to k$ with U a neighborhood of x in X is *regular* at x if

$$f(y) = \frac{g(y)}{h(y)}, \quad g, h \in k[X]$$

on a neighborhood $V \subset U \cap D(h)$ of x (i.e., $h \neq 0$ in V). As usual, we say f is regular in a non-empty, open subset U if it is regular at each $x \in U$. We define

$$\mathcal{O}_X(U) = \mathcal{O}(U) := \text{ the } k - \text{algebra of regular functions in } U.$$

Observe that if U, V are non-empty, open sets and $U \subset V$, then the restriction $\mathcal{O}(V) \to \mathcal{O}(U)$ is a k-algebra homomorphism.

Let $U = \bigcup_{\alpha \in A} U_\alpha$ be an open cover of the open set U. Assume that for each α, we have $f_\alpha \in \mathcal{O}(U_\alpha)$ such that if $U_\alpha \cap U_\beta \neq \emptyset$, then f_α and f_β restrict to the same function in $\mathcal{O}(U_\alpha \cap U_\beta)$. Then there exists $f \in \mathcal{O}(U)$ such that $f|_{U_\alpha} = f_\alpha$ for any $\alpha \in A$ (patching). $(X, \mathcal{O})$ is called a *ringed space* and $\mathcal{O}$ is called a *sheaf of k-valued functions* on X.

Definition 3.2. The ringed space $(X, \mathcal{O}_X)$ (or simply X) as above is called an *affine algebraic variety over k* or an *affine k-variety* or simply an *affine algebraic variety.*

Lemma 3.3. *Let $(X, \mathcal{O}_X)$ be an affine algebraic variety. Then the homomorphism*

$$\begin{aligned} \varphi : k[X] &\to \mathcal{O}(X) \\ f &\mapsto f/1 \end{aligned}$$

is an isomorphism of k-algebras.

If $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ are two ringed space or affine algebraic varieties, and $\phi : X \to Y$ is a continuous map, and f is a function on an open set $V \subset Y$, then define

$$\phi_V^*(f) := f \circ \phi|_{\phi^{-1}(V)},$$

a function on an open subset $\phi^{-1}(V) \subset X$.

Definition 3.4. ϕ is called a *morphism* of ringed space or of affine algebraic varieties if for each $V \subset Y$, ϕ_V^* maps $\mathcal{O}_Y(V)$ into $\mathcal{O}_X(\phi^{-1}V)$.

If $X \subset Y$, $\phi : X \hookrightarrow Y$ is injection and $\mathcal{O}_X = \mathcal{O}_Y|_X$, then $\phi : X \hookrightarrow Y$ is a morphism of ringed spaces. This is the notion of *ringed subspace*.

A morphism $\varphi : X \to Y$ of affine algebraic varieties induces an algebraic homomorphism $\mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$ by composition with φ. Then we get an algebraic homomorphism $\varphi^* : k[Y] \to k[X]$ by Lemma 3.3. Conversely, an algebraic homomorphism $\psi : k[Y] \to k[X]$ also gives a continuous map $(\psi) : X \to Y$ such that $(\psi)^* = \psi$. Hence there is an equivalence of categories

$$\Big\{\text{affine } k\text{-varieties and their morphisms}\Big\} \longleftrightarrow \{\text{affine } k\text{-algebras and their homomorphisms}\}$$

$$\text{affine } k\text{-variety } X \mapsto \text{affine } k\text{-algebra } k[X]$$

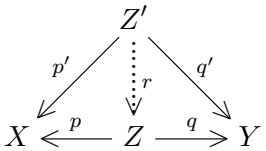
$$\text{morphism } \varphi : X \to Y \mapsto \varphi^* : k[Y] \to k[X] \text{ defined by } \varphi^*(f) = f \circ \varphi$$

Let F be a subfield of k. Similar remarks apply to affine F-varieties and F-subalgebras. Hence affine F-varieties can also be described algebraically. An example is that the affine n-space $\mathbf{A}^n$, $n \geq 0$ with algebra $k[T_1, T_2, \cdots, T_n]$.

Review on Products

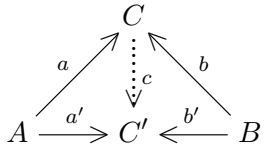
Given two affine algebraic varieties X and Y over k, we would like to define a product affine algebraic variety $X \times Y$.

Definition 3.5 (Universal Property of Product (in any category))**.** A product of X and Y is defined as an affine algebraic variety Z together with morphisms $p : Z \to X$, $q : Z \to Y$ such that the following holds: for any triaple (Z', p', q') as above, there exists a unique morphism $r : Z' \to Z$ such that the diagram



commutes.

Equivalently, we can do this in the category of affine k-algebras. Put $A = k[X]$, $B = k[Y]$, and $C = k[Z]$. Then using the equivalence of categories we can express the universal property algebraically: there exists k-algebra homomorphisms $a : A \to C$, $b : B \to C$ such that for any triple (C', a', b') of affine k-algebras, there is a unique k-algebra homomorphism $c : C \to C'$ such that the diagram



commutes.

Having this property just for the k-algebras (forgetting that C is an affine k-algebra) we already know from abstract algebra that $C = A \otimes_k B$ with

$$a(x) = x \otimes 1, x \in A,$$
$$b(y) = 1 \otimes y, y \in A,$$

satisfies all the requirements.

Lemma 3.6. *Let A, B be k-algebras of finite type.*
(i) If A, B are reduced, then $A \otimes_k B$ is reduced.
(ii) If A, B are integral domains, then $A \otimes_k B$ is an integral domain.

Therefore, for X, Y affine k-varieties, a product variety $X \times Y$ exists (as an affine k-variety). It is unique up to isomorphism. If X and Y are irreducible, then so is $X \times Y$. In fact, it is easy to see the set underlying $X \times Y$ can be identified with the product of the sets underlying X and Y. With this identification, the Zariski topology on $X \times Y$ is finer than the product topology. If F is a subfield of k, a product of two affine F-varieties exists and is unique up to F-isomorphism.

Prevarieties and Varieties

Definition 3.7. A *prevariety over k* is a quasi-compact ringed space $(X, \mathcal{O})$ such that any point of X has an open neighborhood U such that

$$(U, \mathcal{O}|_U) \cong \text{ an affine } k\text{-variety}$$

is an isomorphism in the category of affine k-algebras or affine k-varieties.

Definition 3.8. A *morphism* of prevarieties is a morphism of ringed spaces.

Definition 3.9. A *sub prevariety* of a prevariety is a ringed subspace which is also a prevariety.

A product of two prevarieties exists and is unique up to isomorphism. This allows us to consider the diagonal subset $\Delta_X = \{(x, x) : x \in X\}$ of $X \times X$ equipped with its reduced topology. Denote by

$$\begin{aligned} i : X &\to \Delta_X \\ x &\mapsto (x, x). \end{aligned}$$

Then $i : X \to \Delta_X$ is a homeomorphism of topological spaces for any prevariety X.

Definition 3.10. A prevariety X is called a *variety* or an *algebraic variety over k* or *k-variety* if it satisfies the Separation Axiom, i.e.,

$$\text{(Separation Axiom): } \Delta_X \text{ is closed in } X \times X.$$

Morphisms of varieties are now defined in the usual way.

Example 3.11. Let X be an affine k-variety. Then $\Delta_X = \nu_{X\times X}(I)$ where I is the kernel of the map defined from universal property

$$k[X \times X] = k[X] \otimes_k k[X] \to k[X].$$

In fact, I is generated by $f \otimes 1 - 1 \otimes f$, $f \in k[X]$. Hence X satisfies the Separation Axiom, i.e., it is a variety over k. Also note that

$$k[X \times X]/I \cong k[X],$$

which implies that i gives a homeomorphism of topological spaces $X \to \Delta_X$.

Lemma 3.12. *A topological space X is Hausdorff if and only if Δ_X is closed in $X \times X$ for the product topology.*

Lemma 3.13. *The product of two varieties is a variety.*

Lemma 3.14. *For X a variety, Y a prevariety, if $\varphi : Y \to X$ is a morphism of prevarieties, then its graph $\Gamma_\phi = \{(y, \phi(y)) : y \in Y\}$ is closed in $Y \times X$.*

Lemma 3.15. *Again, for X a variety, Y a prevariety, if two morphisms $\varphi : Y \to X$, $\psi : Y \to X$ coincide on a dense subset, then $\varphi = \psi$.*

Lemma 3.16 (Criterion for a prevariety to be a variety)**.** *(i) Let X be a variety, U, V be affine open sets in X. Then $U \cap V$ is an affine open set and the images under restriction of $\mathcal{O}_X(U)$ and $\mathcal{O}_X(V)$ in $\mathcal{O}_X(U \cap V)$ generate it.*

(ii) Let X be a prevariety and let $X = \cup_{i=1}^m U_i$ be a covering by affine open sets. Then X is a variety if and only if for each pair (i, j), the intersection $U_i \cap U_j$ is an affine open set and the images under restriction of $\mathcal{O}_X(U_i)$ and $\mathcal{O}_X(U_j)$ in $\mathcal{O}_X(U_i \cap U_j)$ generate it.

Remark 3.17. *There are more examples of varieties, for example, projective varieties, which are not affine.*

Definition of Linear Algebraic Groups

Now we introduce the notion of linear algebraic groups.

Definition 3.18. Let k be an algebraically closed field, and let F be a subfield. An *algebraic group* G is an algebraic variety over k which is also a group such that the maps

$$\begin{aligned} \mu : G \times G &\to G \\ (x, y) &\mapsto xy \end{aligned}$$

and

$$\begin{aligned} i : G &\to G \\ x &\mapsto x^{-1} \end{aligned}$$

are morphisms of varieties. An algebraic group G is called a *linear algebraic group* if it is affine as an algebraic variety.

Definition 3.19. Let G, G' be algebraic groups. A *homomorphism of algebraic groups* $\varphi : G \to G'$ is a group homomorphism and a morphism of varieties. (Hence we have the notion of isomorphism and automorphism of algebraic groups).

Note that $G \times G'$ is automatically an algebraic group – called the *direct product* of $G \times G'$.

A closed subgroup H of an algebraic group G (with respect to the Zariski topology) can be made into an algebraic group such that $H \hookrightarrow G$ is a homomorphism of algebraic groups.

Definition 3.20. The algebraic group G is called an *F-group* where $F \subset k$ is a subfield if
(i) G is an F-variety;
(ii) the morphisms μ and i are defined over F;
(iii) the identity element e is an F-rational point.

Similarly, we get F-homomorphisms. For G an F-group, set

$G(F) :=$ the set of F-rational points, which come with a canonical group structure.

Let G be a linear algebraic group. Put $A = k[G]$. Recall that there is an equivalence of categories

$$\Big\{\text{affine } k\text{-varieties and their morphisms}\Big\} \longleftrightarrow \{\text{affine } k\text{-algebras and their homomorphisms}\}.$$

So the morphisms μ and i can be described as algebraic homomorphisms. μ is defined by $\Delta : A \to A \otimes_k A$, called "multiplication". i can be defined by $\iota : A \to A$, called "amtipode". Moreover, the identity element e is a homomorphism $A \to k$. With this in hand, we can write the group axioms algebraically. We denote

$$\begin{aligned} m : A \otimes_k A &\to A \\ f \otimes g &\mapsto fg \end{aligned}$$

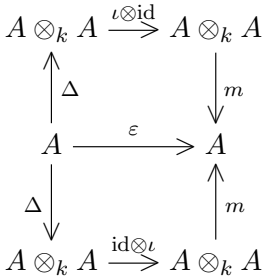
and

$$\varepsilon : \quad \begin{array}{ccc} A & \xrightarrow{\varepsilon} & A \\ & \searrow^{e} & \uparrow \\ & & k. \end{array}$$

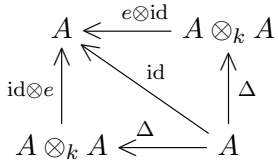
Then associativity in Group Axioms is the same as the diagram

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes_k A \\ \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle \mathrm{id}\otimes\Delta} \\ A \otimes_k A & \xrightarrow{\Delta\otimes_k \mathrm{id}} & A \otimes_k A \otimes_k A \end{array}$$

commutes. The existence of the inverse in Group Axioms is the same as the diagram



commutes. The existence of identity in Group Axioms is the same as the diagram



commutes.

4 Introduction to Linear Algebraic Groups II (09/09)

Examples of Algebraic Groups

We first give several examples of algebraic groups.

Recall that k is algebraically closed, and $F \subset k$ is a subfield.

Example 4.1. $G = k = \mathbf{A}^1$. Another notation is $\mathbf{G}_a$ – "the additive group". $A = k[G] = k[T]$. Multiplication and inversion are

$$\begin{aligned} \Delta : k[T] &\to k[T] \otimes_k k[T] \cong k[T, U] \\ T &\mapsto T + U \end{aligned}$$

and

$$\begin{aligned} \iota : k[T] &\to k[T] \\ T &\mapsto -T. \end{aligned}$$

Note that G is a variety because we have the separation axiom: $\Delta_G = \{(g, g) : g \in G\}$ is closed in $G \times G$. Therefore, Δ and ι are k-algebra homomorphism. This implies μ, i given by

$$\mu(x, y) = x + y, \quad i(x) = -x,$$

are morphisms of varieties. For any $F \subset k$, $F[T]$ defines an F-structure on $\mathbf{G}_a$:

$$\mathbf{G}_a(F) \cong F.$$

Example 4.2. $G = k^* = \mathbf{A}^1 \backslash \{0\}$. Other notation for this group is $\mathbf{G}_m$ – "the multiplicative group", or $\mathbf{GL}_1$. $A = k[G] = k[T, T^{-1}]$. Multiplication and inversion are

$$\begin{aligned} \Delta : k[T, T^{-1}] &\to k[T, T^{-1}] \otimes_k k[T, T^{-1}] \cong k[T, T^{-1}, U, U^{-1}] \\ T &\mapsto TU \end{aligned}$$

and

$$\begin{aligned} \iota : k[T, T^{-1}] &\to k[T, T^{-1}] \\ T &\mapsto T^{-1}. \end{aligned}$$

Also,

$$\begin{aligned} e : k[T, T^{-1}] &\to k \\ T &\mapsto 1 \end{aligned}$$

Again, $F[T, T^{-1}]$ defines an F-structure, $\mathbf{G}_m(F) \cong F^*$. Observe that for any $n \in \mathbb{Z} \backslash \{0\}$, $x \mapsto x^n$ defines a homomorphism of algebraic groups $\mathbf{G}_m \to \mathbf{G}_m$. When is this an isomorphism?

$\mathbf{G}_m \to \mathbf{G}_m$ is an isomorphism $\Leftrightarrow \phi^* : A = k[T, T^{-1}] \to A$ is an isomorphism.

Hence $\mathrm{Aut}(\mathbf{G}_m) \cong \{\pm 1\}$.

Example 4.3. $G = \mathbf{A}^n$, $n \geq 1$. μ and i are given by

$$\mu(x, y) = xy,\ i(x) = -x,$$

and $e = 0$. In particular, $G = \mathbf{M}_n = \{\text{all } n \times n \text{ matrices}\} \cong k^{n^2}$.

Example 4.4. $G = \mathbf{GL}_n = \{x \in \mathbf{M}_n : D(x) \neq 0\}$ where D is the determinant. Note that D is a regular function on M_n, and $\mathbf{GL}_n$ is the principal open set given by $D \neq 0$. μ and i are given by

$$\mu(x, y) = xy,\ i(x) = x^{-1},$$

and $e = I_n$. The k-algebra is $A = k[\mathbf{GL}_n] = k[T_{ij}, D^{-1}]_{1 \leq i,j \leq n, D = \det(T_{ij})}$ with homomorphisms

$$\begin{aligned} \Delta : A &\to A \otimes_k A \\ T_{ij} &\mapsto \sum_{h=1}^{n} T_{ih} T_{hj} \end{aligned}$$

$$\begin{aligned} \iota : A &\to A \\ T_{ij} &\mapsto (i,j) - \text{entry of the} \\ &\qquad \text{inverse of } [T_{kl}]_{1 \leq k,l \leq n}, \end{aligned}$$

and

$$\begin{aligned} e : A &\to k \\ T_{ij} &\mapsto \delta_{ij}. \end{aligned}$$

For any $F \subset k$, $F[T_{ij}, D^{-1}]$ defines an F-structure on $G = \mathbf{GL}_n$ and $G(F) = \mathrm{GL}_n(F)$. Note that any Zariski closed subgroup of GL_n defines a linear algebraic group.

Example 4.5. Any finite closed subgroup of $\mathbf{GL}_n$ is a linear algebraic group.

Example 4.6. $\mathbf{D}_n$, the diagonal matrices in $\mathbf{GL}_n$, is a linear algebraic group.

Example 4.7. $\mathbf{T}_n$, the upper triangulars in $\mathbf{GL}_n$, is a linear algebraic group.

Example 4.8. $\mathbf{U}_n$, the unipotent upper triangular matrices in $\mathbf{GL}_n$, is a linear algebraic group.

Example 4.9. $\mathbf{SL}_n = \{X \in \mathbf{GL}_n : \det(X) = 1\}$, the special linear group, is a linear algebraic group.

Example 4.10. $\mathbf{O}_n = \{X \in \mathbf{GL}_n : {}^tXX = 1\}$, the orthogonal group, is a linear algebraic group. Let

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

Then $\mathbf{O}_n = O_n(J) = \{X \in \mathbf{GL}_n : {}^tXJX = J\}$.

Example 4.11. $\mathbf{SO}_n = \mathbf{O}_n \cap \mathbf{SL}_n$, the special orthogonal group, is a linear algebraic group. Sometimes we distinguish the odd and the even indices as $\mathbf{SO}_{2n+1}$ and $\mathbf{SO}_{2n}$.

Example 4.12. The special orthogonal group, $\mathbf{Sp}_{2n} = \{X \in \mathbf{GL}_{2n} : {}^tXJX = J\}$ where

$$J = \begin{pmatrix} & & & & & & 1 \\ & & & & & \iddots & \\ & & & & 1 & & \\ & & & -1 & & & \\ & & \iddots & & & & \\ & -1 & & & & & \end{pmatrix}_{2n\times 2n} \quad \text{or } J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix},$$

is a linear algebraic group.

Review of Projective Varieties

Definition 4.13. The projective space $\mathbf{P}^n$ is the set $\{1-\text{dim subspace of } k^{n+1}\}$ or equivalently

$$k^{n+1}\backslash\{0\}/\sim$$

where

$$x \sim y \iff y = ax \text{ for some } a \in k^* = k\backslash\{0\}.$$

If $x = (x_0, x_1, \cdots, x_n) \in k^{n+1}\backslash\{0\}$, we write x^* or $[x_0 : x_1 : \cdots : x_n]$ for the equivalence class of x. The x_i's are called the *homogeneous coordinates* of x^*.

We cover the set $\mathbf{P}^n$ by $U_0, U_1, \cdots, U_n$ where

$$U_i := \{(x_0, x_1, \cdots, x_n)^* : x_i \neq 0\}.$$

Each U_i can be given an affine variety structure of $\mathbf{A}^n$ via

$$\begin{aligned} \varphi_i : U_i &\to \mathbf{A}^n \\ (x_0, x_1, \cdots, x_n)^* &\mapsto \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \cdots, \widehat{\frac{x_i}{x_i}}, \cdots, \frac{x_n}{x_i}\right). \end{aligned}$$

Then $\varphi_i(U_i \cap U_j)$ is a principal open $D(f)$ in $\mathbf{A}^n$ because we may take

$$f = \begin{cases} T_j, j > i \\ 1, j = i \\ T_{j+1}, j < i. \end{cases}$$

Declare a subset U of $\mathbf{P}^n$ open if $U \cap U_i$ is open in the affine variety U_i for any $i = 0, 1, \cdots, n$. For $x \in \mathbf{P}^n$, assume $x \in U_i$ for some i. Then a function f in a neighborhood of x is declared

regular at x if $f|_{U_i}$ is regular in the affine structure of U_i and we get a sheaf $\mathcal{O}_{\mathbf{P}^n}$ and a ringed space $(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n})$ that makes $\mathbf{P}^n$ into a prevariety.

In fact, $\mathbf{P}^n$ is a variety. We can check this by using the criterion we had before in Lemma 3.16.

Definition 4.14. A *projective variety* is a closed subvariety of some $\mathbf{P}^n$. A *quasi-projective variety* is an open subvariety of a projective variety.

Closed sets in $\mathbf{P}^n$ are of the form

$$\nu^*(I) = \{x^* \in \mathbf{P}^n : x \in \nu_{k^{n+1}}(I)\}$$

where I is a homogeneous ideal. Recall that a *homogeneous ideal* means an ideal $I \in S = k[T_0, T_1, \cdots, T_n]$ generated by homogeneous polynomials.

Example 4.15. We assume $\mathrm{char}(k) \neq 2, 3$. Define

$$G = \{(x_0, x_1, x_2)^* \in \mathbf{P}^2 : x_0 x_2^2 = x_1^3 + a x_1 x_0^2 + b x_0^3\}$$

where $a, b \in k$ such that the polynomial $T^3 + aT + b$ has no multiple roots. Let $e = (0, 0, 1)^*$ be the point at "∞". Define the sum of three corlinear points in $\mathbf{P}^2$ to be e. It is easy to check that if $x = (x_0, x_1, x_2)^* \in G$, then $-x = (x_0, x_1, -x_2)^*$. It is a bit of work to write addition explicitly. We can also check the associativity. Then G is an algebraic group, which is non-linear.

Review of Dimension

Let X be an irreducible variety. First, assume X to be affine. Since X is irreducible, $k[X]$ is an integral domain. Then we get its fraction field $k(X)$. It is an easy fact (by localization) that if U is any open affine subset of X, then

$$k(U) \cong k(X).$$

If X is any variety, then the above and the criterion for a prevariety to be a variety in Lemma 3.16 imply that if U, V are any two affine open sets, then $k(U)$, $k(V)$ can be canonically identified. Hence we can speak of the fraction field $k(X)$.

Definition 4.16. We define the *dimension* of an irreducible variety X to be

$$\dim X = \text{ transcendence degree of } k(X) \text{ over } k.$$

If X is reducible and $(X_i)_{1 \leq i \leq m}$ are its irreducible components, then

$$\dim X = \max_{1 \leq i \leq m} \dim X_i.$$

Lemma 4.17. *If X is affine and $k[X] = k[x_1, x_2, \cdots, x_r]$, then*

$\dim X =$ *maximal number of elements among $x_1, \cdots, x_r$ that are algebraically independent over k.*

Lemma 4.18. *If X is irreducible and Y is proper irreducible closed subvariety of X, then*

$$\dim Y < \dim X.$$

Lemma 4.19. *If X, Y are irreducible varieties, then*

$$\dim(X \times Y) = \dim X + \dim Y.$$

Lemma 4.20. *If $\varphi : X \to Y$ is a morphism of affine varieties and X is irreducible, then $\overline{\varphi(X)}$ is irreducible, and $\dim \overline{\varphi(X)} \leq \dim X$.*

Example 4.21. $\dim \mathbf{A}^n = n$, and $\dim \mathbf{P}^n = n$.

Remark 4.22. *If U is an open set in X, then $\dim U = \dim X$. If $\dim X = 0$, then X is finite. If $f \in k[T_1, \cdots, T_n]$ is irreducible, then $\nu(f)$ is $(n-1)$-dimensional irreducible subvariety of $\mathbf{A}^n$. Dimension respects field of definition. In other words, if X is an F-variety, then*

$$\dim X = \textit{transcendence degree of } F(X) \textit{ over } F.$$

Basic Results on Algebraic Groups

Let k be an algebraically closed field, G an algebraic group. For $g \in G$, the maps

$$\begin{aligned} L_g : G &\to G \\ x &\mapsto gx \end{aligned}$$

and

$$\begin{aligned} R_g : G &\to G \\ x &\mapsto xg \end{aligned}$$

define isomorphisms of the varieties G.

Proposition 4.23. *(i) There is a unique irreducible component G^0 of G that contains e. It is closed, normal subgroup of finite index.*

(ii) G^0 is the unique connected component of G containing e.

(iii) Any closed subgroup of G of finite index contains G^0.

Proof. (i) Let X, Y be two irreducible components of G containing e. Then $XY = \mu(X \times Y)$ is irreducible (because $X \times Y$ is irreducible, and μ is continuous), and its closure $\overline{XY}$ is irreducible, closed. But irreducible components are maximal irreducible closed subsets, so $X \subset \overline{XY} \subset X$, so $X = \overline{XY} = Y$. This implies X is closed under multiplication.

Now, i is a homeomorphism, hence X^{-1} is an irreducible component of G containing e. So $X^{-1} = X$, i.e., X is a closed subgroup. Now for $g \in G$, gXg^{-1} is an irreducible component containing e. This implies $gXg^{-1} = X$ for any $g \in G$. So X is a normal subgroup of G. So gX must be the irreducible components of G and there are finitely many of them. Hence $G^0 = X$ satisfies (i).

(ii) The cosets gG^0 are mutually disjoint, and each connected component is a union of them. So the irreducible and connected components of G must coincide. This proves (ii).

(iii) Let H be a closed subgroup of G of finite index, then H^0 is a closed subgroup of finite index in G^0. Now H^0 is both open and closed in G^0, but G^0 is connected, so $H^0 = G^0$. □

Convention: we talk about "connected algebraic groups" and not "irreducible algebraic groups".

We need the following two lemmas about morphisms of varieties.

Lemma 4.24. *If $\phi : X \to Y$ is a morphism of varieties, then $\phi(X)$ contains a nonempty open subset of its closure $\overline{\phi(X)}$.*

Lemma 4.25. *If X, Y are F-varieties, and ϕ is defined over F, then $\overline{\phi(X)}$ is an F-subvariety of Y.*

Proposition 4.26. *Let $\phi : G \to G'$ be a homomorphism of algebraic groups. Then*
(i) $\ker \phi$ *is a closed normal subgroup of G.*
(ii) $\phi(G)$ is a closed subgroup of G.
(iii) If G and G' are F-groups and ϕ is defined over F, then $\phi(G)$ is an F-subgroup of G'.
(iv) $\phi(G^0) = \phi(G)^0$.

We need the following two lemmas to prove it.

Lemma 4.27. *If U and V are dense open subgroups of G, then $G = UV$.*

Lemma 4.28. *If H is a subgroup of G, then*
(i) The closure $\overline{H}$ is also a subgroup of G.
(ii) If H contains a non-empty open subset of $\overline{H}$, then $H = \overline{H}$.

Proposition 4.29 (Chevalley)**.** *Let $(X_i, \phi_i)_{i \in I}$ be a family of irreducible varieties and morphisms $\phi_i : X_i \to G$. Denote by H the smallest closed subgroup of G containing $Y_i = \phi_i(X_i)$. Assume that all Y_i contain e. Then*
(i) H is connected.
(ii) $H = Y_{i_1}^{\pm 1} Y_{i_2}^{\pm 1} \cdots Y_{i_n}^{\pm 1}$ for some $n \geq 0, i_1, \cdots, i_n \in I$.
(iii) If G is an F-group, and for all $i \in I$, X_i is an F-variety, and ϕ_i is defined over F, then H is an F-subgroup of G.

Corollary 4.30. *(i) If H and K are closed subgroups of G, one of which is connected, then the commutator subgroup (H, K) is connected.*

(ii) If G is an F-group and H, K are F-subgroups, then (H, K) is a connected F-subgroup. In particular, (G, G) is a connected F-subgroup.

5 Introduction to Linear Algebraic Groups III (09/16)

G-spaces

Let k be an algebraically closed field, X an variety over k, G an algebraic group over k.

Definition 5.1. Let $a : G \times X \to X$ defined by $a(g, x) = g \cdot x$ be a morphism of varieties such that

$$g \cdot (h \cdot x) = (gh) \cdot x, \quad \forall g, h \in G,$$
$$e \cdot x = x.$$

Then X is called a *G-space* or *G-variety*.

Definition 5.2. Let $F \subset k$ be a subfield. If G is an F-group and X is an F-variety, and a is defined over F, then we say X is a *G-space over F*.

Definition 5.3. If F acts trivially on the G-space X, we say X is a *homogeneous space for G*. For $x \in X$, define the *orbit of X* to be

$$G \cdot x = \{g \cdot x : g \in G\}$$

and the *isotropy group of x* to be

$$G_x = \{g \in G : g \cdot x = x\}.$$

Lemma 5.4. *G_x is a closed subgroup of G.*

Proof. Fix $x \in X$.

$$G \to G \times X \to X$$
$$g \mapsto (g, x) \mapsto g \cdot x$$

is continuous and G_x is the inverse image of $\{x\}$, and $\{x\}$ is closed in the Zariski topology, so G_x is closed. □

Definition 5.5. Let X and Y be G-spaces. A morphism $\varphi : X \to Y$ is called a *G-morphism* or *G-equivalent* if

$$\varphi(g \cdot x) = g \cdot \varphi(x), \quad \forall g \in G, x \in X.$$

Lemma 5.6. *(i) An orbit $G \cdot x$ is open in $\overline{G \cdot x}$.*
(ii) There exists closed orbits.

Proof. (i) Fix $x \in X$ and consider the morphism $\varphi : G \to X$ given by $\varphi(g) = g \cdot x$. By a general fact from algebraic geometry, we know $\varphi(G) = G \cdot x$ contains a nonempty open subset U in its closure $\overline{\varphi(G)} = \overline{G \cdot x}$. Now $G \cdot x = \bigcup_{g \in G} g \cdot U$, so $G \cdot x$ is open in $\overline{G \cdot x}$.

(ii) Let $S_x = \overline{G \cdot x} - G \cdot x$, which is closed in X. It is a union of orbits. Consider the family $\{S_x\}_{x \in X}$ of closed subsets in X. It has a minimal subset S_{x_0}. By (i), S_{x_0} must be empty. Then $G \cdot x = \overline{G \cdot x}$ is closed. □

Corollary 5.7. *$G \cdot x$ is locally closed in X, i.e., an open subset of a closed set in X. It has an algebraic variety structure, and is automatically a homogeneous space for G.*

Examples of G-spaces

Example 5.8 (Inner automorphisms)**.** $X = G$, $a : G \times G \to G$ is defined by $a(g, x) = gxg^{-1}$. The orbits are conjugacy classes $G \cdot x = \{gxg^{-1} : g \in G\}$. The isotropy group is $G_x = C_G(x) = \{g \in G : gx = xg\}$.

Example 5.9 (Left and right actions)**.** $X = G$, $a : G \times G \to G$ is defined by $(g, x) \mapsto gx$ or $(g, x) \mapsto xg^{-1}$. G acts simply-transitively, i.e., $G_x = \{1\}$ $\forall x \in G$, and G is a homogeneous space. Then G is called a *principal homogeneous space*.

Example 5.10. Let V be a finite dimensional vector space over k of dimension n. A *rational representation* of G in V is a homomorphism of algebraic groups $r : G \to \mathrm{GL}(V)$. V is also called a G-module, via $g \cdot v = r(g)v$.

Remark 5.11. *Let $F \subset k$ be a subfield. View V as a finite dimensional vector space with an F-structure and view $GL(V)$ as an F-group and r is defined over F, then we call r a rational map over F.*

Example 5.12. With the same notation, any closed subgroup G of $\mathbf{GL}_n$ acts on $X = \mathbf{A}^n$ (left action) so $\mathbf{A}^n$ is a G-space. The orbits of X are $\{0\}$ and $\mathbf{A}^n \backslash \{0\}$. For example, for $G = \mathbf{SL}_n$, the orbit is $\{0\}$.

Now assume G is affine. X is an affine G-space with action $a : G \times X \to X$. We have $k[G \times X] = k[G] \otimes_k k[X]$ and a is given by $a^* : k[X] \to k[G] \otimes_k k[X]$. For $g \in G$, $x \in X$, $f \in k[X]$, define

$$s(g) : k[X] \to k[X]$$
$$(s(g)f)(x) = f(g^{-1}x).$$

Then $s(g)$ is an invertible linear map from (often infinite-dimensional) vector space $k[X]$ to itself. This way, we get a representation of abstract groups $s : G \to \mathrm{GL}(k[X])$.

Proposition 5.13. *Let V be a finite dimensional subspace of $k[X]$.*

(i) There is a finite dimensional subspace W of $k[X]$ containing V such that $s(g)W \subset W$, $\forall g \in G$.

(ii) V is stable under all $s(g)$ if and only if $a^*(V) \subset k[G] \otimes_k V$. In this case, we get a map $s_V : G \times V \to V$ which is a rational representation of G in V.

(iii) If G is an F-group, X is an F-variety, V is defined over F, and a is an F-morphism, then W in part (i) can be taken to be defined over F.

Proof. (i) Without loss of generality, we may assume that $V = kf$ is one dimensional. Write

$$a^*(f) = \sum_{i=1}^{n} u_i \otimes f_i, \quad u_i \in k[G], f_i \in k[X].$$

Then $(s(g)f)(x) = f(g^{-1}x) = \sum_{i=1}^{n} u_i(g^{-1})f_i(x)$. Now $W' = \langle f_i \rangle_{i=1,\cdots,n}$ is finite dimensional and let W be its subspace spanned by all $s(g)f$, $g \in G$. Then W satisfies (i).

(ii) ($\Leftarrow$) is just as in (i).

($\Rightarrow$) Assume V is $s(G)$-stable. Let (f_i) be a basis for V and extend it to a basis $(f_i) \cup (g_i)$ for $k[X]$. Take $f \in V$, and write

$$a^*(f) = \sum_i u_i \otimes f_i + \sum_j v_j \otimes g_j, \quad u_i, v_j \in k[G].$$

Now

$$s(g)f = \sum_i u_i(g^{-1})f_i + \sum_j v_j(g^{-1})g_j.$$

By assumption, $v_j(g^{-1}) = 0$ for all $g \in G$. Hence $v_j = 0$ for all j. So $a^*f \in k[G] \otimes_k V$.

(iii) In the argument for (i), check that if all data is defined over F, then so is W.

□

Observe that there exists an increasing sequence of finite dimensional subspaces (V_i) of $k[X]$ such that (i) each V_i is stable under $s(G)$ and s defines a rational map of G in V_i, and (ii) $k[X] = \bigcup_i V_i$.

Now we still assume that G is affine. Consider the left and right action of G on itself. For $g, x \in G$, $f \in k[G]$, define

$$(\lambda(g)f)(x) = f(g^{-1}x),$$

$$(\rho(g)f)(x) = f(xg).$$

They both define representations of abstract group G in $\mathrm{GL}(k[G])$. If $\iota : k[G] \to k[G]$ is the automorphism of $k[G]$ defined by inversion in G, then we have

$$\rho = \iota \circ \lambda \circ \iota^{-1}.$$

Lemma 5.14. *Both λ and ρ have trivial kernels, i.e., they are "faithful" representations.*

Proof. If $\lambda(g) = \mathrm{id}$, then $f(g^{-1}) = f(e)$ for all $f \in k[G]$. Hence $g^{-1} = e$. So $g = e$. This proves that $\ker \lambda$ is trivial. The proof for ρ is similar. □

Theorem 5.15. *Let G be a linear algebraic group.*

(i) There is an isomorphism of G onto a closed subgroup of some GL_n.

(ii) If G is an F-group, the isomorphism may be taken to be defined over F.

Proof. (i) By part (i) of Proposition 5.13, we may assume $k[G] = k[f_1, \cdots, f_n]$ where (f_i) is a basis of $\rho(G)$-stable subspace V of $k[G]$. By part (ii) of Proposition 5.13, we can write

$$\rho(g)f_i = \sum_{j=1}^{n} m_{ji}(g)f_j, \quad m_{ji} \in k[G], \forall g \in G, i, j = 1, \cdots, n.$$

Define

$$\begin{aligned}\phi : G &\to \mathrm{GL}_n \\ g &\mapsto (m_{ij}(g))_{n\times n}.\end{aligned}$$

Then ϕ is a group homomorphism and a morphism of affine varieties.

We claim that ϕ is injective. If $\phi(g) = e$, then $\rho(g)f_i = f_i$, $\forall i$. But $\rho(g)$ is an algebraic homomorphism and $k[G]$ is generated by the f_i, so

$$\rho(g)f = f, \quad \forall f \in k[G].$$

Hence $g = e$.

We claim that ϕ^* is surjective. Note that $\phi^* : k[\mathrm{GL}_n] = k[T_{ij}, D^{-1}] \to k[G]$ is given by

$$\phi^*(T_{ij}) = m_{ij},$$

$$\phi^*(D^{-1}) = \det(m_{ij})^{-1}.$$

But $f_i(g) = \sum_j m_{ji}(e)f_j(e)$, so each f_i is in $\mathrm{im}(\phi^*)$, hence ϕ^* is surjective. This implies that $\phi(G)$ is a closed subgroup of GL_n. Its algebra is isomorphic to $k[\mathrm{GL}_n]/\ker\phi^* \cong k[G]$. Therefore, ϕ is an isomorphism of algebraic groups $G \cong \phi(G)$. So we have proved (i).

For (ii), we check that the maps above can be taken to be defined over F. □

Lemma 5.16. *Let H be a closed subgroup of G. Then*

$$H = \{g \in G : \lambda(g)\mathcal{I}_G(H) = \mathcal{I}_G(H)\} = \{g \in G : \rho(g)\mathcal{I}_G(H) = \mathcal{I}_G(H)\}.$$

Proof. We consider λ. The proof for ρ is similar. For $g, h \in H$, $f \in \mathcal{I}_G(H)$, we have $(\rho(g)f)(h) = f(g^{-1}h) = 0$, so $\rho(g)f \in \mathcal{I}_G(H)$. This proves $H \subset \{g \in G : \lambda(g)\mathcal{I}_G(H) = \mathcal{I}_G(H)\}$. Now assume that $g \in G$ and $\rho(g)\mathcal{I}_G(H) = \mathcal{I}_G(H)$. Then for all $f \in \mathcal{I}_G(H)$ we have $f(g^{-1}) = (\lambda(g)f)(e) = 0$. So $g^{-1} \in H$, and hence $g \in H$. This proves $H \supset \{g \in G : \lambda(g)\mathcal{I}_G(H) = \mathcal{I}_G(H)\}$. □

6 Jordan Decomposition (09/23)

Jordan Decomposition

Definition 6.1. Let V be a finite dimensional vector space over an algebraically closed field k. Let $x \in \mathrm{End}(V)$. x is called *nilpotent* if $x^n = 0$ for some $n \geq 1$ ($\iff$ 0 is the only eigenvalue of x). x is *semisimple* if the minimal polynomial of x has distinct roots ($\iff$ x is diagonalizable over k). x is *unipotent* if $x = 1 + n$ where n is nilpotent.

Remark 6.2. *0 is the only endomorphism of V that is both nilpotent and semisimple.*

Remark 6.3. *Suppose $x, y \in \mathrm{End}(V)$ commute. Then*
(i) x, y nilpotent $\Rightarrow x + y$ nilpotent.
(ii) x, y unipotent $\Rightarrow xy$ unipotent.
(iii) x, y semisimple $\Rightarrow x + y$ and xy are semisimple.

Proposition 6.4 (Additive Jordan Decomposition)**.** *Let $x \in End(V)$.*

(i) There exists unique $x_s, x_n \in End(V)$ such that $x = x_s + x_n$ and x_s is semisimple, x_n is nilpotent, and $x_s \cdot x_n = x_n \cdot x_s$.

(ii) There exists polynomials $p(T), q(T) \in k[T]$ satisfying $p(0) = q(0) = 0$ such that $x_s = p(x)$ and $x_n = q(x)$. In particular, x_s and x_n commute with x and in fact, they commute with any endomorphism of V that commutes with x.

(iii) If $A \subset B \subset V$ are subspaces and $x(B) \subset A$, then $x_s(B) \subset A$, $x_n(B) \subset A$.

(iv) If $xy = yx$ for some $y \in End(V)$, then

$$(x + y)_s = x_s + y_s,$$

$$(x + y)_n = x_n + y_n.$$

Proof. (i) Let $\det(T \cdot I - x) = \prod_{i=1}^{r} (T - \alpha_i)^{m_i}$ be the characteristic polynomial of x, where α_i are distinct engenvalues of x. Let

$$V_i = \ker(x - \alpha_i I)^{m_i} = \{v \in V : (x - \alpha_i I)^{m_i} v = 0\}$$

be the generalized eigenspaces. Note that if $v \in V_i$, then $(x - \alpha_i I)^{m_i} xv = x(x - \alpha_i I)^{m_i} v = 0$, so V_i is x-stable. By the Chinese Remainder Theorem for polynomials, there is some $p(T) \in k(T)$ such that

$$p(T) \equiv 0 \pmod{T}, \quad p(T) \equiv \alpha_i \pmod{(T - \alpha_i)^{m_i}} \text{ for all i.}$$

Let $x_s = p(x)$. Note that $p(\alpha_i) = \alpha_i$, so the eigenvalues of $x_s = p(x)$ are the same as those of x. Since V_i is x-invariant and p is a polynomial, V_i is x_s-invariant. Also, $x_s|_{V_i} = \alpha_i I|_{V_i}$. It follows that the V_i are the eigenspaces of x_s. Moreover, $V = \oplus_{i=1}^{r} V_i$ (which can be

proved by induction on r). Thus, x_s is semisimple (because the sum of dimensions of its eigenspaces is equal to $\dim(V)$, namely r), and $x_n = x - x_s$ is nilpotent.

Since $x_s = p(x)$ where p is a polynomial, then $x_s x = x x_s$, so

$$x_s x_n = x_s(x - x_s) = x_s x - x_s x_s = x x_s - x_s x_s = x_n x_s.$$

To prove the uniqueness, suppose $x = y_s + y_n$ is another such decomposition. Then $x_s - y_s = y_n - x_n$, hence $x_s - y_s$ and $y_n - x_n$ are both semisimple and nilpotent, hence $x_s = y_s, y_n = x_n$.

(ii) Take $p(T) \in k[T]$ as in part (i), $q(T) = T - p(T)$.

(iii) Since $x(B) \subset A$ and p is a polynomial, $p(x)(B) \subset A$, thus $x_s(B) \subset A$ by part (ii). Similarly $x_n(B) \subset A$.

(iv) This follows from 6.3 and uniqueness in part (i).

□

If we let $x_u = 1 + x_s^{-1} x_n$, then we get the Multiplicative Jordan Decomposition.

Corollary 6.5 (Multiplicative Jordan Decomposition)**.** *Let $x \in \mathrm{GL}(V)$. There exists unique elements $x_s, x_u \in \mathrm{GL}(V)$ such that $x = x_s x_u = x_u x_s$ and x_s is semisimple, x_u is unipotent.*

Remark 6.6. *Suppose V is a finite dimensional vector space over an algebraically closed field k. Let $a \in End(V)$. Let $W \subset V$ be a a-stable space. Then W is stable under a_s and a_n and $a|_W = a_s|_W + a_n|_W$ and $\overline{a} = \overline{a_s} + \overline{a_u}$ where $^-$ means the linear transformation induced on V/W. Similarly, if $a \in \mathrm{GL}(V)$, then $a|_W = a_s|_W \cdot a_u|_W$, and similarly for V/W.*

Remark 6.7. *Suppose V, W are two finite dimensional vector space over k. Let $\varphi : V \to W$ be linear. Let $a \in \mathrm{End}(W)$, $b \in \mathrm{End}(W)$. If $\varphi \circ a = b \circ \varphi$, i.e., the diagram*

$$\begin{array}{ccc} V & \xrightarrow{a} & V \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ W & \xrightarrow{b} & W \end{array}$$

is commutative, then

$$\varphi \circ a_s = b_s \circ \varphi$$

and

$$\varphi \circ a_n = b_n \circ \varphi.$$

Let V be a not necessarily finite dimensional vector space over k. Again

$$\mathrm{End}(V) := \text{algebra of endomorphisms of } V,$$

$$\mathrm{GL}(V) := \text{group of invertible endomorphisms of } V.$$

We say $a \in \mathrm{End}(V)$ is *locally finite* if V is a union of finite dimensional a-stable subspaces. We say $a \in \mathrm{End}(V)$ is *semisimple* if its restriction to any finite dimensional a-stable subspace is semisimple. We say $a \in \mathrm{End}(V)$ is *locally nilpotent* if its restriction to any finite dimensional a-stable subspace is nilpotent. We say $a \in \mathrm{End}(V)$ is *locally unipotent* if its restriction to any finite dimensional a-stable subspace is unipotent. For a locally finite $a \in \mathrm{End}(V)$, we have $a = a_s + a_n$ with a_s locally finite and semisimple, a_n locally finite and locally nilpotent. For $x \in V$, take a finite dimensional a-stable subspace W containing x, and put

$$a_s x := (a|_W)_s,$$

$$a_n x := (a|_W)_n.$$

It follows from the uniqueness statement of the finite dimensional Additive Jordan decomposition that $a_s x$ and $a_n x$ are independent of the choice of W. If $a \in \mathrm{GL}(V)$, we have a similar multiplicative Jordan decomposition $a = a_s \cdot a_u$ where a_s is semisimple, a_u is locally unipotent.

Remark 6.8. *There is an infinite-dimensional generalization of Remark 6.7.*

Jordan Decomposition in Linear Algebraic Groups

We now come to the Jordan decomposition in linear algebraic groups.

Let G be a linear algebraic group and $A = k[G]$. From our discussion of G-actions, we can conclude that the right translation $\rho(g), g \in G$, is a locally finite element of $\mathrm{GL}(A)$, i.e., $\rho(g) = \rho(g)_s \rho(g)_u$.

Theorem 6.9. *(i) There exists unique elements g_s and g_u in G such that $\rho(g)_s = \rho(g_s)$, $\rho(g)_u = \rho(g_u)$, and $g = g_s g_u = g_u g_s$.*

(ii) If $\phi : G \to G'$ is a homomorphism of linear algebraic groups, then $\phi(g)_s = \phi(g_s)$ and $\phi(g)_u = \phi(g_u)$.

(iii) If $G = \mathrm{GL}_n$, then g_s and g_u are the semisimple and unipotent parts of $g \in \mathrm{GL}(V)$, where $V = k^n$ as before.

Remark 6.10. *g_s is called the semisimple part of g, and g_u is called the unipotent part of g.*

Proof of Theorem 6.9. (i) Let $m : A \otimes A \to A$ be the k-algebra homomorphism corresponding to multiplication in G. $\rho(g)$ is an algebra automorphism of A. That means

$$m \circ (\rho(g) \otimes \rho(g)) = \rho(g) \circ m.$$

By Remark 6.7, we have

$$m \circ (\rho(g)_s \otimes \rho(g)_s) = \rho(g)_s \circ m.$$

So $\rho(g)_s$ is also an automorphism of A. So $f \mapsto (\rho(g)_s f)(e)$ defines a homomorphism $A \to k$, i.e., a point in G, and we call it g_s. Now $\rho(g)$ commutes with all left translation $\lambda(x), x \in G$, and the $\lambda(x)$ are locally finite, so $\rho(g)_s$ also commutes with all $\lambda(x)$. In other words, for $f \in A$,

$$\begin{aligned}(\rho(g)_s f)(x) &= (\lambda(x^{-1})\rho(g)_s f)(e) \\ &= (\rho(g)_s \lambda(x^{-1}) f)(e) \\ &= (\lambda(x^{-1})f)(g_s) \quad \text{(by definiton of } g_s) \\ &= f(xg_s) \\ &= (\rho(g_s)f)(x).\end{aligned}$$

Hence $\rho(g)_s = \rho(g_s)$. A similar argument also gives $\rho(g)_u = \rho(g_u)$. So

$$\rho(g) = \rho(g)_s \rho(g)_u = \rho(g_s)\rho(g_u) = \rho(g_s g_u).$$

But ρ is a faithful representation of G (i.e., $\ker \rho$ is trivial), so $g = g_s g_u$. Similarly $g = g_u g_s$.

(ii) Recall that for homomorphism of algebraic groups $\phi : G \to G'$, we saw that $\mathrm{Im}(\phi) = \phi(G)$ is closed in G'. So ϕ can be factored into

$$G \to \mathrm{Im}(\phi) \to G'.$$

This reduces the proof to two cases: case (a) the inclusion $\mathrm{Im}\phi \to G'$, and case (b) the surjection $G \to \mathrm{Im}\phi$.

For case (a), G is a closed subgroup of G' and ϕ is the inclusion. Let $k[G] = k[G']/I$. By Lemma 5.16,

$$G = \{g \in G' : \rho(g)I = I\}.$$

Now $W = I$ is a subspace of $V = k[G']$ and it is stable under $\rho(g)$, so by Remark 6.6, we have a Jordan decomposition on $V/W = k[G]$. So

$$\phi(g)_s = \phi(g_s),$$

$$\phi(g)_u = \phi(g_u),$$

as ϕ is just inclusion.

For case (b), if ϕ is surjective, then $k[G']$ can be viewed as a subspace of $k[G]$, which is stable under all $\rho(g), g \in G$. Again, the result follows from Remark 6.6.

(iii) Let $G = \mathrm{GL}(V)$ with $V = k^n$. Let $0 \neq f \in V^\vee =$ dual of V and define $\tilde{f}(v) \in k[G]$ via $\tilde{f}(v)(g) = f(gv)$. Then $\tilde{f}$ is an injective linear map $V \to k[G]$, and $\forall x \in G$, we have

$$\tilde{f}(gv)(x) = f(xgv) = \tilde{f}(v)(xg) = [\rho(g)\tilde{f}(v)](x).$$

Hence $\tilde{f}(gv) = \rho(g)\tilde{f}(v)$. By Remark 6.8, we have

$$\tilde{f}(g_s v) = \rho(g)_s \tilde{f}(v),$$

$$\tilde{f}(g_u v) = \rho(g)_u \tilde{f}(v),$$

which implies (iii).

□

Corollary 6.11. *$x \in G$ is semisimple $\iff$ for any homomorphism ϕ from G onto a closed subgroup of some $\boldsymbol{GL}_n$, $\phi(x)$ is semisimple. Similarly for unipotent elements.*

Jordan Decomposition and F-structures

Let $F \subset k$ be a subfield. Assume G is an F-group. Note that if $x \in G(F)$, then x_s and x_u need not lie in $G(F)$. Here is an example.

Example 6.12. Assume that $\mathrm{char}(k) = 2$ and $F \neq F^2$ (i.e., F is non-perfect). Let $G = \mathbf{GL}_2$. Let $a \in F \backslash F^2$ and $x = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}$. Then the Jordan decomposition of x in $\mathbf{GL}_2(k)$ is

$$x = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} = x_s x_u = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & \sqrt{a} \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{\sqrt{a}} \\ \sqrt{a} & 0 \end{pmatrix}.$$

But $x_s, x_u \notin \mathbf{GL}_2(F)$. Moreover, it is the case that if F is perfect, then the semisimple and unipotent parts of an element in $G(F)$ are again in $G(F)$.

Unipotent Groups

Definition 6.13. A linear algebraic group G is *unipotent* if all its elements are unipotent.

Example 6.14. The linear group $\mathbf{U}_n = \left\{ \begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \cdots & * \\ 0 & 0 & 1 & \cdots & * \\ 0 & 0 & 0 & \ddots & * \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \right\}$ is unipotent. Actually it turns out that this is essentially the only example.

Proposition 6.15. *Let G be a subgroup of $\boldsymbol{GL}_n$ consisting of unipotent matrices. Then there exists $x \in \boldsymbol{GL}_n$ such that $xGx^{-1} \subset U_n$.*

Before proving Proposition 6.15, we need the Burnside's Theorem.

Theorem 6.16 (Burnside's Theorem)**.** *Let E be a finite dimensional vector space over an algebraically closed field k, R be a subalgebra of* $\mathrm{End}(E)$*. If E is a simple R-module (i.e., the action is irreducible), then $R = \mathrm{End}(E)$.*

Proof of Proposition 6.15. We prove this by induction on n. Suppose this is true for $m < n$, let $V = k^n$. Suppose that there is a non-trivial G-invariant subspace $0 \subsetneq W_1 \subsetneq V$. Let W_2 be the complementary to W_1 so that $V = W_1 \oplus W_2$. Since $n > \dim W_1, \dim W_2$, there are $x_i \in \mathrm{GL}(W_i)$ so that $x_i G x_i^{-1}$ consists of unipotent elements for $i = 1, 2$. Let $x = x_1 \oplus x_2$. Then xGx^{-1} consists of unipotent elements as well.

Next, suppose no non-trivial G-invariant subspace exists, i.e., G acts irreducibly in V. Let $g \in G$. Then $\mathrm{Tr}(g) = n$. Then for any $h \in G$, $\mathrm{Tr}((1-g)h) = \mathrm{Tr}(h) - \mathrm{Tr}(gh) = n - n = 0$. By Burnside's Theorem, the elements in G span the vector space $\mathrm{End}(V)$. This means that $\mathrm{Tr}(h) = \mathrm{Tr}(gh)$ for all $h \in \mathrm{End}(V)$. Now choosing $h = E_{ij}$, we see that this is only possible when $g = 1$, i.e., $G = \{1\}$. □

Remark 6.17. *By Proposition 6.15, if G is unipotent linear algebraic group and $G \to \mathrm{GL}(V)$ is a rational representation of G, then there is a nonzero vector $v \in V$ which is fixed by all of G (consider the first basis element after conjugating into U_n).*

Proposition 6.18 (Kostant-Rosenlicht)**.** *Let G be a unipotent linear algebraic group and let X be an affine G-space. Then all orbits of G in X are closed.*

Proof. Let $\mathcal{O}$ be an orbit. Without loss of generality we may assume that $X = \overline{\mathcal{O}}$ and hence $\mathcal{O}$ is dense in X. Recall that an orbit is open in its closure by Lemma 5.6, so $\mathcal{O}$ is open in $\overline{\mathcal{O}}$. Let $Y = \overline{\mathcal{O}} \backslash \mathcal{O}$. Then G acts locally finitely on the ideal $\mathcal{I}_X(Y)$. Because G is unipotent, we may apply Remark 6.17 to the rational representation $G \to \mathrm{GL}(\mathcal{I}_X(Y))$. So there is a non-zero function $f \in \mathcal{I}_X(Y)$ fixed by elements of G, i.e., $\rho(g)f = f, \forall g \in G$. Now for any $o \in \mathcal{O}$, $(\rho(g)f)(o) = f(o)$. So $f(og) = f(o), \forall o \in \mathcal{O}, \forall g \in G$. Hence $f(o) = f(e), \forall o \in \mathcal{O}$, i.e., f is constant on $\mathcal{O}$. Since $\mathcal{O}$ is dense in X, f is constant on X. Thus $\mathcal{I}_X(Y) = k[X]$, i.e., $Y = \emptyset$, and hence $\mathcal{O} = \overline{\mathcal{O}}$.

□

7 Commutative Linear Algebraic Groups I (09/30)

Structure of Commutative Algebraic Groups

Theorem 7.1 (Kolchin)**.** *Let G be a commutative linear algebraic group. Then*
(i) The sets G_s and G_u of semisimple and unipotent elements are closed subgroups.
(ii) The product map $\pi : G_s \times G_u \to G$ is an isomorphism of algebraic groups.

Proof. (i) We may assume that G is a closed subgroup of some $\mathbf{GL}_n$, by Theorem 5.15. Recall that if $x, y \in \mathrm{End}(V)$, then $xy = yx$ implies that $(xy)_s = x_s y_s$ and $(xy)_u = x_u y_u$. This implies that both G_s and G_u are subgroups.

G_u is a closed subset for general (not necessarily commutative) linear algebraic group G because the set of all unipotent matrices in $\mathrm{GL}_n(k)$ is the zero set of polynomials implied by $(x-1)^n = 0$.

To see G_s is closed, recall that without loss of generality we may assume $G \subset \mathbf{T}_n =$ upper triangular matrices in $\mathbf{GL}_n$ and $G_s \subset \mathbf{D}_n$. This forces $G_s = G \cap \mathbf{D}_n$ which shows that G_s is closed. (Note that for general G, it is rare that G_s is closed).

(ii) π is an isomorphism of abstract groups by the uniqueness of Jordan decomposition in G. Also, π is a morphism of varieties and the map $G \to G_s$ defined by $x \mapsto x_s$ is a morphism of algebraic varieties because it maps x to some of its matrix entries, so it gives polynomials. Hence $\pi^{-1} : x \mapsto (x_s, x_s^{-1}x)$ is a morphism of varieties. Hence π is an isomorphism of algebraic groups. □

Corollary 7.2. *If G is connected, then so are G_s and G_u.*

Proof. G_s and G_u are imagies of the connected group G under continuous maps, so they are connected. □

Proposition 7.3. *Let G be a connected linear algebraic group of dimension 1. Then*
(i) G is commutative.
(ii) Either G is G_s or G_u.
(iii) If G is unipotent and $p = char(k) > 0$, then the elements of G have order dividing p.

Proof. (i) Fix $g \in G$ and consider the morphism $\phi : G \to G$ defined by $x \mapsto xgx^{-1}$. Because G is connected (i.e., irreducible topological group), its image $\phi(G)$ is also an irreducible topological group, which implies $\overline{\phi(G)}$ is an irreducible closed subset of G. If $\overline{\phi(G)}$ is a proper irreducible closed subset of G, it must have dimension less than $\dim G = 1$. So either $\overline{\phi(G)} = \{g\}$ (i.e., G is commutative) or $\overline{\phi(G)} = G$.

Let's assume $\overline{\phi(G)} = G$. Because $\overline{\phi(G)}$ contains a nonempty open subset U of $\overline{\phi(G)}$, we would have $G - \phi(G)$ is finite (it suffices to show $G - U$ is finite since $G - U \supset G - \phi(G)$, but $G - U$ is closed and a variety, and $\dim(G - U) = 0$, so $G - U$ is finite). Viewing G as a closed subgroup of some $\mathbf{GL}_n$, there are only finitely many possibilities (because $\mathrm{char}(x) = \mathrm{char}(yx^{-1}y)$) for the characteristic polynomial $\det(T \cdot 1 - x), x \in G$. But G is

connected, so the characteristic polynomial is constant. Taking x to be identity, it must be $(T-1)^n$. This means G is unipotent. Hence G is solvable. Now $G' = (G, G)$ the commutator subgroup of G is a connected, closed subgroup and can only be $\{e\}$. Now $g^{-1}\phi(G) \subset G'$, which is a contradiction.

(ii) Because G is connected, both G_s and G_u are irreducible, closed subvarieties of G. If $G \neq G_s$, then G_s is a proper subvariety so $\dim(G_s) < \dim(G) = 1$, i.e., $G_s = \{e\}$. Thus $G = G_u$.

(iii) Assume that G is unipotent and $p = \mathrm{char}(k) > 0$. Let

$$G^{p^h} = \{p^h - \text{power of elements of } G\}.$$

Then it is easy to check that G^{p^h} is a connected, closed subgroup of G, so it must be G or $\{e\}$. Viewing G as an upper triangular matrices in some $\mathbf{GL}_n$, $G^{p^h} = \{e\}$ if $p^h \geq n$, which in characteristic p implies $G^p = \{e\}$.

□

Algebraic Tori

Definition 7.4. Let G be a linear algebraic group. A *rational character* (or just a character) of G is a homomorphism of algebraic groups $\chi : G \to \mathbf{G}_m$. We denote

$$X^*(G) = \text{abelian group of rational characters with additive notation,}$$
$$\text{i.e., } (\chi_1 + \chi_2)(g) = \chi_1(g)\chi_2(g).$$

Note that characters are regular functions on G, so $X^*(G) \subset k[G]$. Also, characters are linearly independent in $k[G]$ (this is the Dedekind's Lemma).

Lemma 7.5 (Dedekind's Lemma)**.** *Let G be any group, E be any field. $X(G) = \mathrm{Hom}_{group}(G, E^*)$ is a linearly independent subset of the vector space over E of functions $\{G \to E\}$.*

Proof. If there is a nontrivial linear independence relation among the elements in $X(G)$, take one of minimal length:

$$a_1\chi_1 + \cdots + a_n\chi_n = 0, \quad 0 \neq a_i \in \mathbb{Z}, \chi_i \text{ distinct.}$$

For $g, h \in G$,

$$\sum_{i=1}^{n} a_i\chi_i(g)\chi_i(h) = 0 = \chi_1(g)\sum_{i=1}^{n} a_i\chi_i(h).$$

So

$$\sum_{i=2}^{n} a_i(\chi_i(g) - \chi_1(g))\chi_i(h) = 0.$$

Since $\chi_2 \neq \chi_1$, there exists some $g \in G$ such that $\chi_2(g) - \chi_1(g) \neq 0$. This contradicts the minimality of the length. □

Definition 7.6. A *cocharacter* (or a *multiplicative one parameter subgroup*) of G is a homomorphism of algebraic groups $\mathbf{G}_m \to G$. We denote

$$X_*(G) = \text{the set of cocharacters.}$$

Note that cocharacters may not necessarily be abelian. However, if G is commutative, then $X_*(G)$ is an abelian group. Even G is not commutative, we still have an action of $\mathbb{Z}$ on $X_*(G)$ by

$$(n \cdot \lambda)(a) = \lambda(a)^n.$$

We write $-\lambda = (-1) \cdot \lambda$.

Definition 7.7. A linear algebraic group G is called *diagonalizable* if it is isomorphic to a closed subgroup of some $\mathbf{D}_n$. G is called an *algebraic torus* (or just *torus*) if it is isomorphic to some $\mathbf{D}_n$.

Example 7.8. $G = \mathbf{D}_n$ is a torus, while $G = \mathbf{D}_n \times \{\pm 1\}$ is diagonalizable.

Example 7.9. $G = \mathbf{D}_n = \left\{ \begin{pmatrix} x_1 & & \\ & \ddots & \\ & & x_n \end{pmatrix} : x_i \neq 0 \right\}$. Set $\chi_i(x) = x_i$. Then each χ_i is a character of $\mathbf{D}_n$ and in fact $k[\mathbf{D}_n] = k[\chi_1, \cdots, \chi_n, \chi_1^{-1}, \cdots, \chi_n^{-1}]$. $\chi_1^{a_1}\chi_2^{a_2}\cdots\chi_n^{a_n}$, where $(a_1, \cdots, a_n) \in \mathbb{Z}^n$, are all the characters of $\mathbf{D}_n$, and they form a basis for $k[\mathbf{D}_n]$. Moreover,

$$X^*(\mathbf{D}_n) \cong \mathbb{Z}^n$$

as abelian groups. Also, any cocharacter $\mathbf{G}_m \to \mathbf{D}_n$ is given by

$$x \mapsto \begin{pmatrix} x^{a_1} & & & \\ & x^{a_2} & & \\ & & \ddots & \\ & & & x^{a_n} \end{pmatrix}$$

where $(a_1, \cdots, a_n) \in \mathbb{Z}^n$. In other words,

$$X_*(\mathbf{D}_n) \cong \mathbb{Z}^n$$

as abelian groups.

Theorem 7.10. *The following are equivalent for a linear algebraic group G.*

(i) G is diagonalizable.

(ii) $X^*(G)$ is an abelian group of finite type. $X^*(G)$ is a k-basis for $k[G]$.

(iii) Any rational representation of G is a direct sum of one dimensional representations.

Proof. (i) $\Rightarrow$ (ii). Assume G is diagonalizable. Then G is a closed subgroup of some $\mathbf{D}_n$. Hence $k[G]$ is a quotient of $k[\mathbf{D}_n]$. Restriction of characters from $\mathbf{D}_n$ to G reduces characters of G and they span $k[G]$. By Dedekind's Lemma (Lemma 7.5), they form a basis and any character of G is a linear combination of these restrictions. Hence $X^*(\mathbf{D}_n) \to X^*(G)$ is a surjective homomorphism of abelian groups. Recall that $X^*(\mathbf{D}_n) \cong \mathbb{Z}^n$. So $X^*(G)$ is of finite type.

(ii) $\Rightarrow$ (iii). Let $\phi : G \to \mathrm{GL}(V)$ be a rational representation of G in a finite dimensional vector space V. Then (ii) implies that we can define linear maps $A_\chi : V \to V, \chi \in X^*(G)$ via $\phi(x) = \sum_{\chi \in X^*(G)} \chi(x) A_\chi$ with $A_\chi = 0$ for all but finitely many χ's. To see this, fix a basis for V and write $\phi(x) = [\phi_{ij}(x)]_{n\times n}$. Then $\phi_{ij} \in k[G]$ and by (ii), we can write $\phi_{ij} = \sum_{\chi \in X^*(G)} \alpha_{ij\chi}\chi$. Then $\phi(x) = \sum_{\chi \in X^*(G)} A_\chi \chi(x)$ where A_χ has the matrix $[\alpha_{ij\chi}]_{n\times n}$ with respect to the fixed basis. For $x, y \in G$,

$$\phi(xy) = \sum_{\chi \in X^*(G)} \chi(xy) A_\chi = \phi(x)\phi(y) = \left(\sum_{\chi \in X^*(G)} \chi(x) A_\chi \right) \left(\sum_{\chi \in X^*(G)} \chi(y) A_\chi \right).$$

By Dedekind's Lemma (Lemma 7.5),

$$A_\chi A_\psi = \begin{cases} 0 & \text{if } \chi \neq \psi \\ A_\chi & \text{if } \chi = \psi. \end{cases}$$

Also, $\sum_{\chi \in X^*(G)} A_\chi = \phi(e) = \mathrm{id}$. Put $V_\chi = \mathrm{im}(A_\chi)$. Then it follows that V is a direct sum of V_χ and $x \in G$ acts on V_χ via mapping by $\chi(x)$.

(iii) $\Rightarrow$ (i). This direction is clear.

□

Corollary 7.11. *If a linear algebraic group G is diagonalizable, then $X^*(G)$ is an abelian group of finite type without p-torsion if $p = char(k) > 0$.*

In fact, if G is diagonalizable, the algebra $k[G]$ is isomorphic to the group algebra of $X^*(G)$.

Group Algebras of Abelian Groups

Let M be an abelian group of finite type. The *group algebra* of M is

$$k[M] := \text{ the algebra with basis } (e_m)_{m\in M} \text{ with mapping defined by } e_m \cdot e_n = e_{m+n}.$$

Observe that if M_1, M_2 are two abelian groups of finite type, then

$$k[M_1 \oplus M_2] = k[M_1] \otimes_k k[M_2].$$

Define

$$\Delta : k[M] \to k[M] \otimes_k k[M]$$
$$e_m \to e_m \otimes e_m,$$

$$\iota : k[M] \to k[M]$$
$$e_m \to e_{-m},$$

and

$$e : k[M] \to k$$
$$e_m \to 1.$$

Recall that if M is of finite type, then $M \cong \mathbb{Z}^r \oplus$ (direct sum of finite groups). If $p \cdot m = 0$ for a prime p, then m is called a *p-torsion* element.

Proposition 7.12. *Assume that $p = char(k) > 0$, and M has no p-torsion.*

(i) $k[M]$ is an affine algebra, and there is a diagonalizable linear algebraic group $\mathcal{G}(M)$ with $k[\mathcal{G}(M)] = k[M]$ such that Δ, ι, e are comultiplication, antipode and the identity elements of $\mathcal{G}(M)$.

(ii) There is a canonical isomorphism $M \cong X^*(\mathcal{G}(M))$.

(iii) If G is diagonalizable, then there is a canonical algebraic group isomorphism $\mathcal{G}(X^*(G)) \cong G$.

Example 7.13. Let $M = \mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} = M_1 \oplus M_2$. Then $\mathcal{G}(M) = G_1 \times G_2$ where $G_1 = \mathcal{G}(M_1)$ and $G_2 = \mathcal{G}(M_2)$, and $k[M_1] \cong k[T, T^{-1}]$, $k[M_2] \cong k[T]/(T^{12} - 1)$. By assumption, if $p > 0$, $p \not| 12$ (i.e., $p \neq 2, 3$), then $k[M_2]$ is a reduced algebraic group. Then $\mathcal{G}(M) \cong \mathbf{D}_1 \times$ (finite group).

Example 7.14. $\mathcal{G}(\mathbb{Z}^n) \cong \mathbf{D}_n$.

Corollary 7.15. *Let G be a diagonalizable group.*

(i) G is a direct product of a torus and a finite abelian group of order prime to p, if $p = char(k) > 0$.

(ii) G is a torus $\iff$ G is connected.

(iii) G is a torus $\iff$ $X^*(G)$ is a free abelian group.

Proposition 7.16 (Rigidity of Diagonalizable Groups)**.** *Let G and H be diagonalizable groups and let V be a connected affine variety. Assume that $\varphi : V \times G \to H$ is a morphism of varieties such that for each $v \in V$, the map $G \to H$ defined by $x \to \varphi(v, x)$ is a homomorphism of algebraic groups. Then $\varphi(v, x)$ is independent of v.*

For G an arbitrary linear algebraic group and H a closed subgroup, set

$$Z_G(H) = \{g \in G : ghg^{-1} = h, \forall h \in H\}, \quad - \text{ centralizer of } H \text{ in } G,$$
$$N_G(H) = \{g \in G : gHg^{-1} \in H\}, \quad - \text{ normalizer of } H \text{ in } G,$$

The defining conditions can be expressed as polynomial conditions, so these are closed subgroups of G and $Z_G(H) \triangleleft N_G(H)$.

Corollary 7.17. *If H is a diagonalizable subgroup of G, then $N_G(H)^0 = Z_G(H)^0$ and $N_G(H)/Z_G(H)$ is finite.*

Proof. Let $V = N_G(H)^0$. Apply rigidity (Proposition 7.16) to

$$\begin{aligned} \varphi : N_G(H)^0 \times H &\to H \\ (x, y) &\mapsto xyx^{-1} \end{aligned}$$

to conclude that xyx^{-1} is independent of x, i.e., $xyx^{-1} = y$, $\forall x \in N_G(H)^0$. Thus $N_G(H)^0 \subset Z_G(H)$. This proves $N_G(H)^0 = Z_G(H)^0$.

□

8 Commutative Linear Algebraic Groups II (10/07)

Review of Pairings

Let R be a commutative ring with 1 and let M, N be two (left) R-modules. The set $\mathrm{Hom}_R(M,N) = \{R\text{-linear maps from } M \text{ to } N\}$ is an R-module.

Example 8.1. M is any R-module, $N = R$, then $M^\vee = \mathrm{Hom}_R(R,N)$ is called the *dual module*, or *dual space*, or *R-module of M*.

Example 8.2. $R^\vee = \mathrm{Hom}_R(R,R) \cong R$.

Example 8.3. $R = F$ is a field, M, N are vector spaces over F. This comes from linear algebra.

Definition 8.4. A *pairing* between M and N is a bilinear map $\langle \cdot, \cdot \rangle : M \times N \to R$, i.e., R-linear in each component when the other is fixed.

Example 8.5. A dot product $R^n \times R^n \to R$ is a pairing.

Example 8.6. There are two natural pairings,

$$\begin{aligned} M_n(R) \times M_n(R) &\to R \\ \langle A, B \rangle &= \mathrm{Tr}(AB) \end{aligned}$$

and

$$\begin{aligned} M_n(R) \times M_n(R) &\to R \\ \langle A, B \rangle &= \mathrm{Tr}(AB^{\mathrm{T}}). \end{aligned}$$

Example 8.7. The map

$$\begin{aligned} M \times M^\vee &\to R \\ \langle m, \varphi \rangle &= \varphi(m) \end{aligned}$$

is called the standard pairing between a module and its dual.

Example 8.8. The map

$$\begin{aligned} R[x] \times R[x] &\to R \\ \langle f, g \rangle &= f(0)g(0) \end{aligned}$$

is a pairing. Then $\langle x, g \rangle = 0$ for all $g \in R[x]$ even though $x \neq 0$. In fact, $\langle f, g \rangle = 0$ for all $g \in R[x]$ if $x | f$.

We can use a pairing to think of M and N as part of the dual of the other module. For $m \in M$, $n \mapsto \langle m, n\rangle$ is a functional on N and for $n \in N$, $m \mapsto \langle m, n\rangle$ is a functional on M. However, if the pairing behaves badly, we may have $\langle m, n\rangle = 0\ \forall n$ with $m \neq 0$.

For R-modules M and N, $\mathrm{Hom}_R(M, N^\vee)$, $\mathrm{Hom}_R(N, M^\vee)$ and

$$\mathrm{Bil}_R(M, N; R) = \{\text{bilinear maps from } M \text{ to } N\}$$

are all isomorphic as R-modules. The point is that a bilinear map allows us to use M to parametrize a piece of $N^\vee$ and similarly for N. However, some pairings may make different elements of M behave like the same element of $N^\vee$. For example, a nonzero element of M might pair with every element of N to have the value 0, as behavior we expect if $m = 0$.

The pairings that allow us to identify M and N with each other's full dual module are the "perfect" pairings.

Definition 8.9. A pairing $\langle \cdot, \cdot\rangle : M \times N \to R$ is called a *perfect pairing* if the induced linear maps $M \to N^\vee$ and $N \to M^\vee$ are both isomorphisms.

Note that when R is a field and M, N are finite dimensional vector spaces of the same dimension, then a pairing $\langle \cdot, \cdot\rangle : M \times N \to R$ is perfect if and only if the induced map $M \to N^\vee$ is injective, i.e., $\langle m, n\rangle = 0$ for all $n \in N$ implies $m = 0$. (Then $N \to M^\vee$ is also automatically an isomorphism.) However, an injective linear map of free modules with the same rank need not be an isomorphism, for example, the map $\mathbb{Z} \to \mathbb{Z}$ defined by $x \mapsto 2x$. So in the case of non-field commutative ring R with M and N free of the same finite rank, it is not enough to just check that $M \to N^\vee$ is injective.

Perfect pairing of modules M and N is stronger than just identification of one of them with the dual of the other. It identifies each module as the dual of the other $M \cong N^\vee$ and $N \cong M^\vee$, both coming from the perfect pairing $\langle \cdot, \cdot\rangle : M \times N \to R$.

Characters and Cocharacters of Tori

Let T be a torus. Denote the character group

$$X = X^*(T) = \{\chi : T \to \mathbf{G}_m\}$$

and the cocharacter group

$$Y = X_*(T) = \{\lambda : \mathbf{G}_m \to T\}.$$

For $\chi \in X, \lambda \in Y$, $a \in k^*$, consider the character

$$\begin{aligned} \mathbf{G}_m &\to \mathbf{G}_m \\ a &\mapsto \chi(\lambda(a)). \end{aligned}$$

Recall $X^*(\mathbf{G}_m) \cong \mathbb{Z}$ so $\chi(\lambda(a)) = a^{\langle \chi, \lambda\rangle}$ for some $\langle \chi, \lambda\rangle \in \mathbb{Z}$.

Lemma 8.10. *(i) $\langle \cdot, \cdot \rangle : X \times Y \to \mathbb{Z}$ defines a perfect pairing, i.e., any homomorphism $X \to \mathbb{Z}$ is of the form $\chi \mapsto \langle \chi, \lambda \rangle$ for some $\lambda \in Y$ and any homomorphism $Y \to \mathbb{Z}$ is of the form $\lambda \mapsto \langle \chi, \lambda \rangle$ for some $\chi \in X$. In particular, Y is a free $\mathbb{Z}$-module.*

(ii) The map $a \otimes \lambda \mapsto \lambda(a)$ defines a canonical isomorphism of abelian groups $k^* \otimes_{\mathbb{Z}} Y \cong T$.

Proof. (i) Since T is a torus, it is isomorphic to some D_n. Then $X = \{\chi_1^{a_1}\chi_2^{a_2}\cdots\chi_n^{a_n} : (a_1, a_2, \cdots, a_n) \in \mathbb{Z}^n\} \cong \mathbb{Z}^n$ and $Y = \{x \mapsto \mathrm{diag}(x^{b_1}x^{b_2}\cdots x^{b_n} : (b_1, b_2, \cdots, b_n) \in \mathbb{Z}^n\} \cong \mathbb{Z}^n$. So the assertion is clear.

(ii) This follows from the freeness of Y. □

Tori and F-structures

Let $F \subset k$ be a subfield.

Definition 8.11. An *F-torus* is an F-group which is also a torus. An F-torus T which is F-isomorphic to some $\mathbf{D}_n$ is called *F-split*.

Example 8.12. Let $k = \mathbb{C}$, $F = \mathbb{R}$. Then $G = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbf{GL}_2 \right\}$ is an $\mathbb{R}$-torus which is not $\mathbb{R}$-split.

Proposition 8.13. *(i) An F-torus T is F-split $\iff$ all its characters are defined over F. In that case, the characters form a basis of $F[T]$.*

(ii) Any rational representation over F of an F-split torus is a direct sum of one-dimensional representations over F.

Torus Action

Let X, Y, T as before. Let V be an affine T-space. This leads to locally finite representation s of T in $k[V]$ as before.

For $\chi \in X$, put

$$k[V]_\chi = \{f \in k[V] : s(t) \cdot f = \chi(t)f, \forall t \in T\}.$$

We saw that any rational representation of a diagonalizable group was a direst sum of 1-dimensional rational representations of the subspaces. $k[V]_\chi$ define an X-grading of the algebra $k[V]$, i.e., $k[V] = \oplus_{\chi \in X} k[V]_\chi$ and $k[V]_\chi k[V]_\psi \subset k[V]_{\chi+\psi}$ for $\chi, \psi \in X$.

Example 8.14. If $T = \mathbf{G}_m$, then $X = \mathbb{Z}$ and the grading structure on $k[V]$ is the usual one (given by degrees of monomials).

For Z a variety and $\varphi : \mathbf{G}_m \to Z$ a morphism of varieties, write $\lim_{a\to 0} \varphi(a) = z$ if φ extends to a morphism $\tilde{\varphi} : \mathbf{A}^1 \to Z$ such that $\tilde{\varphi}(0) = z$. Put $\varphi'(a) = \varphi(a^{-1})$ and define $\lim_{a\to\infty} \varphi(a) = \lim_{a\to 0} \varphi'(a)$.

If V is a T-space and $\lambda \in T$, we write

$$V(\lambda) = \{v \in V : \lim_{a\to 0} \lambda(a) \cdot v \text{ exists}\}.$$

Then

$$V(-\lambda) = \{v \in V : \lim_{a\to \infty} \lambda(a) \cdot v \text{ exists}\}.$$

Lemma 8.15. *Assume V is affine.*
(i) $V(\lambda)$ is a closed subset of V.
(ii) $V(\lambda) \cap V(-\lambda)$ is the set of fixed points in Im(λ), i.e.,

$$V(\lambda) \cap V(-\lambda) = \{v \in V : \lambda(k^*) \cdot v = \{v\}\}.$$

Proof. (i) An element $f \in V(\lambda)$ can be written as $f = \sum_\chi f_\chi$, $f_\chi \in k[V]_\chi$. Then

$$s(\lambda(a)) \cdot f = \sum_\chi a^{\langle \chi, \lambda\rangle} f_\chi.$$

So $\lim_{a\to 0} \lambda(a) \cdot v$ exists $\iff$ v annihilates all functions in V_χ with $\langle \chi, \lambda\rangle < 0$. This proves (i).

(ii) Now, $V(\lambda) \cap V(-\lambda)$ is the set of v, annihilating all V_χ with $\langle \chi, \lambda\rangle \neq 0$. Then

$$V(\lambda) \cap V(-\lambda) = \{v \in V : f(\lambda(a) \cdot v) = f(v), \forall f \in k[V], a \in k^*\}.$$

This is just the set of fixed points. □

Example 8.16. Let G is a linear algebra group, $\lambda : \mathbf{G}_m \to G$ be a cocharacter. Consider the action of $T = \mathbf{G}_m$ on G by $a \cdot x = \lambda(a)x\lambda(a)^{-1}$. Write $P(\lambda) = \{x \in G : \lim_{a\to 0} a \cdot x \text{ exists}\}$. This is a subgroup of G. By Lemma 8.15 (i), it is closed and by Lemma 8.15 (ii), $P(\lambda) \cap P(-\lambda)$ is the centralizer of Im(λ).

Additive Functions and Elementary Unipotent Groups

The next goal is to classify connected 1-dimensional groups. It requires a study of "additive functions".

Definition 8.17. An *additive function* on a linear algebraic group G is a homomorphism of algebraic groups $f : G \to \mathbf{G}_a$. Denote

$$\mathcal{A} = \mathcal{A}(G) = \text{ the set of additive functions on } G,$$

which is a subspace of the algebra $k[G]$. Let $F \subset k$ be a subfield and G be an F-group, then write

$$\mathcal{A}(F) = \mathcal{A}(G)(F) = F\text{-vector space of additive functions defined over } F.$$

Note that if $p = \mathrm{char}(k) > 0$, then p-th power of an additive function is again an additive function. This will allow us to define a ring R over which $\mathcal{A}$ is a module.

If $p = \mathrm{char}(k) > 0$, then $\varphi : x \mapsto x^p$ defines an isomorphism of F onto a subfield of F^p (recall F is perfect if $F = F^p$). We define a ring $R = R(F)$ as follows. The underlying additive group is $F[T]$ – polynomials in T, and multiplication is defined by

$$(\sum a_i T^i)(\sum b_j T^j) = \sum a_i(\varphi^i(b_j))T^{i+j}.$$

Then R is an associative but non-commutative ring. Observe that the subfield F of R does not lie in the center of R, and degree has its usual property (i.e., R has no non-zero divisors). If $p = \mathrm{char}(k) = 0$, then define $R(F) = F$.

Now, if $p > 0$, we define a left R-module structure on $\mathcal{A}(F)$ by $(\sum a_i T^i) \cdot f = \sum a_i f^{p^i}$. If $p = 0$, then $R = F$ and $\mathcal{A}(F)$ is trivially an R-module.

Example 8.18. Consider $G = \mathbf{G}_a^n$. Then $F[G] = F[T_1, \cdots, T_n]$ and any additive function in $F[G]$ is an additive polynomial, i.e., $f \in F[T_1, \cdots, T_n]$ satisfying $f(T_1 + u_1, \cdots, T_n + u_n) = f(T_1, \cdots, T_n) + f(u_1, \cdots, u_n)$. The set of additive polynomials is a left R-module denoted by $\mathcal{A}(\mathbf{G}_a^n)(F)$.

Definition 8.19. A unipotent linear algebraic group G is called *elementary* if it is abelian and when $p = \mathrm{char}(k) > 0$, its elements have order dividing p. G is called a *vector group* if $G \cong \mathbf{G}_a^n$ for some n.

Theorem 8.20. *The followings are equivalent for a linear algebraic group G:*
(i) G is an elementary group;
(ii) $\mathcal{A}(G)$ is an R-module of finite type and its elements generate the algebra $k[G]$;
(iii) G is a vector group when $p = 0$, and a product of a vector group and a finite elementary abelian p-group if $p > 0$ (note that elementary abelian p-group is a product of cyclic groups of order p).

Corollary 8.21. *Let G be an F-group. Then G is elementary unipotent if and only if one of the following equivalent conditions hold:*
(i) $\mathcal{A}(G)(F)$ generate $F[G]$;
(ii) G is F-isomorphic to a closed subgroup of some $\mathbf{G}_a^n$.

Corollary 8.22 (Classification of 1-dimensional linear algebraic groups)**.** *Let G be a connected linear algebraic group of dimension 1. Then $G \cong \mathbf{G}_m$ or $G \cong \mathbf{G}_a$.*

Proof. We already know that G must be commutative, and $G = G_s$ or $G = G_u$.

If $G = G_s$, then G is diagonizable, and by connectedness, it is a torus of dimension 1, i.e., $G \cong \mathbf{G}_m$.

If $G = G_u$, then we have an elementary unipotent group, and by (iii) of Theorem 8.20, $G \cong \mathbf{G}_a$ because it is connected. □

9 Derivations and Differentials (10/14)

Derivations and Tangent Spaces of Varieties

Definition 9.1. Let R be a commutative ring with unit and let A be an R-algebra. Also, let M be a left A-module. An R-derivation of A in M is an R-linear map $D : A \to M$ such that

$$D(ab) = a \cdot D(b) + b \cdot D(a), \quad \forall a, b \in A.$$

Note that $D(1) = 0$ because $D(1) = D(1 \cdot 1) = 1 \cdot D(1) + 1 \cdot D(1) = 2D(1)$. So $D(r) = rD(1) = 0$ for all $r \in R$. Also, $\mathrm{Der}_R(A, M)$ becomes a left A-module via

$$(D + D')(a) = D(a) + D'(a),$$

$$(bD)(a) = bD(a), \forall b \in A.$$

$\mathrm{Der}_R(A, A)$ is the derivations of the R-algebra A. If $\varphi : A \to B$ is a homomorphism of R-algebras and N is a left B-module, then N becomes an A-module via $a \cdot n = \varphi(a)n$ and we get a homomorphism of A-modules

$$\begin{aligned} \varphi_0 : \mathrm{Der}_R(B, N) &\to \mathrm{Der}_R(A, N) \\ D &\mapsto D \circ \varphi \end{aligned}$$

because

$$\begin{aligned} (D \circ \varphi)(a_1 a_2) &= D(\varphi(a_1)\varphi(a_2)) \\ &= \varphi(a_1)D(\varphi(a_2)) + \varphi(a_2)D(\varphi(a_1)) \\ &= a_1 \cdot D(\varphi(a_2)) + a_2 \cdot D(\varphi(a_1)) \end{aligned}$$

and so $D \circ \varphi \in \mathrm{Der}_R(A, N)$. The fact that φ_0 is indeed a module homomorphism now follows formally.

Next, we claim that $\ker(\varphi_0) = \mathrm{Der}_A(B, N)$. To see this, if $D \in \ker(\varphi_0)$, then $D(a \cdot b) = D(\varphi(a)b) = \varphi(a)D(b) + bD(\varphi(a)) = \varphi(a)D(b) + b\varphi_0(D)(a) = \varphi(a)D(b) = a \cdot D(b)$, so $D \in \mathrm{Der}_A(B, N)$. On the other hand, if $D \in \mathrm{Der}_A(B, N)$, then $D(a) = 0$ for all $a \in A$, so $D(\varphi(a)) = 0$ for all $a \in A$, so $D \circ \varphi(a) = 0$ for all $a \in A$, then $\varphi_0(D) = D \circ \varphi = 0$, thus $D \in \ker(\varphi_0)$. Therefore, we get an exact sequence

$$1 \longrightarrow \mathrm{Der}_A(B, N) \to \mathrm{Der}_R(B, N) \xrightarrow{\varphi_0} \mathrm{Der}_R(A, N).$$

Review of Basics of Lie Algebras

Let k be an algebraically closed field (of any characteristic). For our purposes, a *Lie algebra* $\mathfrak{g}$ over k is a subspace of an associative k-algebra which is closed under the bracket operation

$$[x, y] := xy - yx.$$

The *adjoint representation* (of Lie algebras) is defined via

$$\begin{aligned} \mathrm{ad} : \mathfrak{g} &\to \mathrm{End}(\mathfrak{g}) \\ (\mathrm{ad}\ x)(y) &= [x, y]. \end{aligned}$$

Example 9.2. $\mathfrak{g} = \mathfrak{gl}(n, k) = M_n(k) = \{n \times n \text{ matrices with entries in } k\}$.

Example 9.3. If A is an arbitrary commutative k-algebra, then the space $\mathcal{D} = \mathrm{Der}_k(A, A)$ has a Lie algebra structure with the Lie bracket given by

$$[D, D'] = D \circ D' - D' \circ D, \quad \forall D, D' \in \mathcal{D}.$$

We need to check that $[D, D']$ is again a derivation in $\mathcal{D}$. Note

$$\begin{aligned} [D, D'](ab) &= D \circ D'(ab) - D' \circ D(ab) \\ &= D(aD'(b) + bD'(a)) - D'(aD(b) + bD(a)) \\ &= aD \circ D'(b) + D(a)D'(b) + bD \circ D'(a) + D'(a)D(b) \\ &\quad - aD' \circ D(b) - D'(a)D(b) - bD' \circ D(a) - D(a)D'(b) \\ &= a(D \circ D'(b) - D' \circ D(b)) + b(D \circ D'(a) - D' \circ D(a)) \\ &= a[D, D'](b) + b[D, D'](a), \end{aligned}$$

so $[D, D'] \in \mathcal{D}$.

Example 9.4. Fix a prime p. We say a Lie algebra $\mathfrak{g}$ is a *p-Lie algebra* (or a *restricted Lie algebra*) if $\mathfrak{g}$ has a p-operation $X \mapsto X^{[p]}$, $X \in \mathfrak{g}$, such that for $X, X' \in \mathfrak{g}$, $a \in k$, we have
(a) $(aD)^{[p]} = a^p D^{[p]}$;
(b) $\mathrm{ad}\ (D^{[p]}) = (\mathrm{ad}\ D)^{[p]}$;
(c) (Jacobson's formula) $(D + D')^{[p]} = D^{[p]} + D'^{[p]} + \sum_{i=1}^{p-1} \frac{s_i(D, D')}{i}$ where $s_i(D, D')$ is the coefficient of a^i in $\mathrm{ad}\ (aD + D')^{p-1}(D')$.

Example 9.5. If $p = \mathrm{char}(k) > 0$, $\mathcal{D} = \mathrm{Der}_k(A, A)$ is a p-Lie algebra with the operation

$$D^{[p]} := D^p = D \circ D \circ \cdots \circ D.$$

One checks that (a)-(c) holds for $\mathcal{D}$. Using the fact that if $p = \mathrm{char}(k) > 0$, $pD = 0$ for all $D \in \mathcal{D}$, they reduce to straightforward, but tedious calculations.

The main example for us will be the "tangent space" at e to an algebraic group. There is a general algebraic construction of tangent spaces of algebraic varieties and for linear algebraic groups we have a way to identify T_eG with "left invariant derivations".

Tangent Spaces of an Algebraic Group

(Heuristic)

Let $X \subset \mathbf{A}^2$ be an irreducible curve defined by a single polynomial equation $f(T_1, T_2) = 0$. Tangent at $x = (x_1, x_2)$ is defined as the solutions to the linear equation

$$\frac{\partial f}{\partial T_1}(x)(T_1 - x_1) + \frac{\partial f}{\partial T_2}(x)(T_2 - x_2) = 0.$$

Unless both partials vanish, the solution set is a line through $x = (x_1, x_2)$.

More generally, let $X \subset \mathbf{A}^n$ be a closed subvariety of $\mathbf{A}^n$. Write $k[X] = k[T_1, \cdots, T_n]/I$ where I is the ideal of polynomial functions vanishing on X. Let $I = (f_1, \cdots, f_s)$. For $x \in X$, let L be a line in $\mathbf{A}^n$ through x. Then $L = \{x + tv | t \in k\}$ for a direction vector $v = (v_1, \cdots, v_n)$. $L \cap X$ is the solution of the system of equations $f_i(x + tv) = 0$, $1 \leq i \leq s$ (and of course, $t = 0$ is a solution). Writing D_i for the partial derivation with respect to T_i in $k[T_1, \cdots, T_n]$, we have

$$f_i(x + tv) = t \sum_{j=1}^{n} v_j (D_j f_i)(x) + \text{ terms of degree in } t \text{ higher than 1.}$$

Now $t = 0$ is a "multiple root" of the system of equations if and only if $\sum_{j=1}^{n} v_j (D_j f_i)(x) = 0, 1 \leq i \leq s$. If this holds, we call L a tangent line and v a tangent vector of X in x.

Write $D' = \sum_{j=1}^{n} v_j D_j$. Then D' is a k-derivation of $k[T_1, \cdots, T_n]$, and the system of equations simply says $D' f_i(x) = 0$ for $1 \leq i \leq s$. Let M_x be the maximal ideal in $k[T]$ of functions vanishing at x. Then $D'T \subset M_x$. Consider the diagram

$$\begin{array}{ccc} k[T] & \longrightarrow & k \cong k[X]/M_x \cong k_x \\ \downarrow & \nearrow_{D} & \\ k[X] = k[T]/I & & \end{array}$$

Viewing k as a $k[X] - module\ k_x$ via the above homomorphism $f \mapsto f(x)$, it turns out that $D \in \mathrm{Der}_k(k[X], k_x)$. Conversely, any $D \in \mathrm{Der}_k(k[X], k_x)$ can be obtained this way from a derivation D' of $k[T]$ with $D'T \subset M_x$. We conclude that

$$\{ \substack{\text{tangent vectors } v \text{ such that the system} \\ f_i(x+tv) = 0,\ 1 \leq i \leq s, \text{ has a "multiple root" } t=0} \} \overset{\text{bijection}}{\longleftrightarrow} \mathrm{Der}_k(k[X], k_x).$$

Here is a summary of the formal definition of tangent space. First, let X be an affine algebraic variety, $x \in X$, and define

$$T_x X := \text{ the } k\text{-vector space } \mathrm{Der}_k(k[X], k_x).$$

We observe that:

(1) A morphism $\varphi : X \to Y$ of affine algebraic varieties with $\varphi^* : k[Y] \to k[X]$, the corresponding homomorphism of k-algebras, gives rise to $\varphi_0^* : \mathrm{Der}_k(k[X], k_x) \to \mathrm{Der}_k(k[Y], k_{\varphi(x)})$, i.e., we get a "differential of φ at x" $d\varphi_x : T_xX \to T_{\varphi(x)}Y$.

(2) If $X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z$ are morphisms of affine varieties, then $d(\psi \circ \varphi)_x = d\psi_{\varphi(x)} \circ d_{\varphi_x}$.

(3) If φ is an isomorphism of affine varieties, then $d\varphi_x$ is also an isomorphism of k-vector spaces. In fact, if φ is an isomorphism of X onto an affine open subvariety of Y, then $d\varphi_x$ is an isomorphism of T_xX onto $T_{\varphi(x)}Y$.

(4) $d(\mathrm{id})_x = \mathrm{id}$.

(5) Here are two more equivalent definitions of T_xX:

(5)-i Let $M_x \subset k[X]$ be the maximal ideal of functions vanishing at x. If $D \in T_xX$, then D maps M_x^2 to 0, so it defines a linear map

$$\lambda(D) : M_x/M_x^2 \to k.$$

In fact, $\lambda : T_xX \to$ dual of M_x/M_x^2 is an isomorphism.

(5)-ii Recall that $\mathcal{O}_x =$ ring of regular functions at x. It is a k-algebra with a maximal ideal $\mathcal{M}_x :=$ regular functions vanishing at x. Then $\mathcal{O}_x/\mathcal{M}_x \cong k$ and we may view k as an $\mathcal{O}_x$-module. Recall that there is an algebraic homomorphism

$$\begin{aligned} k[X] &\to \mathcal{O}_x \\ f &\mapsto f/1 \end{aligned}$$

which induces a linear map $\alpha_0 : \mathrm{Der}_k(\mathcal{O}_x, k) \to \mathrm{Der}_k(k[X], k_x)$. In fact, α_0 is a bijection.

(6) Let X be an affine F-variety and $x \in X(F)$. Then the point x defines an algebraic homomorphism $F[X] \to F$ which makes F into an $F[X]$-module F_x. We then define (a vector space over F)

$$T_xX(F) := \mathrm{Der}_F(F[X], F_x).$$

We have a canonical isomorphism $k \otimes_F T_xX(F) \cong T_xX$.

(7) Both notions in (5) and (6) generalize to arbitrary (not necessarily affine) varieties.

Definition 9.6. Let X be an algebraic variety. We say $x \in X$ is a *simple point* or X *is smooth at* x, or X *is non-singular at* x if $\dim T_xX = \dim X$.

(8) (algebraic differential) Let R be a commutative ring with 1, A a commutative R-algebra. Denote by $m : A \otimes_R A \to A$ the product homomorphism (i.e, $m(a \otimes b) = ab$) and let $I = \ker m$. Then I is an ideal of $A \otimes_R A$ generated by elements $a \otimes 1 - 1 \otimes a$, $a \in A$. The quotient algebra $(A \otimes A)/I$ is isomorphic to A (as R-algebras). The *module of differentials* of the R-algebra A is defined as

$$\Omega_{A/R} := I/I^2.$$

A priori, this is an $A \otimes A$-module, but it is annihilated by I, so we can and will view $\Omega_{A/R}$ as an A-module. Define

$$da = d_{A/R}a := \text{image of } (a \otimes 1 - 1 \otimes a) \text{ in } \Omega_{A/R}.$$

It's easy to check that d is in fact an R-derivation of A in $\Omega_{A/R}$, i.e., $d \in \mathrm{Der}_R(A, \Omega_{A/R})$, and da's generate the A-module $\Omega_{A/R}$.

There are two basic results here.

Let X be an irreducible affine algebraic variety over k. Put $\Omega_X = \Omega_{k[X]/k}$. If $x \in X$, then $T_x X \cong \mathrm{Hom}(\Omega_X, k_x)$. But for any $k[X]$-module M, we have

$$\mathrm{Hom}_{k[X]}(M, k_x) \cong \mathrm{Hom}_k(M(x), k),$$

where $M(x) := M/M_x M$. Hence $T_x X \cong \mathrm{Hom}(\Omega_X, k)$. This allows for the following:

$$(T_x X)^* := \text{“cotangent space”} = \text{dual vector space of the tangent space}$$

can be identified with $\Omega_X(x) = \Omega_X / M_x \Omega_x$.

Theorem 9.7. *Let X be an irreducible variety of dimention e.*
(i) If x is a simple point of X, there is an affine open neighborhood U of x such that Ω_U is a free $k[U]$-module with a bases $(dg_1, \cdots, dg_e)$ for some suitable $g_i \in k[U]$.
(ii) The simple points of X form a non-empty open subset of X.
(iii) For any $x \in X$, we have $\dim T_x X \geq e$.

Definition 9.8. A morphism $\varphi : X \to Y$ of irreducible varieties is called *dominant* if $\varphi(X)$ is dense in Y.

Recall from algebraic geometry that φ^* is injective $\Leftrightarrow$ $\varphi(X)$ is dense in Y. So if φ is dominant, then there is an injection of the quotient fields $k(Y) \to k(X)$. So we may view $k(X)$ as a field extension of $k(Y)$. We say φ is *separable* if this extension is separably generated.

Theorem 9.9. *Let $\varphi : X \to Y$ be a homomorphism of irreducible varieties.*
(i) Assume there is a simple point $x \in X$ such that $\varphi(x)$ is a simple point of Y and $d\varphi_x$ is surjective. Then φ is dominant and separable.
(ii) Assume that φ is dominant and separable, then the points $x \in X$ as in (i) form a non-empty open subset of X.

We may apply previous results to homogeneous spaces.

Theorem 9.10. *Let G be a connected algebraic group.*
(i) Let X be a homogeneous space for G. Then X is irreducible and smooth. In particular, G is smooth.
(ii) Let $\varphi : X \to Y$ to be a G-morphism of homogeneous spaces. Then φ is separable $\iff$ $d\varphi_x$ is surjective for some $x \in X$. If this is the case, then $d\varphi_x$ is surjective for all $x \in X$.
(iii) Let $\varphi : G \to G'$ be a surjective homomorphism of algebraic groups. Then φ is separable $\iff$ $d\varphi_e$ is surjective.

10 The Lie Algebra of a Linear Algebraic Group (10/21)

Let G be a linear algebraic group. Let λ and ρ be left and right translation on $A = k[G]$, so they are both representations of G. $A \otimes_k A$ can be viewed as the algebra of regular functions $k[G \times G]$. If $m : A \otimes_k A \to A$ is the multiplication map, then for $F \in k[G \times G]$, we have

$$(mF)(x) = F(x, x).$$

Let $I = \ker m$, the ideal of functions in $k[G \times G]$ vanishing on the diagonal. For $x \in G$, both automorphisms $\lambda(x) \otimes \lambda(x)$ and $\rho(x) \otimes \rho(x)$ stabilize I and I^2. This induces automorphism of $\Omega_G = I/I^2$, again denoted by $\lambda(x)$ and $\rho(x)$. Hence, we have two representations λ, ρ of G in Ω_G which are locally finite. (Recall we had a k-derivation $d : A \to \Omega_G = I/I^2$ with $da =$ image of $(a \otimes 1 - 1 \otimes a)$). Now, the derivation $d : A \to \Omega_G$ commutes with all $\lambda(x)$ and $\rho(x)$.

Fix $x \in G$. Consider $\mathrm{Int} : G \to G$ defined by $y \mapsto xyx^{-1}$ which is an automorphism of algebraic groups, fixing $e \in G$. Therefore, this induces two linear automorphisms

$$\mathrm{Ad}(x) : T_eG \to T_eG$$

and

$$(\mathrm{Ad}(x))^* : (T_eG)^* \to (T_eG)^*,$$

and we have

$$((\mathrm{Ad}(x)^* u)(X) = u(\mathrm{Ad}(x^{-1}X)), \quad u \in (T_eG)^*, X \in T_eG.$$

Recall that if $M_e \subset A$ is the maximal ideal of functions vanishing at e, then we identify $(T_eG)^*$ with M_e/M_e^2. (We saw that $\lambda : T_xX \cong$ dual of M_x/M_x^2, where $\lambda(D) : M_x/M_x^2 \to k$). If $f \in A$, denote by δf the element $f - f(e) + M_e^2$ in $(T_eG)^* = M_e/M_e^2$. For $X \in \mathrm{Der}_k(A, k_e)$, we have $(\delta f)(X) = Xf$.

Proposition 10.1. *There is an isomorphism of $k[G]$-modules*

$$\Phi : \Omega_G = I/I^2 \to k[G] \otimes_k (T_eG)^*$$

such that
(a) the diagram

$$\begin{array}{ccc}
\Omega_G & \xrightarrow{\Phi} & k[G] \otimes_k (T_eG)^* \\
{\scriptstyle \lambda(x)}\downarrow & & \downarrow{\scriptstyle \lambda(x)\otimes id} \\
\Omega_G & \xrightarrow{\Phi} & k[G] \otimes_k (T_eG)^* \\
{\scriptstyle \rho(x)}\downarrow & & \downarrow{\scriptstyle \rho(x)\otimes (Ad(x))^*} \\
\Omega_G & \xrightarrow{\Phi} & k[G] \otimes_k (T_eG)^*
\end{array}$$

is commutative, so

$$\Phi \circ \lambda(x) \circ \Phi^{-1} = \lambda(x) \otimes id, \qquad \Phi \circ \rho(x) \circ \Phi^{-1} = \lambda(x) \otimes (Ad(x))^*;$$

(b) If $f \in k[G]$ and $\Delta f = \sum_i f_i \otimes g_i$ (recall Δ is comultiplication given by $(\Delta f)(x,y) = f(xy)$), then $\Phi(df) = -\sum_i f_i \otimes \delta g_i$.

Proof. Consider the automorphism $G \times G \to G \times G$ given by $(x,y) \mapsto (x, xy)$. This defines an algebra automorphism $\psi : A \otimes A \to A \otimes A$ with $(\psi F)(x,y) = F(x,xy)$. So ψI is the ideal of functions vanishing on $G \times \{e\}$, which is $k[G] \otimes_k M_e$. Then $\psi I^2 = k[G] \otimes_k M_e^2$. So ψ induces a bijection

$$\Omega_G = I/I^2 \to k[G] \otimes_k M_e/M_e^2.$$

Also, recall that we have an isomorphism $M_e/M_e^2 \cong (T_eG)^*$. Now, let Φ be the composite of these two maps:

$$\begin{array}{ccc} \Omega_G & \longrightarrow & k[G] \otimes_k M_e/M_e^2 \\ & \overset{\Phi}{\searrow} & \downarrow \\ & & k[G] \otimes_k (T_eG)^* \end{array}$$

Then, for $x \in G$, we have

$$(\lambda(x) \otimes \mathrm{id})(\psi F)(x', y') = (\psi F)(xx', y') = F(xx', xx'y') = \psi \circ (\lambda(x) \otimes \lambda(x))(F)(x', y'),$$

and

$$\begin{aligned} ((\rho(x) \otimes \mathrm{Int}(x)) \circ \psi)(F)(x', y') &= (\psi F)(x'x^{-1}, xy'x^{-1}) = F(x'x^{-1}, x'x^{-1}xy'x^{-1}) \\ &= \psi \circ (\rho(x) \otimes \rho(x))(F)(x', y'). \end{aligned}$$

Thus

$$(\lambda(x) \otimes \mathrm{id}) \circ \psi = \psi \circ (\lambda(x) \otimes \lambda(x)), \qquad (\rho(x) \otimes \mathrm{Int}(x)) \circ \psi = \psi \circ (\rho(x) \otimes \rho(x)).$$

These formulas for ψ now give the requirements of (a) for Φ, so (a) is true.

For (b),

$$\begin{aligned} \psi(f \otimes 1 - 1 \otimes f)(x,y) &= (f \otimes 1 - 1 \otimes f)(x, xy) = f(x) - f(xy) \\ &= (\Delta f)(x, e) - (\Delta f)(x, y) \\ &= \sum_i f_i(x) g_i(e) - f_i(x) g_i(y) \\ &= \sum_i f_i(x)(g_i(e) - g_i(y)) \\ &= -\sum_i f_i(x)(\delta g_i)(y). \end{aligned}$$

Thus, $\psi(df) = -\sum_i f_i \otimes \delta g_i$. □

Let G be a linearly algebraic group and $A = k[G]$. Write $\mathcal{D} = \mathcal{D}_G = \mathrm{Der}_k(A, A)$ as last time. Recall that $\mathcal{D}$ had a Lie algebra structure with bracket $[D, D'] = D \circ D' - D' \circ D$. Then λ and ρ define representations of G in $\mathcal{D}$, and we denote by λ and ρ again. So

$$\lambda(x)D = \lambda(x) \circ D \circ \lambda(x)^{-1}, \quad \forall D \in \mathcal{D}, \forall x \in G,$$

$$\rho(x)D = \rho(x) \circ D \circ \rho(x)^{-1}, \quad \forall D \in \mathcal{D}, \forall x \in G.$$

Definition 10.2. The *Lie algebra* of G is defined as

$$L(G) := \{D \in \mathcal{D} : D \text{ commutes with all } \lambda(x), x \in G\}.$$

Here are a few remarks.
(1) $L(G)$ is a subalgebra of the Lie algebra $\mathcal{D}$.
(2) If $p = \mathrm{char}(k) > 0$, $L(G)$ is stable under the p-operation $D \mapsto D^p$.
(3) Let and right translations commute, so all $\rho(x)$ stabilize $L(G)$. We denote the linear map induced again by $\rho(x)$.
(4) There is an isomorphism of $k[G]$-modules

$$\Psi : \mathcal{D}_G \to k[G] \otimes_k T_eG$$

such that

$$\Psi \circ \lambda(x) \circ \Psi^{-1} = \lambda(x) \otimes \mathrm{id},$$

$$\Psi \circ \rho(x) \circ \Psi^{-1} = \rho(x) \otimes \mathrm{Ad}(x),$$

$$\Psi^{-1}(1 \otimes X)(f) = -\sum_i f_i(Xg_i), \quad \forall X \in T_eG.$$

(5) Let $\alpha = \alpha_G : \mathcal{D}_G \to T_eG$ be the linear map with $(\alpha_G D)(f) = (Df)(e)$. Then α induces an isomorphism of vector spaces $L(G) \cong T_eG$, and $\alpha \circ \rho(x) \circ \alpha^{-1} = \mathrm{Ad}x$, and Ad is a rational representation of G in T_eG called the "adjoint representation".
(6) As a corollary of (5), $\dim_k L(G) = \dim G$.
(7) (closed subgroup) Let H be a closed subgroup of G. Let $J \subset K[G]$ be the ideal of functions vanishing on H, so $k[H] \cong k[G]/J$. Put $\mathcal{D}_{G,H} := \{D \in \mathcal{D}_G : DJ \subset J\}$. Then $\mathcal{D}_{G,H}$ is a subalgebra of the Lie algebra $\mathcal{D}_G$ and there is an obvious homomorphism of Lie algebra

$$\psi : \mathcal{D}_{G,H} \to \mathcal{D}_H.$$

In fact, $T_eH = \{X \in T_eG : XJ = 0\}$.

Lemma 10.3. *ψ gives an isomorphism of $\mathcal{D}_{G,H} \cap L(G)$ onto $L(H)$.*

From now on, we identify the Lie algebra $L(G)$ and the tangent space T_eG via α_G so T_eG gets a Lie algebra structure. We usually write

$$\mathfrak{g} = \mathrm{Lie}(G), \mathfrak{h} = \mathrm{Lie}(H).$$

(8) If $\psi : G \to G'$ is a homomorphism of linear algebraic groups, we write $d\psi$ for the tangent map

$$d\psi : \mathfrak{g} \to \mathfrak{g}',$$

called the differential of ψ. $d\psi$ is a homomorphism of Lie algebras, compatible with the p-operation if $p = \mathrm{char}(k) > 0$.

We now add some differential formulas for later use.

(9) Let $\mu : G \times G \to G$, $\mu(x, y) = xy$, and $i : G \to G$, $i(x) = x^{-1}$ as before. Identify $L(G \times G)$ with $\mathfrak{g} \oplus \mathfrak{g}$ (this is easy to check). Then $(d\mu)_{(e,e)} : \mathfrak{g} \oplus \mathfrak{g} \to \mathfrak{g}$ is given by

$$(X, Y) \mapsto X + Y,$$

and $(di)_e : \mathfrak{g} \to \mathfrak{g}$ is given by

$$X \mapsto -X.$$

(10) (i) Let $\sigma : G \to G$ be a morphism of varieties and put $\psi(x) = (\sigma(x))x^{-1}$. Then

$$(d\psi)_e = (d\sigma)_e - 1.$$

(ii) Let $a \in G$. If $\varphi(x) = axa^{-1}x^{-1}$, then

$$(d\varphi)_e = \mathrm{Ad}(a) - 1.$$

(iii) (direct sums and tensor products) Start with a finite dimensional vector space V over k and write $\mathfrak{gl}(V)$ = Lie algebra of endomorphisms of V. Then $\mathfrak{gl}(V) \cong \mathfrak{gl}_{\dim V}$. If $\phi : G \to \mathrm{GL}(V)$ is a rational representation of G, its differential $d\phi$ is a Lie algebra homomorphism $\mathfrak{g} \to \mathfrak{gl}(V)$, i.e., a representation of $\mathfrak{g}$ in V.

Let G_1, G_2 be two linear algebraic groups and let $\phi_i : G_i \to \mathrm{GL}(V_i)$, $i = 1, 2$, be two rational representations. Let $\phi_1 \oplus \phi_2$ be the direct sum representation of $G_1 \times G_2$ in $V_1 \oplus V_2$ and let $\phi_1 \otimes \phi_2$ be the tensor product representation of $G_1 \times G_2$ in $V_1 \otimes V_2$. Identify $L(G_1 \times G_2) = \mathfrak{g}_1 \oplus \mathfrak{g}_2$. Then

$$d(\phi_1 \oplus \phi_2) = d\phi_1 \oplus d\phi_2,$$

and

$$(d(\phi_1 \otimes \phi_2))(X_1, X_2)(v_1, v_2) = (d\phi_1)(X_1)(v_1) \otimes v_2 + v_1 \otimes (d\phi_2)(X_2)(v_2).$$

Example 10.4. Let $G = \mathbf{G}_a$, $A = k[G] = K[T]$. Derivations of $k[G]$ that commute with all translations $T \to T + a$, $a \in k$ are multiplies of $X = \frac{d}{dT}$. If $p = \mathrm{char}(k) > 0$, we have $X^p = 0$. So $\mathfrak{g} = k \cdot X$ with $[X, X] = 0$.

Example 10.5. Let $G = \mathbf{G}_m$, $A = k[G] = K[T, T^{-1}]$. First, for all $a \in k^\times$, we have

$$\left(T\frac{d}{dT}\right)(\lambda(a)f)(x) = x\frac{d}{dT}f(ax) = x \cdot \frac{df}{dT}(ax) \cdot a.$$

Also,

$$\lambda(a)\left(T\frac{d}{dT}f\right)(x) = \left(T\frac{d}{dT}f\right)(ax) = ax\cdot\frac{df}{dT}(ax).$$

So $T\frac{d}{dT}$ commutes with all (left and right) translations $T \to aT$, $a \in k^\times$. (Note that in this case, a left translation is the same as a right translation). In fact, derivations of $k[G]$ commutating with translations $T \to aT$, $a \in k^\times$, are all multiplies of $T\frac{d}{dT}$. If $p > 0$, we have $X^p = X$. So $\mathfrak{g}$ = multiplies of $T\frac{d}{dT}$. So $\mathfrak{g}$ is the same as in Example 10.4, but the p-operation is different when $p > 0$.

Example 10.6. Let $G = \mathbf{GL}_n$, $k[G] = k[T_{ij}, D^{-1}]$ where $D = \det(T_{ij})$. Recall the notation $\mathfrak{gl}_n$; $[X, Y] = XY - YX$, and the usual p-th power p-operation when $p > 0$. If $X = (x_{ij}) \in \mathfrak{gl}_n$, then

$$D_X T_{ij} = -\sum_{h=1}^{n} T_{ih}x_{hj}$$

defines a derivation of $k[G]$ that commutes with all left-translations. So it lies in $L(G)$. Also, the map $X \mapsto D_X$ is injective. By equality of dimensions of Lie algebra and group, $L(G)$ consists of all of the D_X's. So we can identify $\mathfrak{g}$ and $\mathfrak{gl}_n$ (with p-th power operation). For $x \in \mathrm{GL}_n$, $X \in \mathfrak{gl}_n$, we have $\mathrm{Ad}(x)X = xXx^{-1}$.

Example 10.7. If H is a closed subgroup of $\mathbf{GL}_n$, we can view $\mathfrak{h}$ as a subalgebra of $\mathfrak{gl}_n$. Using Remark (7) on closed subgroups, $\mathfrak{h} = \mathcal{D}_{G,H} \cap \mathfrak{gl}_n$, where $\mathcal{D}_{G,H} = \{D \in \mathcal{D}_G : DJ \subset J\}$, $J \subset k[G]$ the ideal of functions vanishing on H. For example, $H = \mathrm{SL}_n$, $\mathfrak{h} = \{X \in \mathfrak{gl}_n : \mathrm{tr}(X) = 0\}$.

11 Homogeneous Spaces, Quotients of Linear Algebraic Groups (10/28)

Review of Homogeneous Spaces

Let G be an algebraic group (not necessarily linear) and let X be a homogeneous space for G. Recall that a homogeneous space for G is a G-space in which G acts transitively. Let G^0 be the identity component of G.

Theorem 11.1. *Let G be an algebraic group and let $\phi : X \to Y$ be an equivariant homomorphism of homogeneous spaces for G. Put $r = \dim X - \dim Y$.*

(i) For any variety Z, the morphism $(\phi, id) : X \times Z \to Y \times Z$ is open.

(ii) If Y' is an irreducible closed subvariety of Y and X' is an irreducible component of $\phi^{-1}Y'$, then $\dim X' = \dim Y' + r$. In particular, if $y \in Y$, then all irreducible components of $\phi^{-1}(y)$ have dimension r.

(iii) ϕ is an isomorphism $\iff$ it is bijective and for some $x \in X$, the tangent map $d\phi_x : T_xX \to T_{\phi(x)}Y$ is bijective.

Corollary 11.2. *Let $\phi : G \to G'$ be a surjective homomorphism of algebraic groups.*

(i) $\dim G = \dim G' + \dim \ker(\phi)$.

(ii) ϕ is an isomorphism $\iff$ ϕ and the tangent map $d\phi_e$ are bijective.

Proof. View G and G' as homogeneous spaces for G (via left translation for G and via $g \cdot g' := \phi(g)g'$ for G'). Apply Theorem 11.1. □

Remark 11.3. *Note that if G and G' are both linear algebraic groups, then the condition on the tangent map in (iii) in Theorem 11.1 can be rephrased as: the Lie algebra homomorphism $d\phi : \mathfrak{g} \to \mathfrak{g}'$ is bijective.*

Remark 11.4. *In (iii) in Theorem 11.1, it is not enough to check that ϕ is bijective, we also need that $d\phi_e$ is bijejctive. For example, consider $\phi : \mathbf{G}_m \to \mathbf{G}_m$ defined by $x \mapsto x^n$ with $char(k) = p > 0$, and $n = p^f$, then ϕ is a bijection (in fact, an isomorphism of abstract groups), but not an isomorphism of algebraic groups.*

Quotients of Linear Algebraic Groups

Let G be a linear algebraic group, H a closed subgroup with respective Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$. Let $F \subset k$ be a subfield. Assume that G is an F-group, and H is an F-subgroup. Our goal is to (1) construct a quotient variety G/H; (2) when H is closed and normal, G/H will be an affine variety, hence a linear algebraic group.

Theorem 11.5 (Chevalley)**.** *There exists a rational representation $\phi : G \to GL(V)$ over F, where V is a finite dimensional subspace of $k[G]$ and there is a nonzero $v \in V(F)$ such that*

$$H = \{x \in G : (\phi x)v \in kv\}, \qquad \mathfrak{h} = \{X \in \mathfrak{g} : (d\phi X)v \in kv\}.$$

Corollary 11.6. *There is a quasi-projective homogeneous space X for G together with a point $x \in X$ such that*
(a) The isotropy group of x in G is H;
(b) The morphism $\varphi : G \to X$ defined by $g \mapsto g \cdot x$ defines an separable morphism $G^0 \to \varphi G^0$;
(c) The fibres of φ are cosets $gH, g \in G$.

Recall that a quasi-projective variety is an open subvariety of a projective variety.

Proof of Corollary 11.6. We skip proof for (b), and prove (a) and (c). Take V and v as in Theorem 11.5 and consider the projective space $\mathbf{P}(V)$. Denote by x the point in $\mathbf{P}(V)$ determined by the line kv. Consider $\pi : V - \{0\} \to \mathbf{P}(V)$ sending each non-zero vector to the line through it. Now, G acts on $\mathbf{P}(V)$ by $g \cdot \pi(v) = \pi(\phi(g) \cdot v)$, with ϕ as in Theorem 11.5. Let X be the G-orbit of x. Recall that $X = G \cdot x$ is open in its closure, so X is quasi-projective. Now

$$\begin{aligned} G_x &= \{g \in G : g \cdot x = x\} \\ &= \{g \in G : \pi(\phi(g) \cdot v) = \pi(v)\} \\ &= \{g \in G : \phi(g)v \in kv\} = H \quad \text{(by Theorem 11.5).} \end{aligned}$$

This proves (a).

For $y = g \cdot x \in X$, $g \in G$, its fibre is

$$\begin{aligned} \varphi^{-1}(y) &= \{\gamma \in G : \gamma \cdot x = y\} \\ &= \{\gamma \in G : \gamma \cdot x = g \cdot x\} \\ &= \{\gamma \in G : g^{-1}\gamma \in H\} \\ &= \{\gamma \in G : \gamma \in gH\} \\ &= gH. \end{aligned}$$

This proves (c). □

Now we prove Theorem 11.5.

Proof of Chevalley's Theorem, Theorem 11.5. It follows from combining the following two lemmas.

Lemma 11.7. *There exists a finite dimensional subspace V of $k[G]$ together with a subspace W of V such that*
(a) V is stable under all right translations $\rho(x), x \in G$;
(b) We have

$$\begin{aligned} H &= \{x \in G : \rho(x)W = W\} \\ \mathfrak{h} &= \{X \in \mathfrak{g} : X \cdot W \subset W\}. \end{aligned}$$

(c) V is defined over F and W is an F-subspace of V.

Proof of Lemma 11.7. Let $I \in k[G]$ be the ideal of functions vanishing on H and let V be a finite dimensional $\rho(G)$-stable subspace of $k[G]$ that is defined over F and contains a set of generators $(f_1, \cdots, f_r)$ of I which lie in $F[G]$. Set $W = V \cap I$. Then (a) is automatic, and (c) is clear.

For (b), if $x \in H$, then $\rho(x)W = W$ (recall by Lemma 5.16, we had $H = \{g \in G : \lambda(g)\mathcal{I}_G(H) = \mathcal{I}_G(H)\} = \{g \in G : \rho(g)\mathcal{I}_G(H) = \mathcal{I}_G(H)\}$). On the other hand, if $\rho(W) = W$, then $\rho(x)f_i \in I$ for all $1 \leq i \leq r$. So $\rho(x)I \subset I$. By the same reason (Lemma 5.16) we must have $x \in H$. For $\langle$, similar argument works (recall we had $\mathcal{D}_{G,H} = \{D \in \mathcal{D}_G : DI \subset I\} \cap L(G) = L(H)$). □

Now let V be an arbitrary finite dimension vector space, W subspace of dimension d. Then the d-exterior power of V $\wedge^d V$ contains the one dimension subspace $L = \wedge^d W$. Let ϕ be the canonical representation of $\mathrm{GL}(V)$ in $\wedge^d V$. Then

$$(d\phi)(X)(v_1 \wedge v_2 \cdots \wedge v_d) = \sum_{i=1}^{d} v_1 \wedge \cdots \wedge (d\phi)(x)v_i \wedge \cdots \wedge v_d.$$

Lemma 11.8. *(i) Let $x \in GL(V)$. We have $x \cdot W = W \iff (\phi x)L = L$.*
(ii) Let $X \in \mathfrak{gl}(V)$. We have $X \cdot W \subset W \iff (d\phi)(X)L \subset L$.

Proof of Lemma 11.8. The direction ($\Longrightarrow$) is clear for both (i) and (ii).

(i) ($\Longleftarrow$) Choose a basis $(v_1, \cdots, v_n)$ of V such that $(v_1, \cdots, v_d)$ is a basis of W. Then $v_{i_1} \wedge \cdots \wedge v_{i_d}$ with $i_1 < i_2 < \cdots < i_d$ form a basis for $\wedge^d V$ and $v_1 \wedge \cdots \wedge v_d$ is a basis for L. Let $x \in \mathrm{GL}(V)$. We may also assume that $v_{l+1}, \cdots, v_{l+d}$ is a basis for $x \cdot W$ for some l. Put $e = v_1 \wedge \cdots \wedge v_d$ and $f = v_{l+1} \wedge \cdots \wedge v_{l+d}$. Then $(\phi(x))e$ is a multiple of f. If $l > 0$, then e and f are linearly independent and $\phi(x)$ does not stabilize L. So $l = 0$, i.e., $x \cdot W = W$.

(ii) ($\Longleftarrow$) If $X \in \mathfrak{gl}(V)$, then

$$(d\phi)(X)e = \sum_{i=1}^{d} v_1 \wedge \cdots \wedge X \cdot v_i \wedge \cdots \wedge v_d.$$

Write $Xv_i = \sum_{j=1}^{n} a_{ij}v_j$. Then

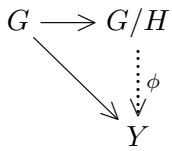
$$(d\phi)(X)e = \sum_{i=1}^{d} \sum_{j=1}^{n} a_{ij} v_1 \wedge \cdots \wedge v_j \wedge \cdots \wedge v_d$$

If $a_{ij} \neq 0$ for $i \leq d$ and $j > d$, then L is not mapped into itself. So $a_{ij} = 0$ for $i \leq d$ and $j > d$. So $X \cdot W \subset W$. □

Thus, we have finished the proof of Theorem 11.5. □

Construction of Quotient

A *quotient of G by H over F* is a pair $(G/H, a)$ of a homogeneous space G/H of G over F together with a point $a \in G/H(F)$ such that the following universal property holds: for any pair (Y, b) of a G-space Y for G over F and a point $b \in Y(F)$ whose isotropy group contains H, there exists a unique equivariant F-morphism $\phi : G/H \to Y$ such that $\phi(a) = b$.



Theorem 11.9. *A quotient $(G/H, a)$ over F exists and is unique up to a G-isomorphism. In fact, if X and x are as earlier, then (X, x) is such a quotient.*

We prove this in the case $F = k$. The proof over general F is similar, but uses some information about the ground fields, which is done in Chapter 11 and 12 of Springer's Linear Algebraic Groups.

Proof of Theorem 11.9 over k, i.e., $F = k$. The uniqueness is trivial given the universal property. So we prove existence. The proof of existence has two steps: in step 1, we define $(G/H, a)$ in the category of ringed spaces, and in step 2, we show that it is isomorphic as a ringed space, to the pair (X, x) as before.

Step 1. G/H has its points the cosets gH, and $a = H$. Let $\pi : G \to G/H$ be the canonical map. Declare $U \subset G/H$ open if $\pi^{-1}(U)$ is open in G (called the quotient topology). Then we get a topology space G/H such that the map π is an open map. We define a sheaf $\mathcal{O}$ of k-valued functions on G/H as follows: if $U \subset G/H$ is open, then set

$$\mathcal{O}(U) = \{f : U \to k : f \circ \pi \text{ is a regular function on } \pi^{-1}(U)\}.$$

It's easy to check that $\mathcal{O}(U)$ is a ring of functions, and $\mathcal{O}$ defines a sheaf. G acts transitively on G/H by left translations and for $x \in G$, the map $gH \mapsto xgH$ defines an isomorphism of ringed spaces $(G/H, \mathcal{O})$. Now, if (Y, b) is as in the universal property, then there exists a unique G-morphism of ringed space $\phi : G/H \to Y$ with $\phi(a) = b$. Just take $\phi(gH) = g \cdot b$.

Step 2. Let X, x and $\psi : G \to X$ be as before. In particular, we have a G-morphism of ringed spaces $\phi : G/H \to X$ defined by $gH \mapsto g \cdot x$. We prove that this is an isomorphism of ringed spaces, which will imply that as an algebraic variety, the ringed space G/H satisfies the theorem.

First, by Corollary 11.6, we know the fibres of φ are the cosets gH, so ϕ is a continuous bijection. If $U \subset G/H$ is open, then $\phi(U) = \psi(\pi^{-1}U)$ is open, so by Theorem 11.1 we conclude that ϕ is a homeomorphism of topological spaces.

Next, we show that ϕ is an isomorphism of ringed spaces. We need to show that if $U \subset X$ is open, then the homomorphism of k-algebras $\mathcal{O}_X(U) \to \mathcal{O}(\phi^{-1}(U))$ defined by

ϕ is an isomorphism of k-algebras. By definition of $\mathcal{O}$, this means that for any regular function f on $V = \psi^{-1}(U)$ such that $f(gh) = f(g), g \in V, h \in H$, there is a unique regular function F on U such that $F(\psi g) = f(g)$ for all $g \in V$. Without loss of generality, we may assume G is connected (because of the following lemma).

Lemma 11.10. *Let G be an algebraic group and let X be a homogeneous space for G. Then*
(i) each irreducible component of X is a homogeneous space for G^0;
(ii) the components of X are open and closed and X is their disjoint union.

Let $\Gamma = \{(g, f(g)) : g \in G\} \subset V \times \mathbf{A}^1$ be the graph of f and put $\Gamma' = (\psi, \mathrm{id})\Gamma$, so $\Gamma' \subset U \times \mathbf{A}^1$. Since Γ is closed in $V \times \mathbf{A}^1$, by Theorem 11.1, we have

$$(\psi, \mathrm{id})(V \times \mathbf{A}^1 - \Gamma) = U \times \mathbf{A}^1 - \Gamma' \text{ is open in } U \times \mathbf{A}^1.$$

So Γ' is closed in $U \times \mathbf{A}^1$. Let $\lambda : \Gamma' \to U$ be the morphism induced by projection onto the first component. Then it follows from definitions that λ is bijective and by Corollary 11.6, λ is separable. In fact, by results from algebraic geometry, λ is an isomorphism. This implies that there is a regular function F on U such that $\Gamma' = \{(u, F(u)) : u \in U\}$ which is what we want. □

Corollary 11.11. *(i) G/H is a quasi-projective variety of dimension* $\dim(G) - \dim(H)$.
(ii) If G is connected, the morphism $G \to G/H$ via $g \mapsto g \cdot a$ is separable.

Proof. This follows from Corollary 11.6. □

Proposition 11.12 (normal subgroups)**.** *Let G be a linear algebraic group and H a normal closed subgroup of G. Then*
(i) G/H is an affine variety;
(ii) with the usual group structure, G/H is a linear algebraic group.

12 Parabolic and Borel Subgroups (11/4)

Review of Complete Varieties

Definition 12.1. An algebraic variety X is called *complete* if for any variety Y, the projection morphism $X \times Y \to Y$ is closed, i.e., it maps closed sets to closed sets.

This is analogous to the notion of "compactness" in topology.

Example 12.2. $X = \mathbf{A}^1$ is not complete. Take $Y = \mathbf{A}^1$ and consider $\phi : \mathbf{A}^1 \times \mathbf{A}^1 \to \mathbf{A}^1$ given by $(x, y) \mapsto y$. Now $C = \{(x, y) \in \mathbf{A}^1 \times \mathbf{A}^1 : xy = 1\}$ is closed in $\mathbf{A}^2$, but $\varphi(C)$ is open in $\mathbf{A}^1$.

Example 12.3. $X = \mathbf{P}^1$ is complete.

Theorem 12.4. *A projectivve variety is complete.*

Proposition 12.5. *Let X be complete.*
(i) A closed subvariety of X is complete.
(ii) If Y is complete, then so is $X \times Y$.
(iii) If $\phi : X \to Y$ is a morphism, then $\phi(X)$ is closed and complete.
(iv) If X is a subvariety of Y, then X is closed in Y.
(v) If X is irreducible, then any regular function on X is constant.
(vi) If X is affine, then X is finite.

Definition 12.6. A closed subgroup P of G is called *parabolic* if the quotient variety G/P is complete.

Facts on Parabolics

Here are a few facts on parabolics.

(1) If X, Y are homogeneous spaces for G and $\phi : X \to Y$ is a bijection of G-morphism, then X is complete $\iff$ Y is complete.

Proof. Recall that given X and Y as above, for any variety Z, the map $(\phi, \mathrm{id}) : X \times Z \to Y \times Z$ is a homeomorphism of topological spaces. Now $X \times Z \to Z$ is closed $\iff$ $Y \times Z \to Z$ is closed. □

(2) P is parabolic in $G \Rightarrow G/P$ is a projective variety.

Proof. Recall that G/P is a quasi-projective variety, i.e., an open subvariety of a projective variety. Now by part (iv) of Proposition 12.5, G/P is closed, so it is a projective variety. □

(3) Let P be a parabolic in G, Q be a parabolic in P, then Q is a parabolic in G.

Proof. We need to show that for any variety X, the projection map $G/Q \times X \to X$ is closed. Consider

$$P \times G \times X \xrightarrow{\alpha} G \times X \xrightarrow{\beta} G/Q \times X \xrightarrow{\mathrm{pr}_2} X$$

$$(p, g, x) \longrightarrow (gp, x)$$

If C is closed in $G/Q \times X$, then $A = \beta^{-1}(C) \subset G \times X$ is closed with the property that if $(g, x) \in A$, then $(gQ, x) \subset A$. We need to show $A' = \mathrm{pr}_2(\beta(A))$ is closed in X. Now $\alpha^{-1}(A) = \{(p, g, x) \in P \times G \times X : (gp, x) \in A\}$ is closed in $P \times G \times X$. Since P/Q is complete, $P/Q \times (G \times X) \to G \times X$ is closed, so the image of $\alpha^{-1}(A)$ under this map, i.e., $\bigcup_{(g,x)\in A}(gp, x)$ is closed in $G \times X$. Now completeness of G/P implies that the projection of this set is closed in X, but that is just A'. □

(4) (i) If P is parabolic in G and Q is a closed subgroup of G containing P, then Q is parabolic in G. (ii) P is parabolic in $G \iff P^0$ is parabolic in G^0.

(5) A connected linear algebraic group G contains no proper parabolic subgroups $\iff$ G is solvable.

Theorem 12.7 (Borel's Fixed Point Theorem)**.** *Let G be a connected solvable linear algebraic group, and let X be a complete G-variety. Then there exists a point $x \in X$ that is fixed by all elements of G.*

Proof. Recall that G has a closed orbit in X. The isotropy group of a point in that orbit is parabolic. By Fact (5) above, this group must be all of G, i.e., we get a fixed point. □

Borel Subgroups

Definition 12.8. A *Borel subgroup* of G is a closed, connected, solvable subgroup of G, which is maximal for these properties.

Note that Borel subgroups always exist, as we can see by taking the maximal dimension.

Theorem 12.9. *(i) A closed subgroup of G is parabolic iff it contains a Borel.*
(ii) A Borel subgroup is parabolic.
(iii) Any two Borel subgroups in G are conjugate.

Proof. (i) By Fact (4)(ii) above, we may assume G is connected. Let B be a Borel and let P be any parabolic. Now B acts on the complete variety G/P and by Borel's Fixed Point Theorem, there exists $gP \in G/P$ such that $bgP = gP$ for all $b \in B$. This implies that $g^{-1}bg \in P$ for all $b \in B$. So P contains a conjugate of B, which is also a Borel. This proves $\Rightarrow$. $\Leftarrow$ will follow if we prove (ii) by Fact (4)(1) above.

(ii) If G is solvable, then there is no proper parabolic and (ii) is obvious. Now assume G is non-solvable, so there is a proper parabolic P. By what we already saw, we may assume $B \subset P$. By induction on $\dim G$, we may assume B is parabolic in P. Now Fact (3) implies B is parabolic in G.

(iii) If B, B' are Borel, then B' is conjugate to a subgroup of B and B is conjugate to a subgroup of B'. Hence $\dim B = \dim B'$. So B is conjugate to B'. □

Corollary 12.10. *If G is connected, then we have $C(G)^0 \subset C(B) \subset C(G)$ for the centers.*

Proof. $C(G)^0$ is closed, connected, and commutative, so it lies in a Borel subgroup. Hence it lies in all Borels since Borels are conjugate. So $C(G)^0 \subset C(B)$.

Next, if $g \in C(B)$, then the morphism $G \to G$ defined by $x \mapsto gxg^{-1}x^{-1}$ induces a morphism $G/B \to G$ which must be constant because G/B is an irreducible complete variety. So $gxg^{-1}x^{-1} = e$ for all $x \in G$, so $g \in C(G)$. □

Corollary 12.11. *Let $\phi : G \to G'$ be a surjective homomorphism of linear algebraic groups. Let P be a parabolic subgroup, respectively a Borel subgroup of G. Then $\phi(P)$ is a parabolic subgroup, respectively a Borel subgroup of G.*

Proof. By part (i) of Theorem 12.9, it is enough to prove it for Borels, $B = P$. Then $\phi(B)$ is closed, connected, solvable. Moreover, the homomorphism $G/B \to G'/\phi(B)$ is surjective. By Proposition 12.5 (iii), $G'/\phi(B)$ is complete, so $\phi(B)$ is a parabolic, hence it contains a Borel of G'. Then $\phi(B)$ is a Borel by maximality. □

Connected Solvable Groups

Theorem 12.12 (Lie-Kolchin)**.** *Let G be a connected solvable closed subgroup of $\boldsymbol{GL}_n$. Then there exists $x \in \boldsymbol{GL}_n$ such that $xGx^{-1} \subset \mathbf{T}_n$ where $\mathbf{T}_n$ is the upper triangular matrices.*

Proof. Apply Borel's Fixed Point Theorem (Theorem 12.7) to G acting on $\mathbf{P}^{n-1}$ to conclude that the elements of G have a non-zero eigenvector. Now induction on n gives the theorem. □

Corollary 12.13. *Assume G is a nilpotent group. Then*
(i) the sets G_s and G_u of semisimple and unipotent elements are closed, connected subgroups and G_s is a central torus;
(ii) The product map $G_s \times G_u \to G$ is an isomorphism of algebraic groups.

Corollary 12.14. *For G connected, solvable closed as above, we have*
(i) the commutator subgroup (G, G) is closed, connected, nilpotent, normal subgroup;
(ii) the set G_u of unipotent elements is a closed, connected, nilpotent, normal subgroup of G and the quotient G/G_u is a torus.

Lemma 12.15. *Assume G is connected, solvable, linear algebraic group which is not a torus. Then there exists a closed normal subgroup N of G that is isomorphic to $\mathbf{G}_a$ and it lies in the center of G_u.*

Definition 12.16. Let G be a connected solvable linear algebraic group. A *maximal torus* of G is a subtorus that has the same dimension as $S = G/G_u$.

Theorem 12.17. *Let G be a connected solvable linear algebraic group.*
(i) Let $s \in G$ be semisimple. Then s lies in a maximal torus. In particular, maximal tori exist.
(ii) The centralizer $Z_G(s)$ of a semisimple element $s \in G$ is connected.
(iii) Two maximal tori in G are conjugate.
(iv) If T is a maximal torus, the product map $\pi : T \times G_u \to G$ is an isomorphism of varieties.

Corollary 12.18. *Let $H \subset G$ be a subgroup whose elements are semisimple.*
(i) H is contained in a maximal torus of G. In particular, a subtorus of G is contained in a maximal torus of G.
(ii) $Z_G(H)$ is connected and it is equal to $N_G(H)$.

Proof. The restriction to H of the canonical homomorphism $G \to G/G_u$ is bijective, so H is commutative. If $H \subset C(G)$, then Corollary 12.18 is clear. Otherwise, take a non-central element $s \in H$. By Theorem 12.17 (ii) , $Z_G(s)$ is connected. Also, it contains H. Now (i) and connectedness of $Z_G(H)$ in (ii) follows by induction on $\dim G$. Finally, if $x \in N_G(H)$, then for $h \in H$, $xhx^{-1}h^{-1} \in H \cap (G, G) \subset H \cap G_u = \{e\}$, so $x \in Z_G(H)$, and hence $Z_G(H) = N_G(H)$. □

Definition 12.19. Now let G be a connected linear algebraic group over k. A *maximal torus* of G is a subtorus of G that is not strictly contained in another subtorus. A *Cartan subgroup* of G is the identity component of the centralizer of a maximal torus. (We will see such centralizers are always connected.)

Example 12.20. Let $G = \mathbf{GL}_2$. $T_1 = \left\{ \begin{pmatrix} a & \\ & b \end{pmatrix} : ab \neq 0 \right\}$ is a maximal torus of G, $Z_G(T_1) = T_1$ is the Cartan subgroup of G.

Example 12.21. Let $G = \mathbf{GL}_2$. Let $T_2 = \left\{ \begin{pmatrix} p & q \\ q & p \end{pmatrix} : p^2 - q^2 \neq 0 \right\}$. Note

$$T_2 \cong D_2 = \mathbf{GL}_1^2$$
$$\begin{pmatrix} p & q \\ q & p \end{pmatrix} \mapsto (p+q, p-q).$$

So T_2 is a torus. It is actually a maximal torus, and $Z_G(T_2) = T_2$ is the Cartan subgroup of G. In fact,

$$T_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} T_1 \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}^{-1}.$$

Theorem 12.22. *Any two maximal tori in G are conjugate.*

Proof. Fix a Borel B in G. A maximal torus T, being connected and solvable, lies in some Borel. By conjugacy of Borels, T must be conjugate to some subtorus of B, which in turn must be a maximal torus in B. But for connected solvable groups, any two maximal tori are conjugate. So we get the theorem. □

Proposition 12.23. *Let T be a maximal torus of G and let $C = Z_G(T)^0$ be the corresponding subgroup.*
(i) C is nilpotent and T is its maximal torus.
(ii) There exists elements $t \in T$ lying in only finitely many conjugates of C.

Proof. We skip the proof, which uses the following Lemma 12.24. □

Lemma 12.24. *Let S be a subtorus in G. Then there exists $s \in S$ such that $Z_G(s) = Z_G(S)$.*

We will state three more theorems.

Theorem 12.25. *(i) Every element of G lies in a Borel.*
(ii) Every semisimple element of G lies in a maximal torus.
(iii) The union of Cartan subgroups of G contains a dense open subset.

The proof of Theorem 12.25 uses the following Lemma 12.26.

Lemma 12.26. *Let H be a closed subgroup of G and let $X = \cup_{x \in G} xHx^{-1}$. Then*
(i) X contains a non-empty open subset of $\overline{X}$. If X is parabolic, then $X = \overline{X}$ is closed.
(ii) Assume H has finite index in its normalizer N and that there exist elements in H that lie in only finitely many conjugates of H. Then $\overline{X} = G$.

Corollary 12.27. *If B is a Borel in G, then $C(B) = C(G)$.*

Theorem 12.28. *Let S be a subtorus of G.*
(i) $Z_G(S)$ is connected.
(ii) If B is a Borel containing S, then $Z_G(S) \cap B$ is a Borel in $Z_G(B)$.

Remark 12.29. *All Borels of $Z_G(S)$ are obtained in this way.*

We apply Theorem 12.28 to the case $S = T$, to get the following corollary.

Corollary 12.30. *Let T be a maximal torus in G.*
(i) $C = Z_G(T)$ is Cartan in G.
(ii) If B is a Borel containing T, then $B \supset C = Z_G(T)$.

Theorem 12.31. *Let B be a Borel in G. Then $N_G(B) = B$.*

Corollary 12.32. *If P is a parabolic in G, then P is connected and $N_G(P) = P$.*

Proof. Since P is a parabolic, P contains a Borel B, which lies in P^0. By conjugacy of Borels, there is some $y \in P^0$ such that $xBx^{-1} = yBy^{-1}$. So $y^{-1}xB(y^{-1}x)^{-1} = B$. So $y^{-1}x \in B \subset P^0$ by Theorem 12.31. Thus $x \in P^0$. □

Corollary 12.33. *If P, Q are two conjugate parabolics in G such that $P \cap Q$ contains a Borel B, then $P = Q$.*

Proof. Let $P = xQx^{-1}$. Then B and xBx^{-1} are two Borels in P, which must be conjugate in P, i.e., $xBx^{-1} = yBy^{-1}$ for some $y \in P$. Arguing as above, we conclude that $x \in Q$, so $P = Q$. □

Corollary 12.34. *Let T be a maximum torus in G, and let $B \supset T$ be a Borel. Then there is a bijection*

$$N_G(T)/Z_G(T) \longleftrightarrow \{\textit{Borel subgroups containing } T\}$$
$$x \mapsto xBx^{-1}.$$

Reductive Groups

Observe that if N and N' are normal subgroups of G, then so is $N \cdot N'$. Also, recall if $(G_i')_{i \in I}$ was a family of closed connected subgroups of G, then the subgroup generated by them was also closed and connected. Using these, it follows that there is a (unique) maximal, closed, connected, normal, solvable subgroup of G, namely a group with these properties of maximal dimension.

Definition 12.35. *The radical of G*, $R(G)$, is the unique maximal, closed, connected, normal, solvable subgroup of G. Similarly, *the unipotent radical of G*, $R_u(G)$, is the maximal, closed, connected, unipotent, normal subgroup of G.

Definition 12.36. G is called *semisimple* if $R(G) = \{e\}$. G is called *reductive* if $R_u(G) = \{e\}$.

For example, SL_n is semisimple, and GL_n is reductive.

13 Weyl Group, Roots, and Root Datum (11/11)

Weyl Group and Roots

Let G be a connected linear algebraic group, let T be a maximal torus in G, and let $X = X^*(T)$ be the character group of $T = \{\chi : T \to \mathbf{G}_m\}$.

Remark 13.1. *Let S be a torus and $r : S \to GL(V)$ be a rational representation. V is a direct sum of 1-dimensional S spaces. In each of these, S acts via a character. Set*

$$V_\chi = \{v \in V : r(s)v = \chi(s)v, \forall s \in S\}.$$

The character χ for which V_χ is nonzero are called the weights of S in V. V_χ is the weight space. Nonzero weights in a weight space are called weight vectors.

If $S = T$, $V = \mathfrak{g}$, $r = \mathrm{Ad}$. Then let P be the set of nonzero weights. Then P is a finite subset of X. (X viewed as a free abelian group in the additive notation.) We now do a few examples.

Example 13.2. Let $G = \mathrm{GL}_2$, $T = \left\{ t = \begin{pmatrix} a_1 & \\ & a_2 \end{pmatrix} : a_1, a_2 \neq 0 \right\}$, $\mathfrak{g} = \left\{ X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \right\} = M_2(k)$. $X \cong \mathbb{Z}^2 = \mathbb{Z}\langle e_1, e_2 \rangle$ where $e_1(t) = a_1, e_2(t) = a_2$. We have

$$\mathrm{Ad}(t) \cdot X = tXt^{-1} = \begin{pmatrix} a_1 & \\ & a_2 \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \begin{pmatrix} a_1^{-1} & \\ & a_2^{-1} \end{pmatrix} = \begin{pmatrix} x_{11} & \frac{a_1}{a_2} x_{12} \\ \frac{a_2}{a_1} x_{21} & x_{22} \end{pmatrix},$$

$$V = k \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \oplus k \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \oplus k \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \oplus k \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

where the first two factors correspond to $\chi = 0$, the third factor corresponds to $\chi = e_1 - e_2$, and the last factor corresponds to $\chi = -(e_1 - e_2)$. Moreover,

$$P = \{\pm(e_1 - e_2)\}.$$

Example 13.3. Let

$$G = \mathrm{GSp}_4 = \left\{ g \in \mathrm{GL}_4 : {}^t g J g = \mu(g) J \right\}$$

where $J = \begin{pmatrix} & & & 1 \\ & & 1 & \\ & -1 & & \\ -1 & & & \end{pmatrix}$. Then $B = \{\text{upper triangular matrices in } G\}$ is a Borel, and

$$T = \left\{ t = \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & b_2 & \\ & & & b_1 \end{pmatrix} : a_1 b_1 = a_2 b_2 = \mu(t) \right\}$$

is a maximal torus in B. We have

$$X \cong \mathbb{Z}^3 = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_0$$

where $e_1(t) = a_1$, $e_2(t) = a_2$, $e_0(t) = \mu(t)$. Also,

$$\begin{aligned} V = \mathfrak{g} =& k\left\langle \begin{pmatrix} x_1 & & & \\ & x_2 & & \\ & & y_2 & \\ & & & y_1 \end{pmatrix} : x_1 + y_1 = x_2 + y_2 \right\rangle \oplus k \begin{pmatrix} 0 & 1 & & \\ & 0 & & \\ & & 0 & -1 \\ & & & 0 \end{pmatrix} \oplus k \begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & & 0 & \\ & & -1 & 0 \end{pmatrix} \\ & \oplus k \begin{pmatrix} 0 & & & \\ & 0 & 1 & \\ & & 0 & \\ & & & 0 \end{pmatrix} \oplus k \begin{pmatrix} 0 & & & \\ & 0 & & \\ & 1 & 0 & \\ & & & 0 \end{pmatrix} \oplus k \begin{pmatrix} 0 & & 1 & \\ & 0 & & -1 \\ & & 0 & \\ & & & 0 \end{pmatrix} \oplus k \begin{pmatrix} 0 & & & \\ & 0 & & \\ 1 & & 0 & \\ & -1 & & 0 \end{pmatrix} \\ & \oplus k \begin{pmatrix} 0 & & & 1 \\ & 0 & & \\ & & 0 & \\ & & & 0 \end{pmatrix} \oplus k \begin{pmatrix} 0 & & & \\ & 0 & & \\ & & 0 & \\ 1 & & & 0 \end{pmatrix}, \end{aligned}$$

where the first factor is 3-dimensional, corresponding to $\chi = 0$, and the second factor corresponds to $\chi = e_1 - e_2$, the third factor corresponds to $\chi = -(e_1 - e_2)$, the forth factor corresponds to $\chi = 2e_2 - e_0$, the fifth factor corresponds to $\chi = -(2e_2 - e_0)$, the sixth factor corresponds to $\chi = e_1 + e_2 - e_0$, the seventh factor corresponds to $\chi = -(e_1 + e_2 - e_0)$, the eighth factor corresponds to $\chi = 2e_1 - e_0$, the the last factor corresponds to $\chi = -(2e_1 - e_0)$. Moreover,

$$P = \{\pm(e_1 - e_2), \pm(2e_2 - e_0), \pm(e_1 + e_2 - e_0), \pm(2e_1 - e_0)\}.$$

Example 13.4. Consider $S = \left\{ \begin{pmatrix} a_1 & & & \\ & 1 & & \\ & & 1 & \\ & & & a_1^{-1} \end{pmatrix} \right\} \subset T \subset \mathrm{GSp}_4$. Let $V = \mathfrak{g} = \mathrm{Lie}(\mathrm{GSp}_4)$, $r = \mathrm{Ad}|_S$. Then

$$P = \{\pm e_1, \pm 2e_1\}.$$

Remark 13.5. *Let $S \subset T$ be a subtorus. Then $Z_G(S) \subset Z_G(T) \iff S$ is not contained in any of the subgroups $\ker \alpha$ of T, $\alpha \in P$.*

Here is an example. Let $G = \mathrm{GL}_3$, $P = \{\pm(e_1 - e_2), \pm(e_1 - e_3), \pm(e_2 - e_3)\}$. If $S = \ker(e_1 - e_2) = \left\{ \begin{pmatrix} a & & \\ & a & \\ & & c \end{pmatrix} = \begin{pmatrix} aI_2 & \\ & c \end{pmatrix} \right\}$, then $Z_G(S) = \left\{ \begin{pmatrix} A & 0 \\ 0 & c \end{pmatrix} : A \text{ is } 2 \times 2 \right\}$, $T = Z_G(T)$.

For $\alpha \in P$, let $G_\alpha := Z_G((\ker \alpha)^0)$, which is a closed connected subgroup. Then Remark 13.5 means that if S is a subtorus of T with $Z_G(S) \neq Z_G(T)$, then there is $\alpha \in P$ such that $Z_G(S) \supset G_\alpha$. In fact, we have the following lemma.

Lemma 13.6. *(i) The $G_\alpha, \alpha \in P$ generate G.*
(ii) If all G_α are solvable, then G in solvable.

We skip the proof of Lemma 13.6. Here is an example:

$$G = \left\{ \begin{pmatrix} a & d & f \\ & b & e \\ & & c \end{pmatrix} \in \mathrm{GL}_3 \right\}, T = \left\{ \begin{pmatrix} a & & \\ & b & \\ & & c \end{pmatrix} \in G \right\}, P = \{e_1 - e_2, e_1 - e_3, e_2 - e_3\},$$

$$G_{e_1-e_2} = \left\{ \begin{pmatrix} a & d & \\ & b & \\ & & c \end{pmatrix} \right\}, G_{e_2-e_3} = \left\{ \begin{pmatrix} a & & \\ & b & e \\ & & c \end{pmatrix} \right\}, G_{e_1-e_3} = \left\{ \begin{pmatrix} a & & f \\ & b & \\ & & c \end{pmatrix} \right\}.$$

Recall that for H diagonalizable, we saw $N_G(H)^0 = Z_G(H)^0$ and $N_G(H)/Z_G(H)$ is finite. Now if T is a maximal torus in G, we define

$$W = W(G,T) := N_G(T)/Z_G(T),$$

which is a finite group, called the Weyl group of G relative to T. W acts faithfully as a group of automorphisms of $X = X^\times(T)$, which is a free abelian group of finite rank. We identify W with this subgroup of automorphisms of X. Let P be as before and $P' = \{\alpha \in P : G_\alpha \text{ is non-solvable}\}$. Note that for $S \subset T$ a subtorus, the Weyl group $W(Z_G(S), T)$ is a subgroup of $W(G,T)$. Also note that if $S \subset C$ is a subset of the center of G, then $G \mapsto G/S$ induces an isomorphism $W(G,T) \cong W(G/S, T/S)$. Recall that we had a bijection

$$\begin{aligned} N_G(T)/Z_G(T) &\to \{\text{Borel subgroups containing } T\} \\ x &\mapsto xBx^{-1}. \end{aligned}$$

This implies that for fixed B, we have bijections

$W \cong \{\text{Borel subgroups of } G \text{ containing } T\} \cong$ set of fixed points of T in $G/B(byleft translation)$.

Fix $\alpha \in P'$. Then the torus $S = (\ker \alpha)^0 \subset C(G_\alpha)$ and the Weyl group $W_\alpha := W(G_\alpha, T) \cong W(G_\alpha/S, T/S)$. Now $T/S \cong \mathbb{G}_m$, this implies that W_α has order ≤ 2 (because W_α can be identified with a subgroup of $\mathrm{Aut}(\mathbb{G}_m) = \{\pm 1\}$.

Proposition 13.7. *Assume G is non-solvable and $\dim T = 1$. Then*
(i) W has order 2.
(ii) If B is a Borel in G, then $\dim G/B = 1$.

Example 13.8. $G = \mathrm{SL}_2$, $T = \left\{\begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}\right\}$, $N_G(T) = \left\{\begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}, \begin{pmatrix} & b \\ -b^{-1} & \end{pmatrix}\right\}$. Then

$$W_\alpha = \{\pm 1\}, \quad B = \left\{\begin{pmatrix} a & b \\ & a^{-1} \end{pmatrix}\right\}, \quad \dim G/B = 1.$$

Fix $\alpha \in P'$. By Proposition 13.7 (i), W_α has order 2, so we can choose $n_\alpha \in N_G(T) \backslash Z_G(T)$. Let $S_\alpha = (n_\alpha \pmod{Z_G(T)}) \in W$. Recall that $X = X^*(T)$, so we can identify it as a subgroup of $V = \mathbb{R} \otimes_{\mathbb{Z}} X$. Similarly, $X^\vee = \mathrm{Hom}(X, \mathbb{Z})$ viewed as a gruop of cocharacters of T, so we can identify it with a subgroup of $V^\vee = \mathbb{R} \otimes_{\mathbb{Z}} X^\vee$. Then we obtain the induced pairing $\langle\ ,\ \rangle$ between V and $V^\vee$. Let $(\ ,\ )$ be a positive definite symmetric bilinear form on V, invariant under the action of W (such form always exist, for example, via averaging over W). Then $s_\alpha, \alpha \in P'$, is a Euclidean reflection with respect to the metric defined by $(\ ,\ )$ and $s_\alpha(x) = x - \frac{2(x,\alpha)}{(\alpha,\alpha)}\alpha$.

Lemma 13.9. *(i) There exists a unique $\alpha^\vee \in V^\vee$ with $\langle \alpha, \alpha^\vee \rangle = 2$ such that*

$$s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha, \forall x \in X.$$

(ii) If $\beta \in P'$ and $G_\beta = G_\alpha$, then $s_\beta = s_\alpha$.

Theorem 13.10. *W is generated by the s_α, $\alpha \in P'$.*

Theorem 13.10 can be proved by using induction on $\dim G$. We skip the proof.

Semisimple Groups of Rank One

We define

$$\mathrm{rank}\ G := \dim T,$$
$$\text{s.s.rank}\ G := \mathrm{rank}(G/R(G)).$$

Theorem 13.11. *Assume that G is connected, semisimple of rank 1. Then $G \cong \boldsymbol{SL}_2$ or $\boldsymbol{PSL}_2$.*

Example 13.12. Consider $G = \mathrm{SL}_2$, $T = \left\{t = \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}\right\}$, $B = \left\{\begin{pmatrix} a & b \\ & a^{-1} \end{pmatrix}\right\}$, $U = \left\{\begin{pmatrix} 1 & b \\ & 1 \end{pmatrix}\right\}$. Let $n = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$. Then

$$ntn^{-1} = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} = \begin{pmatrix} a^{-1} & \\ & a \end{pmatrix} = t^{-1},$$

$B = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2 : c = 0\right\}$, $UnB = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2 : c \neq 0\right\}$, $nUn^{-1} = \left\{\begin{pmatrix} 1 & \\ b & 1 \end{pmatrix}\right\}$, $U \cap nUn^{-1} = \left\{\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}\right\}$.

Reductive Groups of Semisimple Rank 1

Here is a general fact.

Proposition 13.13. *Let G be a connected reductive linear algebraic group.*
(i) $R(G)$ is a central torus. In fact, $R(G) = C(G)^0$.
(ii) $R(G) \cap (G,G)$ is finite.

Example 13.14. Consider $G = \mathrm{GL}_n$, then $C(G) = \left\{ \begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix} \right\}$ is connected and $C(G) = R(G)$. $(G,G) = \mathrm{SL}_n$. $R(G) \cap (G,G) = \mu_n$.

Example 13.15. Consider $G = \{(g_1, g_2) \in \mathrm{GL}_2 \times \mathrm{GL}_2 : \det(g_1) = \det(g_2)\}$. Then $C(G) = \left\{ \left(\begin{pmatrix} a & \\ & a \end{pmatrix}, \begin{pmatrix} b & \\ & b \end{pmatrix} \right) : a^2 = b^2, a \neq 0 \right\}$ is not connected, and $C(G)^0 = \left\{ \left(\begin{pmatrix} a & \\ & a \end{pmatrix}, \begin{pmatrix} a & \\ & a \end{pmatrix} \right) : a \neq 0 \right\} = R(G)$. $(G,G) = \mathrm{SL}_2 \times \mathrm{SL}_2$. The center of (G,G) is $\{(\pm I_2, \pm I_2)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $R(G) \cap (G,G) = \{(I,I), (-I,-I)\}$.

Now we assume that G is connected, reductive, and s.s. rank $G = 1$.

Let $C = R(G)$. Then G/C is s.s. of rank 1, so it is isomorphic to SL_2 or PSL_2. By Proposition 13.13, (G,G) is connected s.s. of rank 1. Let $T_1 \subset (G,G)$ be a maximal torus contained in T, so $T_1 \subset T \subset G$. Then $P = \{\pm\alpha\}$ and $\mathfrak{g} = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$ where both $\mathfrak{g}_\alpha$ and $\mathfrak{g}_{-\alpha}$ are 1-dimensional.

Lemma 13.16. *(i) There exists a homomorphism of algebraic groups $u_\alpha : \mathbf{G}_a \to G$ such that*

$$tu_\alpha(x)t^{-1} = u_\alpha(\alpha(t)x) \quad \forall t \in T, x \in X \quad \text{and} \quad \mathrm{Im}\, du_\alpha = \mathfrak{g}_\alpha.$$

If u'_α is another homomorphism of this type, then $u'_\alpha(x) = u_\alpha(a \cdot x), a \in k^\times$.
(ii) T and Im u_α generate a Borel in G with Lie algebra $\mathfrak{t} \oplus \mathfrak{g}_\alpha$.

Example 13.17. Consider $G = \mathrm{GL}_2$, $\alpha = e_1 - e_2$, $u_\alpha(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ or $u'_\alpha(x) = \begin{pmatrix} 1 & ax \\ 0 & 1 \end{pmatrix}, a \neq 0$. Let $\lambda : \mathbf{G}_m \to T$ be an isomorphism viewed as an element of the cocharacter group $X^\vee$. It turns out that

$$\pm\langle \alpha, \lambda \rangle = \begin{cases} 1 & \text{if } (G,G) = \mathrm{PSL}_2 \\ 2 & \text{if } (G,G) = \mathrm{SL}_2. \end{cases}$$

The Weyl group $W((G,G), T_1)$ has order 2. Let $n \in N_{(G,G)}(T_1)$ be a representative of the nontrivial element of W and let s_α be the corresponding reflection of $V = \mathbb{R} \otimes_{\mathbb{Z}} X$. Let $\alpha^\vee$ be the corresponding element of $\mathbb{R} \otimes_{\mathbb{Z}} X^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$. Then $s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha$ for all $x \in X$, $\alpha^\vee \in X^\vee$ and Im $\alpha^\vee = T_1$, and $n^2 = \alpha^\vee(-1)$.

Example 13.18. Consider $G = \mathrm{GL}_2$, $(G,G) = \mathrm{SL}_2$, $T_1 = \left\{ \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \right\} \subset T = \left\{ \begin{pmatrix} a & \\ & b \end{pmatrix} \right\}$, $\alpha = e_1 - e_2$. Then

$$\alpha^\vee(\lambda) = \begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix}, \quad n = n_\alpha = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}, \quad n^2 = \begin{pmatrix} -1 & \\ & -1 \end{pmatrix} = \alpha^\vee(-1).$$

Let B be the Borel of G containing T whose Lie algebra is $\mathfrak{t} \oplus \mathfrak{g}_\alpha$ as before. Let $\chi \in X$. Consider $\chi : B \to \mathbf{G}_m$ via the composition

$$B \to B/B_u \to T \xrightarrow{\chi} \mathbf{G}_m.$$

Proposition 13.19. *Let $f \in k[G]$ be a regular function on G whose restriction to (G,G) is non-constant. Assume that for $g \in G$, $b \in B$, we have $f(gb) = \chi(b)f(g)$. Then $\langle \chi, \alpha^\vee \rangle > 0$.*

Root Data

Definition 13.20. A *root datum* is a quadruple $\Psi = (X, R, X^\vee, R^\vee)$ where $X, X^\vee$ are free abelian groups of finite rank, in duality by a pairing $\langle\ ,\ \rangle : X \times X^\vee \to \mathbb{Z}$ and R and $R^\vee$ are finite subsets of X and $X^\vee$ respectively, and we are given a bijection $\alpha \mapsto \alpha^\vee$ of R onto $R^\vee$, and with

$$s_\alpha(x) := x - \langle x, \alpha^\vee \rangle \alpha, \quad \forall x \in X,$$
$$s_{\alpha^\vee}(y) := y - \langle \alpha, y \rangle \alpha^\vee, \quad \forall y \in X^\vee.$$

We have:

$$\text{(RD1)} : \alpha \in R \Rightarrow \langle \alpha, \alpha^\vee \rangle = 2,$$
$$\text{(RD2)} : \alpha \in R, s_\alpha R = R, s_{\alpha^\vee} R^\vee = R^\vee.$$

R is called the set of roots. $R^\vee$ is called the set of coroots. $W = W(\Psi) := \langle s_\alpha : \alpha \in R \rangle$ is the Weyl group.

Remark 13.21. *Oberve that:*
(i) $s_\alpha^2 = 1$ and $s_\alpha(\alpha) = -\alpha$.
(ii) $\Psi^\vee = (X^\vee, R^\vee, X, R)$ is also a root datum, called the dual root datum.
(iii) Let Q be the subgroup of X generated by R and put $V' = \mathbb{R} \otimes_{\mathbb{Z}} Q$. If $R \neq \emptyset$, then R is a root system in V'. Similarly, $R^\vee$ is a root system in the dual of V'.

Root Datum of Linear Algebraic Groups

Let G be a connected linear algebraic group. Consider $\beta \in P'$ and the group $G_\beta = Z_G((\ker \beta)^0)$. Then $H = G_\beta / R_u(G_\beta)$ is connected of s.s. rank 1. By earlier results today, there are two nontrivial characters $\pm\alpha'$ of the image of T in H, and their image is isomorphic to T, so we have two corresponding characters $\pm\alpha$ of T. Now we have $(\ker \alpha)^0 = (\ker \beta)^0$, so α is a rational multiple of β, so $\alpha \in P'$. $\{\alpha : \beta \in P'\}$ are called roots of G relative to T, or roots of (G, T).

Notation: let $R = R(G, T)$ be the set of roots. $R = \emptyset \iff G$ is solvable.

Next, we have a map $\alpha \mapsto \alpha^\vee$ of R onto a subset R' of $X^\vee$, which turns out to be bijective. The elements of $R^\vee$ are the coroots of G relative to T. These are the ingredients of a root datum and (RD1), (RD2) hold. So if G is a connected linear algebraic group with T a maximal torus in G, then we get $\Psi = \Psi(G, T)$ a root datum. Since maximal tori are conjugate, G determines Ψ up to isomorphism and also the root system $R = R(G, T)$ up to isomorphism. Also, if $c \in \mathbb{Q}$ and $c\alpha \in R$, then $G_\alpha = G_{c\alpha}$ and G_α determines a pair of roots $\{\pm\alpha\}$ uniquely. So $c = \pm 1$, i.e., $R(G, T)$ is a reduced root system.

14 More on Roots, and Reductive Groups (11/18)

Recall that last time we discussed that if G is a connected linear algebraic group, T a maximal torus, then we get $\Psi = \Psi(G,T) = (X, R, X^\vee, R^\vee)$ a root datum, where (X,R) and $(X^\vee, R^\vee)$ turned out to be reduced root systems.

Positive Roots

Let $(X, R, X^\vee, R^\vee)$ be a root datum with Weyl group W and fix a W-invariant positive definite symmetric bilinear form on $V = \mathbb{R} \otimes_{\mathbb{Z}} X$.

Definition 14.1. A subset R^+ of R is called *a system of positive roots* if there exists $x \in V$ with $(\alpha, x) \neq 0$ for all $\alpha \in R$ such that $R^+ = \{\alpha \in R : (\alpha, x) > 0\}$. Equivalently, if there exists $\lambda \in X^\vee$ with $\langle \alpha, \lambda \rangle \neq 0, \forall \alpha \in R$ such that

$$R^+ = \{\alpha \in R : \langle \alpha, \lambda \rangle > 0\}.$$

Observe that convex hull of R^+ in V does not contain 0; $R = R^+ \cup (-R^+)$, so if $\alpha, \beta \in R^+$ and $\alpha + \beta \in R$ then $\alpha + \beta \in R^+$; $(R^+)^\vee$ is a system of positive roots in $R^\vee$.

Positive Roots and Borels

Recall that if B is a Borel containing R and $\alpha \in R(G,T)$, then $G_\alpha \cap B$ is a Borel in G_α. (Recall $G_\alpha := Z_G((\ker \alpha)^0)$. Then $B' = G_\alpha \cap B / R_u(G_\alpha) \cap B$ is a Borel subgroup of the reductive group $G' = G_\alpha / R_u(G_\alpha)$ containing $T' = \mathrm{Im} T$. Let $\pm\alpha'$ be the characters of T' corresponding to $\pm\alpha$. As we saw

$$B(B') = L(T') \oplus (\text{1-dimensional weight space})$$

where the last one is either weight space of α' or weight space of $-\alpha'$. Hence, B picks out one root out of each pair $\pm\alpha$. Set

$$R^+(B) = \text{roots obtained this way as } \alpha \text{ ranges through } R(G,T).$$

Proposition 14.2. *$R^+(B)$ is a system of positive roots.*

Example 14.3. $G = \mathrm{GL}_3$, B=upper triangulars, $R^+(B) = \{e_1 - e_2, e_1 - e_3, e_2 - e_3\}$.

Example 14.4. $G = \mathrm{GL}_3$, B=lower triangulars, $R^+(B) = \{-e_1 + e_2, -e_1 + e_3, -e_2 + e_3\}$.

Unipotent Radical

Theorem 14.5. *Let G be a connected linear algebraic group and T a maximal torus. Then $R_u(G) = C$ where*

$$C = \left(\bigcap_{B \supset T \text{ Borel}} B_u \right)^0.$$

Corollary 14.6. *Assume G is reductive, then*
(i) if S is a subtorus of G, then $Z_G(S)$ is connected, reductive;
(ii) $Z_G(T) = T$, i.e., Cartans are maximal tori in reductive linear algebraic group;
(iii) the center $C(G) \subset T$.

Example 14.7. $G = \left\{ \begin{pmatrix} a_1 & * & * \\ & \ddots & * \\ 0 & & a_n \end{pmatrix} \in \mathrm{GL}_n \right\}$, then $B = G$ is a Borel in G. But all Borels are conjugate, so this is the only Borel. $T = \left\{ \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \in \mathrm{GL}_n \right\}$, $B_u = \left\{ \begin{pmatrix} 1 & * & * \\ & \ddots & * \\ 0 & & 1 \end{pmatrix} \right\}$. So

$$R_u(G) = \left\{ \begin{pmatrix} 1 & * & * \\ & \ddots & * \\ 0 & & 1 \end{pmatrix} \right\}.$$

Example 14.8. $G = \mathrm{GL}_n$, $T = \left\{ \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \in \mathrm{GL}_n \right\}$, $B = \left\{ \begin{pmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \in \mathrm{GL}_n \right\}$ is a Borel, $B_u = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in \mathrm{GL}_n \right\}$. $B' = \left\{ \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ * & & a_n \end{pmatrix} \in \mathrm{GL}_n \right\}$ is also a Borel, $B'_u = \left\{ \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ * & & 1 \end{pmatrix} \in \mathrm{GL}_n \right\}$. There are other Borels. So $R_u(G) = \{1\}$. So GL_n is reductive.

Example 14.9. Let $G = \left\{ \begin{pmatrix} a & b & & \\ 0 & d & & \\ & & A & \end{pmatrix} : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, A \in \mathrm{GL}_2 \right\}$, $T = \left\{ \begin{pmatrix} a & & & \\ & d & & \\ & & p & \\ & & & q \end{pmatrix} \right\}$.

Then $B = \left\{ \begin{pmatrix} a & b & & \\ & d & & \\ & & p & x \\ & & & q \end{pmatrix} \right\}$ is a Borel, with $B_u = \left\{ \begin{pmatrix} 1 & b & & \\ & 1 & & \\ & & 1 & x \\ & & & 1 \end{pmatrix} \right\}$. $B' = \left\{ \begin{pmatrix} a & b & & \\ & d & & \\ & & p & \\ & & y & q \end{pmatrix} \right\}$ is also a Borel, with $B'_u = \left\{ \begin{pmatrix} 1 & b & & \\ & 1 & & \\ & & 1 & \\ & & y & 1 \end{pmatrix} \right\}$. So

$$R_u(G) = \left\{ \begin{pmatrix} 1 & b & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \right\},$$

therefore G is not reductive.

Review of Structure Theory of Reductive Groups

Let G be a connected, reductive, linear algebraic group, and let T be a maximal torus of G. So we have a root datum $(X, R, X^\vee, R^\vee)$ of (G, T).

Proposition 14.10. *(i) For $\alpha \in R$, there is an isomorphism $u_\alpha : \mathbf{G}_a \to U_\alpha$ onto a closed subgroup of G such that*

$$tu_\alpha(x)t^{-1} = u_\alpha(\alpha(t)x) \quad \forall t \in T, x \in R.$$

Moreover, $Imdu_\alpha = \mathfrak{g}_\alpha$ where $\mathfrak{g}_\alpha$ is the weight space for the α.
(ii) T and the U_α, $\alpha \in R$, generate G.

As a result, the roots in R are the nonzero weights of T in $\mathfrak{g}$. For each $\alpha \in R$, $\dim \mathfrak{g}_\alpha = 1$. If B is a Borel containing T, $\alpha \in R$, then $\alpha \in R^+(B) \iff U_\alpha \subset B \iff \mathfrak{g}_\alpha \subset \mathfrak{b} = \mathrm{Lie}(B)$. $\dim B = \dim T + \frac{1}{2}|R|$ and $\dim G = \dim T + |R|$.

Example 14.11. $G = \mathrm{GL}_3$, $T = \left\{ t = \begin{pmatrix} a_1 & & \\ & a_2 & \\ & & a_3 \end{pmatrix} \right\}$, $R = \{\pm(e_1 - e_2), \pm(e_1 - e_3), \pm(e_2 - e_3)\}$. Let $\alpha = e_1 - e_2$, then $u_\alpha(x) = \begin{pmatrix} 1 & x & \\ & 1 & \\ & & 1 \end{pmatrix}$,

$$\begin{aligned} tu_\alpha(x)t^{-1} &= \begin{pmatrix} a_1 & & \\ & a_2 & \\ & & a_3 \end{pmatrix} \begin{pmatrix} 1 & x & \\ & 1 & \\ & & 1 \end{pmatrix} \begin{pmatrix} a_1^{-1} & & \\ & a_2^{-1} & \\ & & a_3^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 1 & \frac{a_1}{a_2}x & \\ & 1 & \\ & & 1 \end{pmatrix} = u_\alpha(\frac{a_1}{a_2}x) = u_\alpha(\alpha(t)x), \end{aligned}$$

$$\mathfrak{g}_{e_1-e_2} = \left\{ \begin{pmatrix} 1 & x & \\ & 1 & \\ & & 1 \end{pmatrix} \right\}.$$

Take $B = \left\{ \begin{pmatrix} a & * & * \\ & b & * \\ & & c \end{pmatrix} \right\}$. $R^+(B) = \{e_1 - e_2, e_1 - e_3, e_2 - e_3\}$. $|R| = 6$, $\dim(T) = 3$, $\dim(B) = 6$. So $\dim(G) = 3 + 6 = 9$.

Example 14.12. $G = \mathrm{Sp}_4 = \left\{ g \in \mathrm{GL}_4 : {}^t g J g = J \right\}$ where $J = \begin{pmatrix} & & & 1 \\ & & 1 & \\ & -1 & & \\ -1 & & & \end{pmatrix}$, and

$$T = \left\{ t = \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & a_2^{-1} & \\ & & & a_1^{-1} \end{pmatrix} \right\}.$$

$R = \{\pm(e_1 \pm e_2), \pm 2e_1, \pm 2e_2\}$. $U_{e_1-e_2}(x) = \left\{ t = \begin{pmatrix} 1 & x & & \\ & 1 & & \\ & & 1 & -x \\ & & & 1 \end{pmatrix} \right\}$, $U_{2e_2}(x) = \left\{ t = \begin{pmatrix} 1 & & 1 & x \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \right\}$.

If $B = \left\{ \begin{pmatrix} a_1 & * & * & * \\ & a_2 & * & * \\ & & a_2^{-1} & * \\ & & & a_1^{-1} \end{pmatrix} \right\}$, then $R^+(B) = \{e_1 - e_2, 2e_1, e_1 + e_2, 2e_2\}$, $\dim(B) = 2 + 4 = 6$, $\dim(B) = 2 + 8 = 10$.

The Weyl group of (G, T) is $W := N_G(T) \backslash T$. We identify it with the Weyl group of the root datum of (G, T). For $\alpha \in R$, $s_\alpha \in W$ and $s_\alpha = s_{-\alpha}$, we have the following:

- We may choose u_α such that for all $\alpha \in R$, we have $n_\alpha = u_\alpha(1) u_{-\alpha}(1) u_\alpha(1) \in N_G(T)$ and its image is $s_\alpha \in W$. For $x \in k^\times$, $u_\alpha(x) u_{-\alpha}(-x^{-1}) u_\alpha(x) = \alpha^\vee(x) n_\alpha$.

- $n_\alpha^2 = \alpha^\vee(-1)$ and $n_{-\alpha} = n_\alpha^{-1}$.

- For $u \in U_\alpha - \{1\}$, there exists a unique $u' \in U_{-\alpha} - \{1\}$ such that $uu'u \in N_G(T)$.

- If $(u'_\alpha)_{\alpha \in R}$ is another such family, then $u'_\alpha(x) = u_\alpha(c_\alpha x)$ with $c_\alpha c_{-\alpha} = 1$ for all $\alpha \in R, x \in k$.

Example 14.13. $G = \mathrm{SL}_2$, $R = \{\pm(e_1 - e_2)\}$, $T = \left\{ t = \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \right\}$. $u_{e_1-e_2}(x) = \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix}$, $u_{-(e_1-e_2)}(x) = \begin{pmatrix} 1 & \\ x & 1 \end{pmatrix}$. Let $\alpha = e_1 - e_2$, then

$$u_\alpha(x)u_{-\alpha}(-x^{-1})u_\alpha(x) = \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ -x^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} = \begin{pmatrix} & x \\ -x^{-1} & \end{pmatrix} = \begin{pmatrix} x & \\ & x^{-1} \end{pmatrix} \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$$

where $\alpha^\vee(x) = \begin{pmatrix} x & \\ & x^{-1} \end{pmatrix}$, $n_\alpha = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$, and

$$n_\alpha^2 = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}^2 = \begin{pmatrix} -1 & \\ & -1 \end{pmatrix} = \alpha^\vee(-1).$$

Definition 14.14. We call a family $(u_\alpha)_{\alpha \in R}$ with these properties a realization of the root system R in G.

Theorem 14.15. *Assume that G is semisimple.*
(i) The U_α, $\alpha \in R$, generate G.
(ii) $G = (G, G)$.
(iii) Let $G_1 \neq G$ be a nontrivial connected closed normal subgroup of G. Then G_1 is semisimple, and there is a similar group G_2 such that $(G_1, G_2) = \{e\}$, $G_1 \cap G_2$ finite and $G = G_1G_2$.
(iv) The number of minimal non-trivial connected, closed normal subgroups of G is finite, say $G_1, \cdots, G_r$. Then $(G_i, G_j) = \{e\}$ if $i \neq j$, and $G_i \cap \prod_{j \neq i} G_j$ is finite and $G = G_1G_2 \cdots G_r$ and the G_i's have no closed, normal subgroups of dimension > 0.

If G is reductive, then
(i) $G = R(G) \cdot (G, G)$.
(ii) (G, G) is semisimple.

Example 14.16. $G = \mathrm{GL}_n$, $(G, G) = \mathrm{SL}_n$, and $R(G) = \left\{ \begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix} \right\}$.

Recall that given (G, T), we have the root datum $(X, R, X^\vee, R^\vee)$.
Notation: For A a subgroup of X, we denote

$$A^\perp := \{y \in X^\vee : \langle A, y \rangle = \{0\}\}, \quad \text{annihilator of } A,$$

$$\tilde{A} := \{x \in X : \mathbb{Z} \cdot x \cap A \neq \{0\}\}, \quad \text{rational closure of } A.$$

$\tilde{A}/A$ is the torsion subgroup of X/A. We have similar notions for $X^\vee$. It's easy to check that $\tilde{A} = (A^\perp)^\perp$.

We define Q to be the subgroup of X generated by R, and $Q^\vee$ to be the subgroup of $X^\vee$ generated by $R^\vee$.

Here are some facts:

- $C(G) = \cap_{\alpha \in R} \ker \alpha$.

- $R(G) =$ the subgroup of G generated by $\mathrm{Im} y, y \in Q^\vee \subset T$ and

$$X^*(R(G)) \cong X \backslash \tilde{Q},$$

$$X_*(R(G)) \cong Q^\perp.$$

- The subtorus $T_1 = \langle \mathrm{Im}\alpha^\vee : \alpha \in R \rangle \subset T$ is a maximal subtorus of (G, G). Also

$$X^*(T_1) \cong X/(Q^\vee)^\perp,$$

$$X_*(T_1) \cong \tilde{Q}^\perp.$$

- The root datum of $((G, G), T_1)$ is $(X/(Q^\vee)^\perp, R, \tilde{Q}^\perp, R^\vee)$.

- Assume G is semisimple, then $Q^\vee = \{0\}$, $X = \tilde{Q}$. Q has finite index in X. The finite group $C^* = C^*(G) := X/Q$ is called the cocenter of G. Define $P := \{x \in V = \mathbb{R} \otimes_{\mathbb{Z}} X : \langle x, R^\vee \rangle \subset \mathbb{Z}\}$. Then P is a lattice in V and $Q \subset P$. Given a root system R in V, there are finitely many possibilities for x. Q is the root lattice of R, and P is the weight lattice of R. For G semisimple as above, G is called *adjoint* if $X = Q$. G is called *simply-connected* if $X = P$. The finite abelian group P/Q is called the fundamental group of R.

Borels and Positive Systems

Fix a Borel $B \supset T$ in G. Write $U : B_u$ the unipotent radical of B, $R^+ = R^+(B)$ positive system of roots determined by B. Fix a total order on R.

B_u is generated by groups $U_\alpha, \alpha \in R^+$.

For $\alpha, \beta \in R$, $\alpha = \pm\beta$, there exist "structure constants" $c_{\alpha,\beta;i,j} \in R$ such that

$$(u_\alpha(x), u_\beta(y)) = \prod_{\substack{i\alpha + j\beta \in R \\ i,j>0}} u_{i\alpha+j\beta}(c_{\alpha,\beta;i,j} x^i y^j) \quad \forall x, y \in R$$

(order according to the fixed total ordering).

Let $\tilde{R}^+$ be an arbitrary system of positive roots. Then
(i) T and the $U_\alpha, \alpha \in \tilde{R}^+$ generate a Borel in G.
(ii) there exists a unique $w \in W$ with $\tilde{R}^+ = w \cdot R^+$.

Let $\mathcal{W}$ be the set of Borel subgroups of G containing T. We saw that $\mathcal{W}$ acts simply transitively on $\mathcal{W}$. Two Borels $B, B' \subset \mathcal{W}$ are called *adjacent* if $\dim(B \cap B') = \dim B - 1 = \dim B' - 1$.

We say two systems of positive roots R^+ and $\tilde{R}^+$ are *adjacent* if

$$|R^+ \cap \tilde{R}^+| = |R^+| - 1 = |\tilde{R}^+| - 1.$$

We have:
(i) $B, B' \in \mathcal{W} \Rightarrow$ there exists a family $B = B_0, B_1, B_2, \cdots, B_n = B'$ in $\mathcal{W}$ such that B_i and B_{i+1} are adjacent.
(ii) If R^+ and $\tilde{R}^+$ are two systems of positive roots, then there exists a family of system of positive roots $R^+ = R_0^+, R_1^+, \cdots, R_n^+ = \tilde{R}^+$ such that R_i^+ and R_{i+1}^+ are adjacent.
(iii) If R^+ and $\tilde{R}^+$ are adjacent, then there exists a unique $\alpha \in R^+$ such that $\tilde{R}^+ = s_\alpha R^+$.

15 Bruhat Decomposition, Parabolic Subgroups, the Isomorphism Theorem, and the Existence Theorem (12/2)

Recall that the pair of a reductive group and a maximal torus (G, T) determines a root datum $\Psi = \Psi(G, T) = (X, R, X^\vee, R^\vee)$. Given $\alpha \in R$, we have $u_\alpha : \mathbf{G}_a \to U_\alpha$ satisfying

$$tu_\alpha(x)t^{-1} = u_\alpha(\alpha(t)x), \quad \forall x \in k, t \in T,$$

and $\mathfrak{g}_\alpha = \mathrm{Im} du_\alpha$. We know that T and U_α generate G. Let $W = N_G(T)/T$, identified with $W(R(G,T))$. Take $B \supset T$ a Borel in G, then we have $R^+(B)$ a system of positive roots. Then $R = R^+(B) \cup (-R^+(B))$.

Since G is reductive, $G = R(G) \cdot (G, G)$ where $R(G)$ is a central torus, (G, G) is semisimple, generated by the U_α's. Last time, we described the root data for both $R(G)$ and (G, G). We continue the study on Borel subgroups.

Let R^+ be a system of positive roots. Let

$$D = D(R^+) := \{\alpha \in R^+ : s_\alpha \cdot R^+ \text{ and } R^+ \text{ are adjacent}\}.$$

If $R^+ = R^+(B)$ with $R \supset T$, we also write $D = D(B)$. We call D the basis of R defined by R^+. Its elements are called the *simple roots* in R^+.

Let $S = S(R^+) = S(B) := \{s_\alpha : \alpha \in D\}$ be simple reflections defined by B or R^+. We have

- $D(w \cdot R^+) = wD(R^+)$.
- $S(w \cdot R^+) = wS(R^+)w^{-1}$.
- For $\alpha \in D$, s_α permutes the elements of $R^+ - \{0\}$.
- For $\alpha, \beta \in D$, $\alpha \neq \beta$, $\langle \alpha, \beta \rangle \leq 0$.

Theorem 15.1. *(i) S generate W.*
(ii) $R = W \cdot D$.
(iii) The roots in D are linearly independent. A root in R^+ is a linear combination $\sum_{\alpha \in D} n_\alpha \alpha$, $n_\alpha \in \mathbb{Z}_{\geq 0}$. These two properties characterize the subsets D of R^+.

Corollary 15.2. *G is generated by T and the groups $U_{\pm\alpha}, \alpha \in D$.*

Bruhat Decomposition

For $w \in W$, define

$$R(w) := \{\alpha \in R^+ : w\alpha \in -R^+\}.$$

For example, for $\alpha \in D$, $R(s_\alpha) = \{\alpha\}$, we have

$$R(ws_\alpha) = \begin{cases} s_\alpha R(w) \cup \{\alpha\} & \text{if } w\alpha \in R^+, \\ s_\alpha(R(w) \cup \{\alpha\}) & \text{if } w\alpha \in -R^+. \end{cases}$$

Define $l(w) :=$ smallest integer $h \geq 0$ such that w is a product of heights in S. A reduced decomposition of w is a sequence $s = (s_1, \cdots, s_h)$ in S with $w = s_1 s_2 \cdots s_h$ and $h = l(w)$. Note that $l(w) = l(w^{-1})$.

Let $(\dot{w})_{w \in W}$ be a set of representatives in $N_G(T)$ of elements in W. Then $C(w) = B\dot{w}B$ is the Bruhat cell, which is a locally closed subvariety of G.

Theorem 15.3 (Bruhat Decomposition)**.**

$$G = \coprod_{w \in W} C(w).$$

In other words, an element of G can be written uniquely as $u\dot{w}b$, $w \in W$, $u \in U_{w^{-1}} = \prod_{\alpha \in R(w^{-1})} U_\alpha$.

Corollary 15.4. *The intersection of two Borels of G contains a maximal torus.*

Proof. Let B and $B' = gBg^{-1}$ be two Borels. Write $g = b\dot{w}b'$, then $bTb^{-1} \in B \cap B'$. □

Corollary 15.5. *There is a unique open double coset, namely $C(w_0)$, where w_0 is the longest element of W.*

Example 15.6. $G = \mathrm{GL}_2$, $T = \left\{ \begin{pmatrix} a & \\ & b \end{pmatrix} \right\}$, $B = \left\{ \begin{pmatrix} a & * \\ & b \end{pmatrix} \right\}$, $W = \left\{ 1, \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \right\}$.

Parabolic Subgroups

Let G, T, B be as before. Let

$$\begin{aligned} I \subset D &= \text{simple roots} \\ W_I &: = \text{subgroup of } W \text{ generated by reflections } s_\alpha,\ \alpha \in I; \\ R_I &: = \text{set of roots in } R \text{ that are linear combinations of the roots in } I; \\ S_I &: = \left(\bigcap_{\alpha \in I} \ker \alpha \right)^0, \quad L_I := Z_G(S_I). \end{aligned}$$

We saw that L_I is a connected reductive subgroup of G with maximal torus T and Borel subgroup $B_I = B \cap L_I$.

Here are some facts:

- The root system $R(L_I, T) = R_I$, and $W(L_I, T) = W_I$.
- $R_I^+(B_I) = R_I^+ = R^+ \cap R_I$ and the corresponding simple roots in I.
- $P_I := \bigcup_{w \in W_I} C(w)$ is a parabolic subgroup of G containing B and L_I.
- $R_u(P_I)$ is generated by the $U_\alpha, \alpha \in R^+ - R_I$.
- The product map $L_I \times R_u(P_I) \to P_I$ is an isomorphism of varieties.
- If P is a parabolic subgroup of G containing B, then there exists a unique subset I of D such that $P = P_I$.

Definition 15.7. Let P be a parabolic subgroup of G. A *Levi subgroup* of P is a closed subgroup of P such that the product map $L \times R_u(P) \to P$ is bijective.

Note that a maximal torus of P lies in a unique Levi subgroup.

Example 15.8. $G = \mathrm{GL}_n, T = \left\{ \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \in \mathrm{GL}_n \right\}, B = \left\{ \begin{pmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \in \mathrm{GL}_n \right\}.$

The root is of type A_{n-1}:

$$R(G,T) = \{\pm(e_i - e_j), 1 \le i, j \le n, i \ne j\},$$
$$R^+(B) = \{(e_i - e_j), i < j\},$$
$$D(B) = \{e_1 - e_2, e_2 - e_3, \cdots, e_{n-1} - e_n\}.$$

Dynkin Diagrams

Let R be a root system in the Euclidean space V. Fix a metric $(\ ,\ )$ in V that is $W(R)$-invariant such that $\langle \alpha, \beta^\vee \rangle = \frac{2(\alpha,\beta)}{(\beta,\beta)}$ as before. Let D be a basis of R.

Definition 15.9. The *Dynkin diagram* $\mathcal{D}$ defined by D is a graph with vertex set D and two vertices α, β joined by $\langle \alpha, \beta^\vee \rangle \langle \beta, \alpha^\vee \rangle$ bonds. When α and β have different lengths, we add an arrow pointing towards the shortest root.

Observe that if $\alpha \perp \beta$, then $\langle \alpha, \beta^\vee \rangle = 0$, so no bonds (no edges between them).

The Cartan matrix is $\left(\langle \alpha_i, \alpha_j^\vee \rangle \right)$.

If R is an irreducible root system, then it's easy to check that:

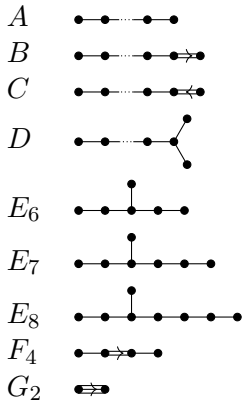
- D is a connected graph, in fact, a tree.

- A multiple bond is either double or triple.

- Triple bond only occurs in the case $\bullet\!\!\Leftarrow\!\!\bullet$.

- At most one double bond can occur and if it does, D is a chain.

- If multiple bonds occur, we have only two root lengths (long and short). In fact, here is a classification of irreducible Dynkin diagrams.



Recall that given an irreducible root system R in the Euclidean space V, we define $P = \{x \in V : \langle x, R^\vee\rangle \subset \mathbb{Z}\}$ and $Q \subset P$ by $Q =$ subgroup in V generated by R. They are both free $\mathbb{Z}$-modules. When $R = R(G,T)$, then $Q \subset X = X^*(T) \subset P$.

Example 15.10. One-dimensional irreducible root systems:

$A_1 : \bullet$. $\alpha = e_1 - e_2$, $-\alpha = e_2 - e_1$, $\alpha^\vee = e_1^* - e_2^*$, and $\langle \alpha, \alpha^\vee\rangle = (1)(1) + (-1)(-1) = 2$. $V = \{(x,y) \in \mathbb{R}^2 : x+y = 0\}$. The Cartan matrix is (2). $P = \mathbb{Z}\cdot\frac{e_1-e_2}{2}$, and $Q = \mathbb{Z}\cdot(e_1-e_2)$. We have two possibilities: if $X = P$, then we get simplely-connected $G = \mathrm{SL}_2$; if $X = Q$, then we get an adjoint group $G = \mathrm{PSL}_2$ or PGL_2.

Example 15.11. Two-dimensional irreducible root systems: (two-dimensional reducible: $A_1 \times A_1 = D_2$)

(a) $A_2 : \bullet\!\!-\!\!\bullet$. $\alpha = e_1 - e_2$, $\beta = e_2 - e_3$, $V = \{(x,y,z) \in \mathbb{R}^3 : x+y+z = 0\}$. The Cartan matrix is $\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$. We have $P = \mathbb{Z}\langle \frac{1}{3}\alpha + \frac{2}{3}\beta, \frac{2}{3}\alpha + \frac{1}{3}\beta\rangle$, and $Q = \mathbb{Z}\langle e_1 - e_2, e_2 - e_3\rangle$. The

index is $[P : Q] = 2$. We have two possibilities: if $X = P$, then we get simplely-connected $G = \mathrm{SL}_3$; if $X = Q$, then we get an adjoint group $G = \mathrm{PSL}_3$ or PGL_3.

(b) B_2 : •⇒•. $\alpha = e_1 - e_2$, $\beta = e_2$, $\alpha^\vee = e_1^* - e_2^*$, $\beta^\vee = 2e_2^*$, $V = \mathbb{R}^2$. The Cartan matrix is $\begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix}$. We have $P = \{(m + \frac{n}{2}, \frac{n}{2}), m, n \in \mathbb{Z}\} = \mathbb{Z}\langle e_1, \frac{e_1+e_2}{2}\rangle$, and $Q = \mathbb{Z}\langle e_1, e_2\rangle$. If $X = P$, then we get simplely-connected $G = \mathrm{Sp}_4 \cong \mathrm{Spin}_5$; if $X = Q$, then we get an adjoint group $G = \mathrm{SO}_5 \cong \mathrm{PSp}_4 \cong \mathrm{PGSp}_4$.

(c) G_2 : •⇛•. $\alpha = e_1 - e_2$, $\beta = -2e_1 + e_2 + e_3$. $V = \{(x, y, z) : x + y + z = 0\}$, and the Cartan matrix is $\begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}$. $X = P = Q$. So we get simply-connected and adjoint G_2.

Here are identical isomorphisms:

$$\begin{aligned} A_1 = B_1 = C_1, \\ \mathrm{SL}_2 \cong \mathrm{Spin}_3 \cong \mathrm{Sp}_2, \\ \mathrm{PSL}_2 \cong \mathrm{SO}_3 \cong \mathrm{PSp}_2, \\ B_2 \cong C_2, \\ \mathrm{Spin}_5 \cong \mathrm{Sp}_4, \\ \mathrm{SO}_5 \cong \mathrm{PSp}_4. \end{aligned}$$

The Isomorphism Theorem

Definition 15.12. Let G and G_1 be two connected, reductive algebraic groups over k, with maximal torus T and T_1 respectively, and root data $\Psi = (X, R, X^\vee, R^\vee)$ and $\Psi_1 = (X_1, R_1, X_1^\vee, R_1^\vee)$. An *isogeny* $\varphi : G \to G_1$ is a surjective homomorphism of algebraic groups with finite kernel.

We have the following:

- $\ker \varphi$ is a central subgroup of G lying in T.
- $\dim G = \dim G_1$.
- Assume $\varphi(T) = T_1$. Then φ defines homomorphisms $f = f(\varphi) : X_1 \to X$ and $f^\vee = f^\vee(\varphi) : X^\vee \to X_1^\vee$ such that $\langle x_1, f^\vee(\lambda)\rangle = \langle f(x_1), \lambda\rangle$ for all $x_1 \in X_1, \lambda \in X^\vee$.
- Also, there is a bijection $b : R \to R_1$ with $\varphi U_\alpha = R_{b\alpha}$ for all $\alpha \in R$.
- If φ is an isomorphism of algebraic groups, then $f(b\alpha) = \alpha$ for all $\alpha \in R$ and f defines an isomorphism of root data $\Psi_1 \to \Psi$, i.e., isomorphisms $X_1 \to X$ mapping R_1 onto R such that its dual maps $R^\vee$ onto $R_1^\vee$.

Theorem 15.13 (Isomorphism Theorem)**.** *Let $f : \Psi_1 \to \Psi$ be an isomorphism of root data. Then there is an isomorphism of algebraic groups $\varphi : G \to G_1$ with $\varphi(T) = T_1$ and $f = f(\varphi)$. If φ' is another isomorphism, then there exists $t \in T$ such that $\varphi'(t) = \varphi(tgt^{-1})$.*

Let φ be an arbitrary isogeny. Then f is an isomorphism of X_1 onto a subgroup of X of finite index and we have

$$f(b\alpha) = q(\alpha)\alpha,$$
$$f^\vee(\alpha^\vee) = q(\alpha)(b\alpha)^\vee,$$

for some $q(\alpha) = \begin{cases} 1 & \text{if char } k = 0 \\ \text{some power of } p & \text{if char } k = p. \end{cases}$

If $q(\alpha) \equiv 1$, then we say φ is a central isogeny. We say a triple $\mu = (f, b, q)$ with $f : X_1 \twoheadrightarrow$ a subgroup of X of finite index, $b : R \to R_1$ bijective, $q : R \to \{p^n\}_{n>0}$, defines a p-morphism of φ_1 to φ if the above properties hold.

Theorem 15.14. *Let $\mu = (f, b, q)$ be a p-morphism of φ_1 to φ. There is an isogeny $\varphi : G \to G_1$ with $\varphi T = T_1$ and $\mu = \mu(\varphi)$. If φ' is another such isogeny with theses properties, then there exists $t \in T$ such that $\varphi'(g) = \varphi(tgt^{-1})$.*

The Existence Theorem

Theorem 15.15. *Let $\Psi = (X, R, X^\vee, R^\vee)$ be a root datum. There exists a connected, reductive, linear algebraic group G over k with a maximal torus T, such that the root datum $\Psi(G, T)$ is isomorphic to Ψ.*

We outline the ideas of proof. Step (a): Reduce to the case that R spans X and is irreducible. Then the group is quasi-simple (i.e., no proper, connected, closed normal subgroup) and adjoint. Step (b): In that case, G is constructed as a group of automorphisms of its Lie algebra in the case R is simply-faced. In this case, one constructs the Lie algebra first, which requires explicit description of the structure of constants. Step (c): For arbitrary (non-simply-faced) root system R, the construction of G is reduced to the simply-faced case via "automorphisms folding".

Example 15.16. Consider $\Psi_n = (X, R, X^\vee, R^\vee)$, $X = \mathbb{Z}e_0 \oplus \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$, $X^\vee = \mathbb{Z}e_0^* \oplus \mathbb{Z}e_1^* \oplus \cdots \oplus \mathbb{Z}e_n^*$.

$$R = \begin{cases} \pm(e_i - e_j), \pm(e_i + e_j), & 1 \le i < j \le n, \\ \pm e_i & 1 \le i \le n, \end{cases}$$

$$R^\vee = \begin{cases} \pm(e_i^* - e_j^*), \pm(e_i^* + e_j^* - e_0^*), & 1 \le i < j \le n, \\ \pm 2e_i^* - e_0^* & 1 \le i \le n. \end{cases}$$

$\langle\ ,\ \rangle : X \times X^\vee \to \mathbb{Z}$ is the standard pairing. It's easy to check that this is a root datum. (X, R) is a root system of type B_n, and $(X^\vee, R^\vee)$ is a root system of type C_n. Choose a Borel B such that the simple roots are $D = \{e_1 - e_2, e_2 - e_3, \cdots, e_{n-1} - e_n, e_n\}$. Then

$$D^\vee = \{e_1^* - e_2^*, e_2^* - e_3^*, \cdots, e_{n-1}^* - e_n^*, e_n^*\}.$$

The group determined by Ψ_n is usually called GSpin_{2n+1}.

When $n = 2$, one can construct the U_α's abstractly. The U_α's corresponding to positive roots are $U_{e_1-e_2}$, $U_{e_1+e_2}$, U_{e_1}, U_{e_2}, and they generate $R_u(B)$. The U_α's corresponding to negative roots are $U_{-e_1+e_2}$, $U_{-e_1-e_2}$, U_{-e_1}, U_{-e_2}, and they generate $R_u(\bar{B})$. To generate T, choose $\{e_o^*(x)\}$ and $\gamma^\vee(x)$ where $\gamma = \alpha, \alpha + \beta, \alpha + 2\beta$. This group $(n = 2)$ is called GSpin_5, where root system is of type B_2 and coroot system is of type C_2. But the two root systems are isomorphic, so $\Psi_2^\vee = (X^\vee, R^\vee, x, r)$ is a root datum isomorphic to Ψ_2. So when $n = 2$, $\mathrm{GSpin}_5 \cong \mathrm{GSp}_4$.