University of Oregon Mathematics Department

Moursund Lectures 1998

J.-P. Serre

Notes by W.E. Duckworth

These informal notes are closely based on a series of eight lectures given by J.-P. Serre at the University of Oregon in October 1998. Professor Serre gave two talks per week for four weeks.

The first talk each week was concerned with constructing embeddings of finite groups, especially $\mathrm{PSL}_2(p)$ and $\mathrm{PGL}_2(p)$, into Lie groups. The second talk each week was about generalizations of the notion of complete reducibility in group theory, especially in positive characteristic.

The notes are divided into two parts, one for each of the topics of the lecture series. At the end of the notes, there is a short list of references as a guide to further reading.

Part I

Finite subgroups of Lie groups

Lecture 1

We begin with a guiding example. Let G be the compact Lie group $\mathrm{SO}_3(\mathbb{R})$. The finite subgroups of G fall into the following families:

- The cyclic subgroup C_n of order n. This appears as a subgroup of the maximal torus T of G consisting of rotations around some fixed axis. It is not really interesting: it's there because of the torus, not really because of G.

- The dihedral group D_n of order $2n$. Again, such subgroups lie in another Lie subgroup of G, namely the normalizer N of T in G. The index $(N : T) = 2$ and the additional reflection generating D_n lies inside N.

- Three more "exceptional" examples: the alternating group A_4 on four letters, the symmetric group S_4, and the alternating group A_5. These may be viewed as the automorphisms of the regular tetrahedron, cube and icosahedron respectively.

Let us indicate one reason for the importance of this example for complex analysis and topology. One can view $\mathrm{SO}_3(\mathbb{R})$ as a maximal compact subgroup of the group $\mathrm{PGL}_2(\mathbb{C})$, that is, the group of all transformations $z \mapsto \frac{az+b}{cz+d}$ with $ad-bc \neq 0$. Up to conjugacy, compact subgroups of $\mathrm{PGL}_2(\mathbb{C})$ and $\mathrm{SO}_3(\mathbb{R})$ are the same. So the above list also describes the embeddings of finite subgroups Γ into $\mathrm{PGL}_2(\mathbb{C})$. Now, $\mathrm{PGL}_2(\mathbb{C})$ is the automorphism group of the projective line $\mathbb{P}_1$ over $\mathbb{C}$, so a finite subgroup $\Gamma \subset \mathrm{PGL}_2(\mathbb{C})$ acts on $\mathbb{P}_1$. Dividing, we get a (ramified) Galois covering

$$\mathbb{P}_1 \xrightarrow{\Gamma} \mathbb{P}_1/\Gamma \cong \mathbb{P}_1$$

of a curve of genus 0 by another, and our list of finite subgroups gives all possible Galois coverings of $\mathbb{P}_1$ by $\mathbb{P}_1$.

We wish to consider finite subgroups of more general Lie groups G. We will restrict our attention to the following sorts of Lie group:

- Compact, real, connected Lie groups, especially the semisimple ones: SU_n, SO_n, $\ldots$, E_8.

- The corresponding complex groups: $\mathrm{SL}_n(\mathbb{C})$, $\mathrm{SO}_n(\mathbb{C})$, $\ldots$, $E_8(\mathbb{C})$.

- Any of these groups $G(k)$ over an arbitrary field k. Indeed, thanks to Chevalley, we can define these groups even over $\mathbb{Z}$.

In fact as we will see, one can often use the groups $G(k)$ over fields of positive characteristic to shed light on the first two problems. An example of this philosophy appears in the work of Minkowski, who was studying lattices $\Lambda \subset \mathbb{R}^n$ (cf. [Min]). The group $\Gamma := \mathrm{Aut}(\Lambda)$ is finite, and he was interested in finding an upper bound for the exponent of a given prime ℓ in $|\Gamma|$. Now $\Lambda \cong \mathbb{Z}^n$ so $\Gamma \subset \mathrm{GL}_n(\mathbb{Z})$. If we reduce modulo p then we have a map $\Gamma \to \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Minkowski showed that for $p \geq 3$ this is an embedding, so that $|\Gamma|$ divides $|\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})| = (p^n-1)(p^n-p)\dots(p^n-p^{n-1})$. Now, by varying p one gets an upper bound for the exponent of ℓ in $|\Gamma|$, namely, $\left[\frac{n}{\ell-1}\right] + \left[\frac{n}{\ell(\ell-1)}\right] + \dots$. (This is correct only for $\ell > 2$; the case $\ell = 2$ requires a slightly different argument.) Moreover, this upper bound is exact.

From now on G is a semisimple group, e.g. SL_n, …, E_8. We want to understand the possible finite groups $\Gamma \subset G(\mathbb{C})$. First, we discuss the case that Γ is *abelian*. Let T be a maximal torus of G of dimension $r = \operatorname{rank} G$. So, $T \cong \mathbb{G}_m \times \dots \times \mathbb{G}_m$ (r copies) where $\mathbb{G}_m$ is the one dimensional multiplicative group. So over $\mathbb{C}$, $T(\mathbb{C}) \cong \mathbb{C}^* \times \cdots \times \mathbb{C}^*$. Thus we can realize any abelian finite group on r generators as a subgroup of $T(\mathbb{C})$. In fact, *almost* all finite abelian subgroups subgroups of $G(\mathbb{C})$ arise in this way, but there are exceptions. For example, recall our embedding of the Klein group D_2, which is an elementary abelian $(2,2)$-group, in $\mathrm{SO}_3(\mathbb{R}) \subset \mathrm{PGL}_2(\mathbb{C})$: it cannot be embedded in $T(\mathbb{C})$ since $\mathrm{PGL}_2(\mathbb{C})$ only has rank 1.

Let us restrict our attention to elementary abelian $(p, p, \dots, p)$-groups E. Then all subgroups of $G(\mathbb{C})$ isomorphic to E are 'toral', that is, are contained in some maximal torus, unless p is one of finitely many *torsion primes*. For each of these torsion primes, there is an 'exceptional' embedding of some E into $G(\mathbb{C})$; R. Griess has classified such embeddings, cf. [G]. The torsion primes for simply connected, simple G are as follows:

A_n	$B_n, n \geq 3$	C_n	$D_n, n \geq 4$	G_2	F_4	E_6	E_7	E_8
none	2	none	2	2	2,3	2,3	2,3	2,3,5

These primes first arose in topology in the 1950s (cf, e.g. [Bo]). For a compact Lie group G, the cohomology ring $H^*(G, \mathbb{Z})$ with coefficients in $\mathbb{Z}$ is not always a free $\mathbb{Z}$-module. The primes p such that $H^*(G, \mathbb{Z})$ has p-torsion are called the torsion primes. Moreover, these primes can be described in terms of the root data: if all the roots have the same length, they are the primes that divide a coefficient of the highest root when written in terms of the simple roots.

For another example of one of these exceptional embeddings, consider $G = G_2$. We view $G_2(\mathbb{C})$ as the group of automorphisms of the *Cayley* *algebra.* This algebra has a standard basis $\{1, e_\alpha \mid \alpha \in \mathbb{Z}/7\mathbb{Z}\}$ and the automorphisms determined by $e_\alpha \mapsto \pm e_\alpha$ for $\alpha = 1, 2, 3$ give an 'exceptional' elementary abelian $(2, 2, 2)$-group inside $G_2(\mathbb{C})$. This subgroup is important in studying the Galois cohomology of G_2.

These results on abelian subgroups can be extended somewhat to *nilpotent subgroups* using a result of Borel-Serre (cf. [BS]): every finite nilpotent subgroup of $G(\mathbb{C})$ is contained in the normalizer of some maximal torus of $G(\mathbb{C})$.

Now we consider a second, quite different situation, namely, we let Γ be a *quasi-simple* group (i.e. the quotient by its center is simple and non-abelian). If $G = \mathrm{SL}_n$ then one can classify all possible embeddings $\Gamma \hookrightarrow G(\mathbb{C})$ by viewing the natural $G(\mathbb{C})$-module as a representation of Γ and using character theory. A variation of this approach allows one to tackle the problem also for $G = \mathrm{SO}_n$, Sp_{2n} and even G_2 (since this can be viewed as the subgroup of SO_7 which leaves invariant an alternating 3-linear form). In other words, in these cases, the problem can be reduced to a question about the character table of Γ. This leaves the cases F_4, E_6, E_7 and E_8. A lot of work in the last few years, in particular by A. Cohen, R. Griess and A. Ryba, has resulted in a list of the possible Γ that can arise. This list is complete according to computer verifications. There are still open questions however. For instance, the number of conjugacy classes of such subgroups is not known in general.

Some of the most interesting questions arise when $\Gamma = \mathrm{PSL}_2(\mathbb{F}_p)$. For instance, if $G = E_8$, then $G(\mathbb{C})$ has finite subgroups $\mathrm{PSL}_2(\mathbb{F}_p)$ for $p = 31, 41, 61$ (cf.[GR], [S3]). The principal difficulty is in proving the *existence* of these subgroups. We now discuss briefly the sorts of method one can use for such a construction.

The first method depends upon computer calculations. For instance, to embed $\mathrm{PSL}_2(\mathbb{F}_{61})$ in $E_8(\mathbb{C})$, start with a Borel subgroup $B \subset \mathrm{PSL}_2(\mathbb{F}_{61})$ consisting of all upper triangular matrices and its opposite B^- consisting of all lower triangular matrices. Then B is isomorphic to a semidirect product of cyclic subgroups of order 61 and 30. Choose an element in $E_8(\mathbb{C})$ of order 30, namely, a *Coxeter element.* There is a subgroup of $E_8(\mathbb{C})$ generated by an element of order 61 upon which this Coxeter element acts by an automorphism of order 30. We map B to the subgroup of $E_8(\mathbb{C})$ generated by these two elements. Then one needs an involution within $E_8(\mathbb{C})$ which gives the embedding of the other Borel B^-, and this is where the computer comes in. In fact, the computer calculations are done by working within $E_8(\mathbb{F}_\ell)$ for some large prime ℓ not dividing the order of Γ. The results are then lifted (easily) to $E_8(\mathbb{C})$.

The second method (cf.[S3]) is quite different, and depends on lifting from *the same characteristic* $p = 61$. There is a so-called *principal homomorphism* $\mathrm{SL}_2 \to E_8$ with kernel $\{\pm 1\}$. This is defined over $\mathbb{F}_p$, giving an embedding of $\mathrm{PSL}_2(\mathbb{F}_p)$ into $E_8(\mathbb{F}_p)$. The idea is to lift this embedding to an embedding in characteristic 0. However, there may be a non-trivial obstruction preventing a lift to an embedding $\mathrm{PSL}_2(\mathbb{F}_p) \hookrightarrow E_8(\mathbb{Z}/p^2\mathbb{Z})$. So one has to proceed more indirectly, and we will discuss the argument in more detail in the remaining lectures.

Finally, we return to our opening example. Recall we had subgroups $A_4 \cong \mathrm{PSL}_2(\mathbb{F}_3)$, $S_4 \cong \mathrm{PGL}_2(\mathbb{F}_3)$ and $A_5 \cong \mathrm{PSL}_2(\mathbb{F}_5)$ inside $\mathrm{SO}_3(\mathbb{R})$, corresponding to the symmetries of the tetrahedron, cube and icosahedron. The analogues of these embeddings for E_8 are the embeddings of $\mathrm{PSL}_2(\mathbb{F}_{31})$, $\mathrm{PGL}_2(\mathbb{F}_{31})$ and $\mathrm{PSL}_2(\mathbb{F}_{61})$! In fact, quite generally for any simple, simply-connected G, let h be the *Coxeter number* defined as $\dfrac{\dim G}{\operatorname{rank} G} - 1$. Notice in the rank 1 case $\mathrm{SO}_3(\mathbb{R})$, we have $h = 2$. In the case of E_8 we have $h = 30$. It is true in general that if $h+1$ or $2h+1$ is prime then $G(\mathbb{C})$ has subgroups of the form $\mathrm{PSL}_2(\mathbb{F}_{h+1})$, $\mathrm{PGL}_2(\mathbb{F}_{h+1})$ and $\mathrm{PSL}_2(\mathbb{F}_{2h+1})$.

Lecture 2

We continue to assume that G is a simple algebraic group over an algebraically closed field k of characteristic zero. We recall our notation: $r = \operatorname{rank} G$, h is the Coxeter number $\frac{\dim G}{r} - 1$, and W_G is the Weyl group of G (uniquely determined up to isomorphism). Also fix $q = p^e$ for some prime p.

The group W_G has a natural reflection representation V of dimension r. Let $k[V]$ denote the coordinate ring of V, a polynomial ring in r generators. By general theory (cf.[B], Chap V, §5), the ring of invariants $k[V]^{W_G}$ is a graded polynomial ring in r generators, $P_1, \dots, P_r$ say. Moreover, the degrees $2 = d_1 \le d_2 \le \cdots \le d_r = h$ of these generators $P_1, \dots, P_r$ are uniquely determined. The invariant degrees are listed in Table 1.

Now let Γ be either $\mathrm{SL}_2(q)$ or $\mathrm{GL}_2(q)$. Let U be the unipotent subgroup of Γ consisting of all upper triangular unipotent matrices, so U is an elementary abelian group of type $(p, \dots, p)$ (e times). Suppose we have a map

$$f : \Gamma \to G,$$

which is *nondegenerate* in the sense that $\ker f$ is contained in the center of Γ. We say that f is of *toral type* if $f(U)$ is contained in a torus of G.

TABLE 1: INVARIANT DEGREES

G	degrees	$\dim G$	h
A_r	$2,3,\ldots,r+1$	$(r+1)^2-1$	$r+1$
B_r	$2,4,\ldots,2r$	$2r^2+r$	$2r$
C_r	$2,4,\ldots,2r$	$2r^2+r$	$2r$
D_r	$2,4,\ldots,2r-2,r$	$2r^2-r$	$2r-2$
G_2	2,6	14	6
F_4	2,6,8,12	52	12
E_6	2,5,6,8,9,12	78	12
E_7	2,6,8,10,12,14,18	133	18
E_8	2,8,12,14,18,20,24,30	248	30

In the remaining lectures we will give a partial proof of the following:

Main Theorem. *Suppose $q \geq 5$. There exists a nondegenerate map*

$$f : \mathrm{SL}_2(q) \to G$$

of toral type if and only if $q-1$ divides $2d$ for some degree d.

We begin with the easy implication, namely, that the existence of such a map f implies that $q-1$ divides some $2d$. In fact one proves more: if there is a nondegenerate toral map from a Borel subgroup of $\Gamma = \mathrm{SL}_2(q)$ to G then $q-1$ divides $2d$.

Let T be a maximal torus in G, N its normalizer. Then $N/T = W_G$ acts on T. Moreover, N *controls the fusion* of T in G; this means:

(F) . *If A and A' are subsets of T, $g \in G$ with $gAg^{-1} = A'$ then there exists $n \in N$ such that $nan^{-1} = gag^{-1}$ for all $a \in A$.*

We will also need the following theorem of Springer [Sp2]:

(Sp). *Let $m \geq 1$. The following are equivalent:*

(i) *m divides one of the degrees of W_G;*
(ii) *there exists $w \in W_G$ and an eigenvalue λ of w (for the natural representation) whose order is m.*

We assume now that q is odd (the even case being similar). Let B be the Borel subgroup of $\mathrm{SL}_2(q)$ consisting of all upper triangular matrices. Let f be a nondegenerate homomorphism of B into G. Let A be the image of U; we can assume that $A \subset T$. Then $A \cong \mathbb{F}_q$ and B acts upon A as squares, that is, conjugating by $\left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right)$ acts as multiplication by t^2. In particular there exists an automorphism σ of A induced by B of the form $a \mapsto \lambda a$ for $\lambda \in \mathbb{F}_q^*$ of order $\frac{q-1}{2}$.

Now, σ has an eigenvalue in $\overline{\mathbb{F}}_p$ of order $\frac{q-1}{2}$, and by (F) above, the action of σ is induced by an element $w \in W_G$. Viewing A as a subset of $T[p]$, which is the reduction modulo p of the standard representation of W_G, we deduce that in characteristic zero there exists an eigenvalue of w which has order $\frac{q-1}{2}p^\alpha$ for some α. By (Sp), $\frac{q-1}{2}p^\alpha$ divides some degree d, as required.

Note that the same arguments apply (with minor modifications) to maps from $\Gamma = \mathrm{GL}_2(q)$ to G as well: in this case, one finds that $q-1$ divides one of the degrees.

Now we turn to the converse. The case where G is classical can be handled directly using the knowledge of the character table of $\Gamma = \mathrm{PSL}_2(\mathbb{F}_q)$. For instance, if G is of type A, one uses the irreducible representation of Γ of degree $\frac{q-1}{2}$ (assuming $p \neq 2$; if $p = 2$, use a representation of degree $q-1$).

So let G be exceptional. One can easily work out which $\mathrm{PSL}_2(q)$ need to be constructed, remembering our assumption $q \geq 5$:

- For G_2, $q-1$ should divide 4 or 12. But there is a subgroup A_2 of G_2, and the case $q-1$ divides 6 has been treated already, working inside this A_2. So one just needs to embed $\mathrm{PSL}_2(13)$ into $G_2(k)$.
- Again, for F_4, $q-1$ should divide $4, 12, 16$ or 24, but most of the first two cases have already been dealt with since F_4 contains a subgroup G_2. So we need embeddings of $\mathrm{PSL}_2(17)$ and $\mathrm{PSL}_2(25)$.
- For E_6 the new cases are $q = 11, 19$.
- For E_7, they are $q = 29, 37$.
- For E_8, they are $q = 31, 41, 49, 61$.

We will give a uniform proof of existence in all these cases provided q is prime. The missing cases (essentially, $q = 25$ for F_4 and 49 for E_8) have been done by computer calculation, cf. [GR].

Some can be done right away with the next theorem, which for instance covers E_8 for $q = 31$.

Theorem 1. ([S3]) *Let k be an algebraically closed field of characteristic 0. If $p = h+1$ is prime, then there exists a nondegenerate toral map* $\mathrm{PGL}_2(\mathbb{F}_p) \to G$.

Let us sketch the proof. We may assume that G is split, so that $G(R)$ makes sense for any ring R. In particular we have $G(\mathbb{Z}/p\mathbb{Z})$, $G(\mathbb{Z}/p^2\mathbb{Z})$, etc... and

$$\varprojlim G(\mathbb{Z}/p^r\mathbb{Z}) = G(\mathbb{Z}_p)$$

where $\mathbb{Z}_p$ denotes the ring of p-adic integers. Let us start from an embedding of $\mathrm{PGL}_2(\mathbb{F}_p)$ into $G(\mathbb{F}_p)$ in which the non-trivial elements of U are regular unipotent elements of $G(\mathbb{F}_p)$. The existence of such an embedding over $\mathbb{F}_p$ was proved by Testerman (this requires $p \geq h$ which is true in our setting: $p = h + 1$) see [Te] and [S3].

This embedding of Γ into $G(\mathbb{F}_p)$ lifts to $G(\mathbb{Z}/p^2\mathbb{Z})$:

$$\begin{array}{ccccccccc} 1 & \rightarrow & \mathrm{Lie}\, G_{/\mathbb{F}_p} & \rightarrow & G(\mathbb{Z}/p^2\mathbb{Z}) & \rightarrow & G(\mathbb{Z}/p\mathbb{Z}) & \rightarrow & 1 \\ & & & & & & \uparrow & & \\ & & & & & & \Gamma & & \end{array}$$

Indeed, the obstruction to such a lift is 0 because of:

Theorem 2. *$H^i(\Gamma, \mathrm{Lie}\, G_{/\mathbb{F}_p}) = 0$ for $i \geq 1$.*

The proof of Theorem 2 uses the embedding

$$H^i(\Gamma, \mathrm{Lie}\, G_{/\mathbb{F}_p}) \hookrightarrow H^i(C_p, \mathrm{Lie}\, G_{/\mathbb{F}_p}),$$

where $C_p \cong U$ is a Sylow p-subgroup of Γ. Now,

$$\dim H^0(C_p, \mathrm{Lie}\, G_{/\mathbb{F}_p}) = \dim\,(\text{Lie algebra of the centralizer of } C_p)$$

and, since the non-trivial elements of C_p are regular, this dimension is r, cf. [St]. Using the fact that $\dim G = pr$, one sees that every Jordan block of the action of C_p on $\mathrm{Lie}\, G_{/\mathbb{F}_p}$ has size p, and $H^i(C_p, \mathrm{Lie}\, G_{/\mathbb{F}_p}) = 0$ as required.

Hence, the lifting to $\mathbb{Z}/p^2\mathbb{Z}$ is possible. The same argument applies to $\mathbb{Z}/p^3\mathbb{Z}$, etc. One ends up with an embedding of $\mathrm{PGL}_2(\mathbb{F}_p)$ in $G(\mathbb{Z}_p)$, hence in $G(\mathbb{Q}_p)$. Since $\mathbb{Q}_p$ is of characteristic 0, an easy argument then gives an embedding in $G(\mathbb{C})$ (or even in $G(K)$ where K is a number field), as was to be shown.

Remark. In Theorem 1, the hypothesis that k has characteristic 0 can be suppressed (cf.[S3]), except in one case: G of type A_1, and k of characteristic equal to 2. (Indeed, there is no embedding of S_4 into $\mathrm{PGL}_2(k)$ when $\mathrm{char}(k) = 2$.)

Lecture 3

Let us give a sketch of an existence proof in the remaining cases of the Main Theorem with q prime, postponing some of the technical details until Lecture 4.

As before let G be quasi-simple and split over $\mathbb{Z}$. Let h be its Coxeter number. Suppose we have a non-trivial morphism $\phi : \mathrm{SL}_2 \to G$ such that:

(1) ϕ is defined over the local ring of $\mathbb{Z}$ at p, i.e. over $\mathbb{Z}_{(p)}$;
(2) writing $\mathrm{Lie}\, G = \bigoplus L(n_i)$ where $L(n_i)$ is the irreducible representation of SL_2 with highest weight n_i, we require that all n_i are $< p$, exactly one n_i equals 2, and exactly one n_i equals $p-3$;
(3) $p > h$.

We will prove:

Theorem 3. *If* $\phi : \mathrm{SL}_2 \to G$ *is a morphism satisfying the above conditions, then there exists a non-degenerate morphism* $\mathrm{SL}_2(\mathbb{F}_p) \to G(\mathbb{C})$.

As a special case take ϕ to be the principal embedding, as discussed by Kostant and others [K]. Here property (1) has been verified by Testerman [Te]. Denoting the invariant degrees $d_1, \ldots, d_r$, the n_i in this case are

$$\{2d_i - 2 \mid i = 1, \ldots, r\}.$$

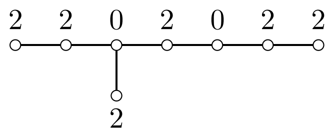
In particular the largest n_i is $2h-2 = p-3$ and the conditions (2) and (3) are satisfied. We then obtain as a consequence of Theorem 3 a proof of a well known conjecture of Kostant (in the special case where $2h+1$ is prime).

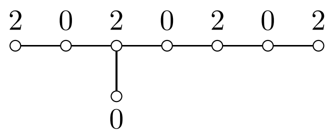
As another special case consider $G = \mathrm{SL}_n$, with degrees are $2, 3, \ldots, n$. The n_i's are $\{2d_i - 2 \mid i = 1, \ldots, r\}$. So taking $n = \frac{p-1}{2}$, the conditions of the theorem are satisfied, and we recover the well known fact (due to Frobenius) that $\mathrm{SL}_2(\mathbb{F}_p)$ has an irreducible character of degree $\frac{p-1}{2}$. The existence of an irreducible character of degree $\frac{p+1}{2}$ can be proved similarly.

Other examples come from Dynkin's classification of A_1 type subgroups of simple algebraic groups in characteristic 0 (see [Dy]). Dynkin's work shows that such embeddings are determined uniquely up to conjugacy in the following way. Let $\phi : \mathrm{SL}_2 \hookrightarrow G$ be an embedding and $\{\alpha_1, \ldots, \alpha_r\}$ a base of the root system of G. We may assume that ϕ maps the maximal torus $\mathbb{G}_m$ of SL_2 into the maximal torus T of G. For a root α, the inner product $\langle \phi, \alpha \rangle$ is defined as the integer corresponding to the composite function

$$\mathbb{G}_m \xrightarrow{\phi|_{\mathbb{G}_m}} T \xrightarrow{\alpha} \mathbb{G}_m.$$

We may also assume that ϕ belongs to the Weyl chamber, i.e. that all $\langle \phi, \alpha_i \rangle$ are ≥ 0. Then the embedding ϕ is determined up to conjugacy by the weights $\langle \phi, \alpha_i \rangle$ for $i = 1, \dots, r$. Writing these on the corresponding nodes of the Dynkin diagram of G, we obtain a *labelled diagram* determining the embedding ϕ. Dynkin worked out precisely which labelled diagrams can arise. We mention two examples with $G = E_8$ when the labelled diagrams are:





One shows that Theorem 3, applied to such diagrams, gives embeddings with $p = 41$ and $p = 31$. Similarly, one gets $p = 29$ and $p = 37$ for E_7. (All these cases have also been done by computer, except $p = 29$.)

We now begin the proof of the theorem. Let $\mathbb{Q}_p$ be the field of p-adic numbers. It is not possible to work over $\mathbb{Q}_p$ as, for example, the values of the character of $\mathrm{SL}_2(p)$ of degree $\frac{p-1}{2}$ involve $\frac{-1+\sqrt{\pm p}}{2}$. So we need to work over the ramified extension $K_{p,u} := \mathbb{Q}_p(\sqrt{pu})$ where u is a unit in $\mathbb{Z}_p$ (there are only two cases according as u is square $\mathrm{mod}\, p$ or not). Set $R_{p,u} := \mathbb{Z}_p[\sqrt{pu}]$, the corresponding ring of integers, with residue field $\mathbb{F}_p$ as before. We will prove:

Theorem 4. *One may choose u so that the subgroup $\phi(\mathrm{SL}_2(\mathbb{F}_p)) \subset G(\mathbb{F}_p)$ can be lifted to a subgroup of $G(R_{p,u})$.*

Viewing $G(R_{p,u})$ as a subgroup of $G(\mathbb{C})$ this implies Theorem 3.

To prove Theorem 4, we first abbreviate $R = R_{p,u}$, $\pi = \sqrt{pu}$, $A = \phi(\mathrm{SL}_2(\mathbb{F}_p))$. As G is smooth, we have surjective maps $G(R) \to G(R/\pi^n R)$ with kernels denoted G_n. Then $G = G_0 \supset G_1 \supset \dots$ and $G = \varprojlim G/G_n$. We note the following basic properties (cf. [DG]):

$$
\begin{aligned}
G/G_1 &= G(\mathbb{F}_p) \\
G/G_2 &= G(R/\pi^2 R) = G(R/pR) \cong \mathrm{Lie}_p\, G \rtimes G(\mathbb{F}_p) \\
(G_i, G_j) &\subset G_{i+j} \\
G_i/G_{i+1} &\cong \mathrm{Lie}_p\, G
\end{aligned}
$$

By assumption, A is embedded in G/G_1, and we would like to lift this to G/G_2. The split exact sequence

$$1 \to \operatorname{Lie}_p G \to G/G_2 \to G/G_1 \to 1$$

gives an obvious lift $\sigma : A \to G/G_2$. However, this σ does not lift to G/G_3, so we need to modify it. For any $\alpha \in H^1(A, \operatorname{Lie}_p G)$ represented by a 1-cocycle a, we can define a new lift $\sigma_a(s)$ by setting $\sigma_a(s) = \sigma(s)a(s)$. Two liftings are conjugate by an element in the kernel if and only if the corresponding cocycles are cohomologous. So studying $H^1(A, \operatorname{Lie}_p G)$ is crucial. We will show that there is a choice of α which allow us to continue lifting to every G/G_n.

Hypothesis (2) is known to imply that $\operatorname{Lie}_p G = \bigoplus L(n_i)_p$ with $n_i < p$. When $n < p$ one can show that $\dim H^1(A, L(n))$ is 1 if $n = p - 3$ and zero otherwise. When $n < p - 1$ one can show that $\dim H^2(A, L(n))$ is 1 if $n = 2$ and zero otherwise. Hence

$$\dim H^1(A, \operatorname{Lie}_p G) = 1 \quad \text{and} \quad \dim H^2(A, \operatorname{Lie}_p G) = 1.$$

We wish to use the sequence $\operatorname{Lie}_p G \to G/G_3 \to G/G_2$ to lift $A \xrightarrow{\sigma} G/G_2$ to a map $A \to G/G_3$. The corresponding obstruction is denoted by $\operatorname{obs}(\sigma) \in H^2(A, \operatorname{Lie}_p G)$. With σ equal to the lift of the original embedding $A \hookrightarrow G/G_1$ we have $\operatorname{obs}(\sigma) \neq 0$. Now if we take $\alpha \in H^1(A, \operatorname{Lie}_p G)$ and calculate σ_α one finds (cf. Lecture 4) that $\operatorname{obs}(\sigma_\alpha) = \operatorname{obs}(\sigma) + \frac{1}{2}[\alpha, \alpha]$ where $[\ ,\ ]$ is the cup product in cohomology induced by

$$[\ ,\ ] : \operatorname{Lie}_p G \times \operatorname{Lie}_p G \to \operatorname{Lie}_p G.$$

So we try to choose α such that $\operatorname{obs}(\sigma) + \frac{1}{2}[\alpha, \alpha] = 0$. If there is no α satisfying this equation, then we change our choice of u (in fact in all the cases I know, the choice of $u = -1$ works).

So now we may assume that $A \xrightarrow{\sigma} G/G_2$ is liftable to G/G_3. Call this lift τ. The lift to G/G_4 may again have a non-trivial obstruction in $H^2(A, \operatorname{Lie}_p G)$. Again one can modify τ by a 1-cocycle $b : A \to \operatorname{Lie}_p G$, and one proves that $\operatorname{obs}(\tau_b) = \operatorname{obs}(\tau) + [\alpha, \beta]$, where β is the class of b in $H^1(A, \operatorname{Lie}_p G)$. Since $\alpha \neq 0$ one can choose β such that $[\alpha, \beta] = -\operatorname{obs}(\tau)$, hence $\operatorname{obs}(\tau_b) = 0$ and τ_b can be lifted to G/G_4.

The process continues in this manner: we obtain inductively a lift of a map $A \to G/G_n$ to G/G_{n+1} and then modify this lift to get a map to G/G_{n+2}. Putting it all together completes our sketch of the proof of Theorem 4.

Lecture 4

In this lecture, we go back to discuss some of the technical points arising in the proof of Theorem 4. We will consider a general setup which includes the situation considered in Lecture 3.

Consider a sequence of surjective group homomorphisms $E_3 \to E_2 \to E_1$ with $M_1 = \ker E_3 \to E_2$, $M_2 = \ker E_3 \to E_1$ and $M_3 = \ker E_2 \to E_1$. One has a short exact sequence:

$$1 \to M_1 \to M_2 \to M_3 \to 1.$$

Assumption A. Assume that M_1, M_3 are abelian, and M_1 is in the center of M_2. (This gives natural actions of E_2 on M_2 and of E_1 on M_1 and M_3.)

Now let A be a group and $\phi : A \to E_2$. Call $\mathrm{obs}(\phi) \in H^2(A, M_1)$ the obstruction to lifting ϕ to $A \to E_3$. Let x be a 1-cocycle $A \to M_3$, and ϕ_x be the map $s \mapsto x(s)\phi(s)$ of A into E_2. Write $\underline{x}$ for the class of x in $H^1(A, M_3)$. We want to compare $\mathrm{obs}(\phi)$ and $\mathrm{obs}(\phi_x)$; note that A acts the same way on M_1 by ϕ or by ϕ_x since E_1 acts on M_1. We have the following key formula:

Proposition 1. $\mathrm{obs}(\phi_x) = \mathrm{obs}(\phi) + \Delta(\underline{x})$

where $\Delta : H^1(A, M_3) \to H^2(A, M_1)$ is the (non-abelian) coboundary map associated with the exact sequence of A-groups:

$$1 \to M_1 \to M_2 \to M_3 \to 1,$$

(cf. [S4] Ch I, §5.7). This formula will be verified by a direct computation given at the end of the lecture.

Next, we want to compute $\Delta : H^1(A, M_3) \to H^2(A, M_1)$. We make the following assumption:

Assumption B. The map $m \mapsto m^2$ of M_1 onto itself is bijective (in additive notation M_1 is a $\mathbb{Z}[\frac{1}{2}]$-module).

This allows us to define an *addition* in M_2 by $x + y = x.y.(x, y)^{-1/2}$ (note that (x, y) is the usual commutator and belongs to M_1) and a *Lie bracket* $[x, y] = (x, y)$. This makes M_2 into *a Lie algebra.* (I am using here an elementary case of the inversion of the Hausdorff formula, cf. [B], Chap II, §6.)

Call M_2^{ab} the corresponding abelian group. We have an exact sequence of A-modules:

$$0 \to M_1 \to M_2^{\mathrm{ab}} \to M_3 \to 0,$$

hence by (abelian) cohomology an additive map

$$\delta : H^1(A, M_3) \to H^2(A, M_1).$$

On the other hand the bracket defines a bilinear map

$$M_3 \times M_3 \to M_1,$$

hence a (cup product) map

$$H^1(A, M_3) \times H^1(A, M_3) \to H^2(A, M_1)$$

which we denote by $\alpha, \beta \mapsto [\alpha.\beta]$. It is symmetric. We can now state the formula giving Δ:

Proposition 2. $\Delta(\alpha) = \delta(\alpha) + \frac{1}{2}[\alpha.\alpha]$ *for every* $\alpha \in H^1(A, M_3)$.

This is verified again by a direct computation which we will give at the end of the lecture. Note that $\delta(\alpha)$ is linear in α and $[\alpha.\alpha]$ is quadratic; hence Δ is a polynomial function of degree 2. We conclude with the computations mentioned above.

Computations for Proposition 1. If $s \in A$, one has $\phi(s) \in E_2$; choose $z_s \in E_3$, with $z_s \mapsto \phi(s)$. This defines a 2-cocycle $o(s,t)$ by the usual formula

$$z_s z_t = o(s,t) z_{st}\ , \quad o(s,t) \in M_1.$$

The class of $o(s,t)$ in $H^2(A, M_1)$ is $\mathrm{obs}(\phi)$.

Similarly, choose $b_s \in M_2$ with $b_s \mapsto x(s)$ in M_1. By [S4], *loc. cit.*, $\Delta(\underline{x})$ is the class in $H^2(A, M_1)$ of the 2-cocycle $\Delta(s,t)$ defined by

$$\Delta(s,t) = b_s.{}^s b_t.b_{st}^{-1}$$

(where ${}^s b_t$ means the transform of b_t by $\phi(s)$, i.e. $z_s b_t z_s^{-1}$.) Since $\phi_x(s) = x(s)\phi(s)$ we may choose $b_s z_s$ as a lifting of $\phi_x(s)$ in E_3. This gives a cocycle $o_x(s,t)$ by:

$$b_s z_s.b_t z_t = o_x(s,t).b_{st} z_{st}$$

and the class of $o_x(s,t)$ is $\mathrm{obs}(\phi_x)$.

We calculate $b_s z_s b_t z_t$:

$$\begin{aligned} b_s.z_s b_t z_s^{-1}.z_s z_t &= b_s.z_s b_t z_s^{-1}.o(s,t) z_{st} \\ &= b_s.{}^s b_t.o(s,t).z_{st} \\ &= \Delta(s,t) b_{st} o(s,t) z_{st}. \end{aligned}$$

Hence $o_x(s,t)b_{st} = \Delta(s,t)b_{st}o(s,t)$. Since b_{st} commutes with $o(s,t)$, this gives $o_x(s,t) = \Delta(s,t).o(s,t)$, as desired.

Computations for Proposition 2. Choose a 1-cocycle (a_s) of A in M_3 representing the class α, and lift a_s to $b_s \in M_2$. The cocycle $\Delta(s,t)$ defined by

$$\Delta(s,t) = b_s.{}^s b_t.b_{st}^{-1}$$

represents $\Delta(\alpha)$, cf. above.

On the other hand, the coboundary $\delta(\alpha)$ may be represented by the 2-cocycle $\delta(s,t)$ given by

$$\delta(s,t) = b_s * {}^s b_t * b_{st}^{-1},$$

where $x * y$ is the product of x, y with respect to the composition law $x.y.(x,y)^{-1/2}$. By collecting terms, this gives

$$\delta(s,t) = \Delta(s,t)\gamma(s,t),$$

where $\gamma(s,t) = (b_s, {}^s b_t)^{-1/2}(b_s {}^s b_t, b_{st}^{-1})^{-1/2}$. In additive notation, this means:

$$\gamma(s,t) = -\frac{1}{2}[a_s, {}^s a_t] + \frac{1}{2}[a_s + {}^s a_t, a_{st}].$$

But $a_s + {}^s a_t = a_{st}$, since a is a 1-cocycle. Hence the last term is 0. As for $s, t \mapsto [a_s, {}^s a_t]$, it is the cup-product (with respect to $[\ ,\ ]$) of the cocycle a with itself. Hence $\gamma = -\frac{1}{2}[\alpha.\alpha]$ and since $\Delta(\alpha) = \delta(\alpha) - \underline{\gamma}(\alpha)$, where $\underline{\gamma}(\alpha)$ is the class of $\gamma(s,t)$, this gives the required formula.

Part II

The notion of complete reducibility in group theory

Lecture 1

Let Γ be a group. We will discuss *linear representations* of Γ over some fixed field k of characteristic $p \geq 0$. By this we mean a group homomorphism $\Gamma \to \mathrm{GL}(V)$ for some finite dimensional vector space V over k. We will usually refer to V instead as a Γ-module, though of course technically we should say $k[\Gamma]$-module where $k[\Gamma]$ denotes the group algebra of Γ over k. Recall that V is *irreducible* or *simple* if:

(1) $V \neq 0$;
(2) no subspace of V is Γ-stable apart from 0 and V.

One says that V is *completely reducible* or *semisimple* if V is a direct sum of irreducible submodules; equivalently, V is semisimple if V is generated by irreducible submodules.

The category of semisimple Γ-modules is stable under the usual operations of linear algebra. In other words one can take Γ-stable subspaces, quotients, direct sums and duals all within this category. Indeed, all of these statements (apart from dual spaces) are true for modules over an arbitrary ring. But when we consider groups, we can also consider the operations of multilinear algebra. For instance, given two Γ-modules V_1, V_2 we can impose a Γ-module structure upon $V_1 \otimes V_2$ using the diagonal map $\Gamma \to \Gamma \times \Gamma$. From this we can construct exterior powers, symmetric powers, etc....

Around 1950, Chevalley proved the following simple looking result:

Theorem 1. (cf. [C]) *Suppose that k has characteristic 0. If V_1, V_2 are semisimple Γ-modules, then $V_1 \otimes V_2$ is again semisimple.*

An interesting feature of this result is that, although it is stated in elementary terms, the only known proofs involve some algebraic geometry. We sketch the idea. One starts with a series of reductions, reducing to the case that k is algebraically closed and Γ is a subgroup of $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$. Then one replaces Γ by its Zariski closure in $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$. So now Γ is an algebraic group. The connected component Γ° of Γ containing the identity is a normal subgroup of Γ of finite index (this is one bonus of using the Zariski topology). In other words, Γ/Γ° is a finite group and since the characteristic is 0, one easily then reduces to the case that $\Gamma = \Gamma^\circ$. So now, Γ is connected. Let $R^u\Gamma$ be the unipotent radical of Γ, i.e. its largest normal unipotent subgroup. In any semisimple representation, $R^u\Gamma$ acts trivially, and the converse is known to be true in characteristic zero. Since V_1 and V_2 are semisimple and the representation of Γ on $V_1 \oplus V_2$ is faithful, we deduce that $R^u\Gamma$ is trivial, and we are done.

Now we ask what happens for $p > 0$. Chevalley's result does not remain true in general. For instance, consider $\Gamma = \mathrm{SL}_2(k) = \mathrm{SL}(V)$ with $\dim V = 2$. Let $\mathrm{Sym}^n(V)$ be n^{th} symmetric power of V. If $n < p$ then $\mathrm{Sym}^n(V)$ is an irreducible representation of Γ. But if $n = p$, the subspace $V^{[1]} \subset \mathrm{Sym}^p(V)$ generated by x^p and y^p, where $\{x, y\}$ is any basis of V, is stable under the action of Γ. This gives a short exact sequence

$$0 \to V^{[1]} \to \mathrm{Sym}^p(V) \to L \otimes \mathrm{Sym}^{p-2}(V) \to 0$$

where $L = \det V$ is one-dimensional. This sequence does not split (unless $p = |k| = 2$). So $\mathrm{Sym}^p(V)$ is not semisimple in general. Hence, $V \otimes \ldots \otimes V$ (p times) is not semisimple either.

Now a general principle is that if a statement is true in characteristic zero then it is also true for "large" p. In keeping with this, we have the following:

Theorem 2. ([S1]) *Let $V_1, \ldots, V_n$ be semisimple Γ-modules. Then*

$$V_1 \otimes \ldots \otimes V_n \text{ is semisimple if } p > \sum_{i=1}^{n} (\dim V_i - 1).$$

The proof again uses a reduction to algebraic group theory. As above we may assume that k is algebraically closed, the representation $\Gamma \to \mathrm{GL}(V)$ is faithful and Γ is a closed subgroup of $\mathrm{GL}(V)$ in the Zariski topology, where $V = V_1 \oplus \ldots \oplus V_n$. But we can no longer reduce to the case that Γ is connected. Indeed, if Γ is finite of order divisible by p, this assumption will be no help at all. So we need to do more. We need Γ to be *saturated*.

To define this notion (cf. [N],[S1]), suppose that $x \in \mathrm{GL}_n(k)$ has order p. Write $x = 1 + \varepsilon$ for some matrix ε and note that $\varepsilon^p = 0$. For any $t \in k$ define $x^t := 1 + t\varepsilon + \binom{t}{2}\varepsilon^2 + \ldots + \binom{t}{p-1}\varepsilon^{p-1}$. Since $\varepsilon^p = 0$ we have constructed a one parameter subgroup $\{x^t \mid t \in k\}$ of $\mathrm{GL}_n(k)$. By definition, a subgroup $\Gamma \subset \mathrm{GL}_n(k)$ is said to be *saturated* if it is Zariski closed and $x \in \Gamma$ with $x^p = 1$ implies that $x^t \in \Gamma$ for all $t \in k$. One can define the *saturated closure* of a subgroup Γ denoted by Γ^{sat}. It is the smallest saturated subgroup of $\mathrm{GL}_n(k)$ containing Γ.

Here are some examples:

- If $p > 2$ every classical group in its natural representation is saturated.
- If $p > 3$ the group $G_2(k)$, embedded in $\mathrm{GL}_7(k)$, is saturated.

- If $p = 2$ the group $\mathrm{PGL}_2(k)$, embedded in $\mathrm{GL}_3(k)$ by its adjoint representation, is not saturated.
- If $p = 11$ the Janko group J_1, embedded in $\mathrm{GL}_7(k)$, has for saturated closure the group $G_2(k)$.

It can be checked that our problem is stable under replacing Γ by Γ^{sat}. So, we may assume that Γ is saturated. This implies that Γ/Γ° is finite of order prime to p, so we can reduce as before to the case where Γ is a connected reductive algebraic group. Then we resort to the general theory of representations of algebraic groups to complete the proof, which is somewhat technical. (cf. [S1])

One can also ask about various converse theorems (cf. [S2]). For instance:

(1) Does $V_1 \otimes V_2$ semisimple imply V_2 semisimple?
(2) Does $\bigwedge^2 V$ semisimple imply V semisimple?
(3) Does $\mathrm{Sym}^2 V$ semisimple imply V semisimple?

For question (1) the answer in characteristic zero is yes unless $\dim V_1 = 0$. In characteristic $p > 0$, the answer is yes unless $\dim V_1 = 0$ in k, i.e. unless $\dim V_1 \equiv 0 \pmod{p}$.

For question (2) the answer in characteristic zero is yes unless $\dim V = 2$. In characteristic $p > 0$ the answer is yes unless $\dim V \equiv 2 \pmod{p}$.

For question (3) the answer is yes in characteristic zero, while in characteristic $p > 0$ the answer is yes unless $\dim V \equiv -2 \pmod{p}$.

Remarks. These questions make sense more generally in the setting of a "tensor category", cf. [D]. Such a category has tensor products and duals, as well as a distinguished object $\underline{1}$. There is the notion of dimension of an object: consider the composition of the natural maps

$$\underline{1} \to V \otimes V^* \to \underline{1}.$$

This determines an element of $k = \mathrm{End}(\underline{1})$, which is called the dimension of V. In particular it is possible for the dimension to be -2 in k. In this formalism, there is a way of transforming symmetric powers into exterior powers, by changing categories. Deligne noticed that if one proves in this setting one of the two statements:

$$\bigwedge^2 V \text{ semisimple} \Rightarrow V \text{ semisimple if } \dim V \neq 2 \text{ in } k$$
$$\mathrm{Sym}^2 V \text{ semisimple} \Rightarrow V \text{ semisimple if } \dim V \neq -2 \text{ in } k$$

then the other is true as well (cf. [S2],§6.2). (Here k is assumed to be of characteristic not equal to 2.)

W. Feit has provided various counterexamples showing that the results are essentially the 'best possible' for questions (1) and (2), (cf. [S2], appendix). The situation is different for question (3). For instance, with $p = 7$ there is no known example in which $\mathrm{Sym}^2 V$ is semisimple but V is not.

We turn now to giving a generalization of the notion of complete reducibility (cf. [T2]). Let k be algebraically closed, G be a connected, reductive algebraic k-group and $\Gamma \subset G(k)$. I shall say that Γ is *G-completely reducible* (G-cr for short) if for every parabolic subgroup P of $G(k)$ containing Γ there exists a Levi subgroup of P, also containing Γ.

The definition of G-cr may be reformulated within the context of Tits buildings (cf. [T1]). The Tits building of G is the simplicial complex X, with simplices corresponding to the parabolic subgroups of $G(k)$ and inclusions being reversed. The group $G(k)$ acts simplicially on X. So if $\Gamma \subset G(k)$, we can consider the complex X^Γ of all Γ-fixed points. One can prove that there are precisely two possibilities:

(1) X^Γ is contractible (homotopy type of a point);
(2) X^Γ has the homotopy type of a bouquet of spheres.

One can show that (2) occurs precisely when Γ is G-cr.

The property of Γ being G-cr relates nicely to the usual property of a Γ-module being semisimple. If we take G to be $\mathrm{GL}(V)$ for some vector space V, it is clear that Γ is G-cr if and only if V is a semisimple Γ-module. More generally, if $p \neq 2$ and G is any symplectic group, orthogonal group, or G_2 then Γ is G-cr if and only if the natural representation of $G(k)$ is a semisimple Γ-module. We would like in a general setting, given $\Gamma \subset G(k)$ and a linear representation V of $G(k)$, to relate the property "Γ is G-cr" to the property that V is a semisimple Γ-module (for p larger that some bound $n(V)$). This will be discussed in the later lectures.

Finally, we give an application of these ideas. The Dynkin diagram of D_4 has a symmetry of order 3 which gives rise to an automorphism τ of Spin_8. Consequently, there are three irreducible modules for Spin_8 of dimension 8, say V_1, V_2, and V_3. Suppose that Γ is a subgroup of Spin_8. Is it true that:

$$V_1 \text{ is } \Gamma\text{-semisimple} \Rightarrow V_2 \text{ and } V_3 \text{ are } \Gamma\text{-semisimple?}$$

The answer is yes if $p > 2$ (and sometimes no if $p = 2$): this follows from the fact that V_i is Γ-semisimple if and only if Γ is Spin_8-cr.

Lecture 2

Fix an algebraically closed field k and let G be a connected, reductive algebraic k-group. We are interested only in the case where $p = \mathrm{char}\, k > 0$. Recall that a subgroup $\Gamma \subset G(k)$ is called G-cr if for every parabolic subgroup P of $G(k)$ containing Γ, there exists a Levi subgroup of P also containing Γ. We wish to relate this to the usual notion of complete reducibility.

Let T be a maximal torus of G, and B be a Borel subgroup containing T with U its unipotent radical. This determines a root system and a set of positive roots. Let $X(T) = \mathrm{Hom}(T, \mathbb{G}_m)$ be the character group, and $Y(T) = \mathrm{Hom}(\mathbb{G}_m, T) = \mathrm{Hom}(X(T), \mathbb{Z})$ the cocharacter group. We have a natural pairing $\langle ., . \rangle : X(T) \times Y(T) \to \mathbb{Z}$ and for each α in the root system we have the coroot $\alpha^\vee \in Y(T)$.

For each $\lambda \in X(T)$ define

$$n_G(\lambda) = n(\lambda) := \sum_{\alpha>0} \langle \lambda, \alpha^\vee \rangle.$$

Note we can also write this as $\langle \lambda, \phi \rangle$ where $\phi = \sum_{\alpha>0} \alpha^\vee$, the *principal homomorphism* of $\mathbb{G}_m$ into T. If V is any finite dimensional G-module, let us put;

$$n_G(V) = n(V) := \sup n(\lambda)$$

where the supremum is taken over all the weights λ of T in V.

As an example, consider $G = \mathrm{GL}_m$, with V the natural m-dimensional representation. Then $n(V) = m-1 = \dim V - 1$ and $n(\bigwedge^i V) = i(\dim V - i)$. In general, if V_1 and V_2 are any G-modules, $n(V_1 \otimes V_2) = n(V_1) + n(V_2)$.

Note that if V is a *nondegenerate* linear representation of G, i.e. the connected kernel of the representation is a torus, then $n(V) \geq h - 1$, where h is the Coxeter number of G. Indeed, let λ be a highest weight of V. So $n(V) = n(\lambda) = \langle \lambda, \sum_{\alpha>0} \alpha^\vee \rangle \geq \langle \lambda + \rho, \beta^\vee \rangle - 1$, where ρ is half the sum of positive roots and $\beta^\vee$ is the highest coroot. Since λ is nonzero and dominant we have $\langle \lambda, \beta^\vee \rangle \geq 1$ and $\langle \rho, \beta^\vee \rangle = h - 1$.

Our goal is to prove the following result:

Main Theorem. *Let V be G-module with $p > n(V)$. Let Γ be a subgroup of $G(k)$. Then*

$$\Gamma \textit{ is } G\textit{-cr} \Rightarrow V \textit{ is } \Gamma\textit{-semisimple}.$$

Moreover, the converse is true if V is nondegenerate, i.e. the connected kernel of the representation is a torus.

Some of the results mentioned in Lecture 1 are immediate consequences. For example, let $\{V_1, \ldots, V_m\}$ be a collection of semisimple Γ-modules and $p > \sum_i(\dim V_i - 1)$. Then the theorem, applied to $G = \prod \mathrm{GL}(V_i)$ and $V = \bigotimes V_i$, tells us that $V_1 \otimes \cdots \otimes V_m$ is also semisimple. Alternatively, suppose that V is a semisimple Γ-module with $p > i(\dim V - i)$. Then the theorem shows that $\bigwedge^i V$ is Γ semisimple. (This was stated as an open question at the end of [S2]; and the special case where V is irreducible had been proved by McNinch.)

The proof of the main theorem uses the notion of *saturation* with respect to the group G. In order to define it, we need to introduce the "exponential" x^t, for x unipotent in G and $t \in k$. This is possible (for p not too small) thanks to:

Theorem 3. *Assume $p \geq h$ (resp. $p > h$ if G is not simply connected). There exists a unique isomorphism of varieties* $\log : G^u \to \mathfrak{g}_{nilp}$ *with the following properties:*

(i) $\log(\sigma u) = \sigma \log u$ *for all* $\sigma \in \mathrm{Aut}\, G$*;*
(ii) *the restriction of* $\log$ *to* $U(k)$ *is an isomorphism of algebraic groups* $U(k) \to \mathrm{Lie}\, U$*, whose tangent map is the identity;*
(iii) $\log(x_\alpha(\theta)) = \theta X_\alpha$*, for every root* α *and every* $\theta \in k$*.*

Here, $\mathfrak{g}_{\mathrm{nilp}}$ is the nilpotent variety of $\mathrm{Lie}\, G$, $x_\alpha : \mathbb{G}_a \to U_\alpha$ denotes some fixed parameterization of the root group U_α of U, and $X_\alpha = \frac{d}{d\theta}(x_\alpha(\theta))|_{\theta=0}$ is the corresponding basis element of $\mathrm{Lie}\, U_\alpha$. We are viewing $\mathrm{Lie}\, U$ as an algebraic group over k via the Campbell-Hausdorff formula: $XY := X + Y + \frac{1}{2}[X, Y] + \frac{1}{12}[X, [X, Y]] + \ldots$ (cf. [B], Chap II, §6) which makes sense in characteristic p because of the assumption $p \geq h$ and the fact that the nilpotency class of $\mathrm{Lie}\, U$ is at most h.

For the proof, uniqueness is obvious since the U_α generate U and G^u is the union of conjugates of U. (Moreover, one can show that (iii) is a consequence of (i) and (ii).) However, the existence part is less easy. One possible method is to define first log on U and then extend it to G^u. This approach uses the fact that $\mathfrak{g}_{\mathrm{nilp}}$ is a normal variety (cf. [D], [BR]) when p is good, that G^u is a normal variety (cf. [St]) and draws on work by Springer (cf. [Sp2]).

Given the theorem, let $\exp : \mathfrak{g}_{\mathrm{nilp}} \to G^u$ denote the inverse to log. For $x \in G^u(k)$ and $t \in k$ we define x^t as $\exp(t \log x)$. Note that the exponential map $x, t \mapsto x^t$ may be viewed as a morphism $F : G^u \times \mathbb{A}^1 \to G^u$. Moreover this map is the "reduction mod p" of the corresponding well-known map in characteristic zero, and this gives a convenient way to compute it.

Lecture 3

Continue with the notation of the previous lecture. Recall that we have just defined the map $x \mapsto x^t$ for any unipotent element $x \in G(k)$ and any $t \in k$. We can now at last define the saturation process (assuming $p \geq h$). A subgroup Γ of $G(k)$ is *saturated* if

(1) Γ is Zariski closed;
(2) whenever $x \in \Gamma \cap G^u$, we have $x^t \in \Gamma$ for all $t \in k$.

We wish in the remainder of this lecture to describe some basic properties of saturated subgroups and G-cr subgroups. We will apply these properties in Lecture 4 to prove the Main Theorem.

We begin by mentioning some elementary examples: every parabolic subgroup is saturated; the centralizer of any subgroup of $G(k)$ is saturated; Levi subgroups are saturated, since they may be realized as the centralizer of a torus. We also note that in the case of saturated subgroups lying in U, there are various alternative characterizations giving further 'unipotent' examples:

Property 1. *Let V be a closed subgroup of $U(k)$. The following are equivalent:*

(i) *V is saturated;*
(ii) *$V = \exp(\mathfrak{v})$ for $\mathfrak{v}$ a Lie subalgebra of $\operatorname{Lie} U$;*
(iii) *$\log V$ is a vector subspace of $\operatorname{Lie} U$.*

Another basic property is as follows:

Property 2. *Let H be a semisimple subgroup of G with $H(k)$ saturated. If x is any unipotent element of $H(k)$, then the element x^t (defined relative to H) coincides with x^t (defined relative to G).*

Even to state Property 2 correctly, we need first to know that the Coxeter number h_H of H does not exceed the Coxeter number h_G of G. In fact, a stronger result holds:

Theorem 4. *Let p be any prime, and H be a semisimple subgroup of a semisimple group G. Let $d_{i,H}$ and $d_{j,G}$ be the invariant degrees of the Weyl groups of H and G respectively. Then, the polynomial $\prod(1 - T^{d_{i,H}})$ divides $\prod(1 - T^{d_{j,G}})$.*
(For the properties of the invariant degrees, see [B], Chap V, §5.)

As a corollary we see that each $d_{i,H}$ divides some $d_{j,G}$. For, choosing T to be a primitive $d_{j,H}{}^{\text{th}}$ root of unity, the theorem implies that $\prod(1-T^{d_{j,G}})$ vanishes, so $(1-T^{d_{j,G}})$ vanishes for some j. Since the Coxeter number h_H is the largest degree $d_{i,H}$, and similarly for G, we deduce in particular that $h_H \leq h_G$, as required for the statement of Property 2 to make sense.

We sketch the proof of Property 2. Assume that H is a semisimple subgroup of G with $H(k)$ saturated. We may assume that there is a maximal unipotent subgroup U_H of H with $U_H \subset U$. Note that $U_H(k)$ is also a saturated subgroup of G. We need to show that $\log_G(x) = \log_H(x)$ for any unipotent $x \in H(k)$. Conjugating, it suffices to prove this for $x \in U_H(k)$. We have an isomorphism $\log : U(k) \to \operatorname{Lie} U$. Viewing $\operatorname{Lie} U_H$ as a subgroup of $\operatorname{Lie} U$, we conclude that the restriction of $\log_G$ gives a isomorphism $U_H \cong \operatorname{Lie} U_H$ which is compatible with conjugation and whose tangent map is the identity. By the uniqueness in the definition of $\log_H$ we conclude that the restriction of $\log_G$ is equal to $\log_H$, as required.

Property 3. *If $H \subset G$ is saturated then the index $(H : H^\circ)$ is prime to p.*

To prove Property 3, suppose p divides $(H : H^0)$ and take some element x of the finite group H/H^0 of order p. One proves, from general principles, that there exists $\tilde{x} \in H^u(k)$ which maps onto x in the quotient. By saturation, $\{\tilde{x}^t \mid t \in k\}$ is a subgroup of $H(k)$, hence of $H^0(k)$ since it is connected. So $\tilde{x} \in H^0(k)$, a contradiction.

We turn to discussing some basic properties of G-cr subgroups, as defined in Lectures 1 and 2. Recall that given a completely reducible H-module for an algebraic group H, the unipotent radical of H acts trivially. The next property that we will need is similar, but stated intrinsically within the groups.

Property 4. *If Γ is G-cr and V is a normal unipotent subgroup of Γ then $V = 1$. In particular, if in addition Γ is Zariski closed, then Γ^0 is reductive.*

The proof of this depends on the construction of Borel and Tits (cf. [BT]) which associates to the subgroup V a parabolic subgroup P of G with $V \subset R^u(P)$. Now Γ normalizes V, and since P is defined in a canonical fashion, Γ normalizes P. Therefore $\Gamma \subset P$. Now we use the fact that Γ is G-cr to deduce that $\Gamma \cap R^u(P) = 1$, whence $V = 1$.

Property 5. *Let $\Gamma_0 \subset \Gamma$ be a normal subgroup of Γ of index prime to p. Then, Γ_0 is G-cr $\Rightarrow \Gamma$ is G-cr.*

(Before sketching the proof of this, we mention an open problem: if $\Gamma_0 \subset \Gamma$ is normal, is it true that Γ is G-cr $\Rightarrow \Gamma_0$ is G-cr?)

Now for the proof, let P be a parabolic subgroup of G containing Γ, and let L be a Levi subgroup of P which contains Γ_0. Write $P = R^u P \rtimes L$. Let Γ_L be the image of Γ under the projection $P \to L$. The kernel of this projection is $\Gamma \cap R^u P = 1$ so we have an isomorphism $\Gamma \to \Gamma_L$. Then Γ is obtained from Γ_L by a 1-cocycle $a : \Gamma \to R^u P$, with a equal to a coboundary on restriction to Γ_0. This implies that a is induced by a 1-cocycle a' on Γ/Γ_0 with values in $V = R^u P \cap Z(\Gamma_0) = (R^u P)^{\Gamma_0}$. Now, V has a composition series made up of k-vector spaces, and since $|\Gamma/\Gamma_0|$ is prime to p, the cocycle induced by a' on each such composition factor is a coboundary. This implies that a', whence a, is a coboundary, so that we can conjugate Γ to a subgroup of L, as required.

Lecture 4

Now we proceed to prove the Main Theorem. We begin with:

Theorem 5. *Suppose $p \geq h$. Let V be a G-module with associated representation $\rho_V : G \to \mathrm{GL}(V)$. For every unipotent element u of G, let $d_u(V)$ be the degree of the polynomial map $t \mapsto \rho_V(u^t) \in \mathrm{End}(V)$. Then $d_u(V) \leq n(V)$, and there is equality if u is regular.*

The proof is in several steps.

(1) *The case $G = \mathrm{SL}_2$.* In this case we may assume $u = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $u^t = \left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$, and we have to prove $d_u(V) = n(V)$.

(1.1) *One has $d_u(V) \leq n(V)$.* Write $\rho_V(u^t)$ as $1+\sum_{i\geq 1} a_i t^i$, $a_i \in \mathrm{End}(V)$. If $s_\lambda = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ with $\lambda \in k^*$, we have $s_\lambda u^t s_\lambda^{-1} = u^{\lambda^2 t}$, hence

$$\rho^V(s_\lambda).\sum a_i t^i.\rho_V(s_\lambda^{-1}) = \sum a_i \lambda^{2i} t^i,$$

which implies $\rho_V(s_\lambda) a_i \rho_V(s_\lambda)^{-1} = \lambda^{2i} a_i$ for every i. Hence a_i has weight $2i$ in $\mathrm{End}(V) = V \otimes V^*$. By definition of the invariant n this shows that $a_i \neq 0 \Rightarrow 2i \leq n(V \otimes V^*) = n(V) + n(V^*) = 2n(V)$, i.e. $i \leq n(V)$. Hence $d_u(V) \leq n(V)$.

(1.2) *One has $d_u(V) \geq n(V)$.* If V has Jordan-Hölder quotients V_α, it is clear that $n(V) = \sup n(V_\alpha)$, $d_u(V) \geq \sup d_u(V_\alpha)$. Hence we may assume that V is simple. In that case, the equality $n(V) = d_u(V)$ is obvious from the explicit description of V à la Steinberg.

(2) *The case G arbitrary, u regular.* Choose a principal homomorphism $\mathrm{SL}_2 \to G$, (cf. [Te] - see also [S3]). It is known that a nontrivial unipotent

of SL_2 gives a regular unipotent of G. On the other hand, one has $n_G(V) = n_{\mathrm{SL}_2}(V)$, almost by definition. Hence the result follows from (1).

(3) *General case.* For u unipotent of G, write $\rho_V(u^t)$ as above:

$$\rho_V(u^t) = 1 + \sum a_i(u)t^i \in \mathrm{End}(V).$$

The a_i are regular functions of u (viewed as a point of the unipotent variety G^u). If $i < n(V)$ then $a_i(u)$ is 0 when u is regular, by (2). Since the regular unipotents are dense in G^u, this implies $a_i(u) = 0$ for every u.

Corollary 1. *If H is a reductive and saturated subgroup of G, one has $n_H(V) \leq n_G(V)$.*

Choose a regular unipotent element $u \in H$. One gets $n_H(V) = d_u(V) \leq n_G(V)$ by Theorem 5, applied to both H and G.

Corollary 2. *The following are equivalent:*

(i) $p > n(V)$;
(ii) $\rho_V(u^t) = \rho_V(u)^t$ *for every unipotent u of G, and every $t \in k$.*

Indeed (ii) holds if and only if the degree of $t \mapsto \rho_V(u^t)$ is $< p$, i.e. if and only if $d_u(V) < p$. Since $n(V) = \sup_u d_u(V)$, this shows the equivalence of (i) and (ii). (The same proof shows that (i) and (ii) are equivalent to:

(ii′) $\rho_V(u^t) = \rho_V(u)^t$ *for every regular u, and every $t \in k$.*)

Theorem 6. *Let G be reductive connected, and let V be a G-module. Assume $p > n(V)$. Let Γ be a subgroup of $G(k)$, which is G-cr. Then V is Γ-semisimple.*

The proof is in several steps.

(1) We may assume that $\rho_V : G \to \mathrm{GL}(V)$ has trivial kernel.

(2) *We have $p \geq h$.* This follows from $p > n(V) \geq h - 1$ (cf. Lecture 2).

(3) *The G-module V is semisimple.* Write G as $T.S_1 \ldots S_m$, where T is the maximal central torus, and $S_1 \ldots S_m$ is the decomposition of (G, G) into quasi-simple factors. To prove (3), it is enough to show that V is S_i-semisimple for every i (this is an easy lemma, cf. [J2] and comments below); since $n_{s_i}(V) \leq n_G(V)$ we are reduced to the case where G is quasi-simple. With the usual notation we have, for every weight λ of V, $\lambda \neq 0$,

$$\langle \lambda + \rho, \beta^\vee \rangle \leq 1 + \sum_{\alpha > 0} \langle \lambda, \alpha^\vee \rangle \leq p,$$

where the inequality on the left is in [S1], p.519. This shows that the simple modules $L(\lambda_i)$ in a Jordan-Hölder series of V are of two types: $\lambda_i = 0$, or $\langle \lambda_i + \rho, \beta^\vee \rangle \leq p$. But it is known (cf. [J1]) that this implies $L(\lambda_i)$ $\mathrm{Ext}^1_G(L(\lambda_i), L(\lambda_i)) = 0$ for every pair λ_i, λ_j (e.g. because these $L(\lambda_i)$ are Weyl modules). Hence V is semisimple.

We pause to discuss a variant of this proof. If λ is a dominant weight with $\sum_{\alpha>0} \langle \lambda, \alpha^\vee \rangle < p$, then $L(\lambda) = V(\lambda)$, where $V(\lambda)$ is the Weyl module. The proof is by reduction to G quasi-simple, and one distinguishes between two cases: $\lambda = 0$, where it is obvious, and $\lambda \neq 0$, where we have $\langle \lambda + \rho, \beta^\vee \rangle \leq p$. Moreover, if λ, μ have the property $L(\lambda) = V(\lambda)$, $L(\mu) = V(\mu)$ then $\mathrm{Ext}^1_G(L(\lambda), L(\mu)) = 0$. See [J2] for more details.

(4) *The Γ^{sat}-module V is semisimple.* (Note that we can define Γ^{sat} since $p \geq h$ by (2).) Let H be the connected component of Γ^{sat}. Since Γ^{sat} is G-cr (because Γ is), H is a reductive group. By Corollary 1 to Theorem 5, we have $n_H(V) \leq n_G(V)$ hence $n_H(V) < p$ and part (3) above (applied to H) shows that V is H-semisimple. Since $(\Gamma^{\mathrm{sat}} : H)$ is prime to p, this implies that V is Γ^{sat}-semisimple (cf. [S1], p.523).

(5) *If a subspace W of V is Γ-stable, it is Γ^{sat}-stable.* Let H_W be the stabilizer of W in G. If $u \in H_W$ is unipotent, one has $\rho_V(u^t) = \rho_V(u)^t$ by Corollary 2 to Theorem 5 above. Since $\rho_V(u)W = W$ the same is true for $\rho_V(u)^t$ for every t. This shows that H_W is saturated. Since it contains Γ, it also contains Γ^{sat}.

(6) *End of proof.* By (5), the subspaces of V which are Γ-stable are the same as those which are Γ^{sat}-stable. Since, by (4), V is Γ^{sat}-semisimple, it is Γ-semisimple.

Note that this is the "Main Theorem" announced at the beginning of these lectures. It implies for instance the following (where k is arbitrary of characteristic p):

If V_α are semisimple Γ modules, and $i_\alpha \geq 0$ integers with

$$\sum i_\alpha (\dim V_\alpha - i_\alpha) < p,$$

then $\bigotimes_\alpha \bigwedge^{i_\alpha} V_\alpha$ is semisimple.

(Sketch of proof. Apply Theorem 6 to $\prod_\alpha \mathrm{GL}(V_\alpha)$ and $V = \bigotimes_\alpha \bigwedge^{i_\alpha} V_\alpha$, and deduce the statement when k is algebraically closed. Next show that one can assume $i_\alpha \leq (\dim V_\alpha)/2$, and $\dim V_\alpha < p$ for all α; deduce that V_α is absolutely semisimple (i.e. remains semisimple after extension of scalars from k to $\overline{k}$); hence $\bigotimes_\alpha \bigwedge^{i_\alpha} V_\alpha$ is absolutely semisimple.)

Theorem 7 (Eugene). (cf. [J2], [Mc], [LS]) *Let $H \subset G$ be connected reductive, and $p \geq h_G$. Then H is G-cr.*

The proof starts by reducing to the case G is quasi-simple. Then there are separate proofs for type A_n (Jantzen), B_n, C_n, D_n (Jantzen-McNinch), and exceptional type (Liebeck-Seitz). There is a little extra work involved in the B_n, C_n, D_n cases when H is of type A_1. (Note that in special cases $p \geq h_G$ can be improved.)

Theorem 8. *Let* $\Gamma \subset G$. *Assume* $p \geq h_G$. *The following are equivalent:*

(i) Γ *is* G*-cr;*
(ii) *the connected component of* Γ^{sat} *is reductive.*

The direction (i)⇒(ii) is clear since Γ is G-cr $\Rightarrow$ Γ^{sat} is G-cr, and hence $(\Gamma^{\text{sat}})^0$ is reductive.

For (ii)⇒(i) apply Theorem 7 to $H = (\Gamma^{\text{sat}})^0$. One sees that H is G-cr, hence also Γ^{sat}, hence also Γ.

Theorem 9. *Let* V *be a nondegenerate* G*-module. Assume* $n(V) < p$. *If* $\Gamma \subset G$, *the following are equivalent:*

(i) Γ *is* G*-cr;*
(ii) V *is* Γ*-semisimple.*

The direction (i)⇒(ii) is Theorem 6. Conversely, if V is Γ-semisimple, it is also Γ^{sat}-semisimple (cf. argument of Theorem 6), hence $(\Gamma^{\text{sat}})^0$-semisimple and by Theorem 8 this shows that Γ is G-cr.

Note: The implication (ii)⇒(i) proved above under the condition $p > n(V)$ is far from best possible. Example: take $G = \mathrm{GL}(W)$, and $V = \bigwedge^2 W$, which is nondegenerate if $\dim W \neq 2$. One has $n(V) = 2(\dim W - 2)$ and one sees that:

$$\textstyle\bigwedge^2 W \text{ is } \Gamma\text{-semisimple} \;\Rightarrow\; W \text{ is } \Gamma\text{-semisimple}$$

if $p > 2(\dim W - 2)$. However, an elementary argument [S2], shows that this remains true as long as p does not divide $\dim W - 2$.

Example of Theorem 8: If one takes for V the adjoint representation $\mathrm{Lie}\, G$, which is nondegenerate, one has $n(\mathrm{Lie}\, G) = 2h - 2$ and Theorem 8 gives:

$$\Gamma \text{ is } G\text{-cr} \iff \mathrm{Lie}\, G \text{ is } \Gamma\text{-semisimple}$$

provided $p > 2h - 2$. (In fact, for $G = \mathrm{GL}_n$, no condition on p is needed for ⇐, cf. [S2], Theorem 3.3.)

A few references

[BR] P. Bardsley and R. W. Richardson, Étale slices for algebraic transformation groups in characteristic p, *Proc. London Math. Soc.* **51** (1985), 295–317.

[Bo1] A. Borel, Sous-groupes commutatifs et torsion des groupes de Lie compacts connexes, *Tôhoku Math. J.*, (2) **13** (1961), 216-240

[BS] A. Borel and J.-P. Serre, Sur certains sous-groupes des groupes de Lie compacts, *Comm. Math. Helv.* **27** (1953), 128–139.

[BT] A. Borel and J. Tits, Éléments unipotents et sous-groupes paraboliques des groupes réductifs, *Invent. math.* **12** (1971), 95-104.

[B] N. Bourbaki, *Groupes et algèbres de Lie*, Chap I-VI, Hermann, Paris (1968).

[C] C. Chevalley, *Théorie des groupes de Lie*, vol. III, Hermann, Paris, (1954).

[D] P. Deligne, Catégories Tannakiennes, *The Grothendieck Festschrift*, Vol II, Birkhäuser, Boston (1990), 111-195.

[De] M. Demazure, Invariants symétriques entiers des groupes de Weyl et torsion, *Invent. math.* **21** (1973), 287-301.

[Dy] E. Dynkin, Semisimple subalgebras of semisimple Lie algebras, *A.M.S. Translations series 2* **6** (1957), 111-245.

[G] R. Griess, Elementary abelian p-subgroups of algebraic groups, *Geom. Dedicata* **39** (1991), 253–305.

[GR] R. Griess and A. Ryba, Finite simple groups which projectively embed in an exceptional Lie group are classified!, preprint, April 14, (1998).

[J1] J. Jantzen, *Representations of Algebraic Groups*, Academic Press, Orlando, Pure and Applied Mathematics **131** (1987).

[J2] J. Jantzen, Low dimensional representations of reductive groups are semisimple, *Algebraic Groups and Lie groups: a volume in honor of R.W. Richardson.* Cambridge (1997).

[K] B. Kostant, The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group, *Amer. J. Math.* **81** (1959), 973-1032.

[LS] M. Liebeck G. Seitz, Reductive subgroups of exceptional algebraic groups, *Memoirs of the A.M.S.* **580** (1996).

[Mc] G. McNinch, Dimensional criteria for semisimplicity of representations, *Proc. London Math. Soc.*(3) **76** (1998), 95–149.

[Min] H. Minkowski, *Gesammelte Abhandlungen*, New York, Chelsea Pub. Co. (1967).

[N] M. V. Nori, On subgroups of $\mathrm{GL}_n(\mathbb{F}_q)$, *Invent. math.* **88** (1987), 257–275.

[S1] J.-P. Serre, Sur la semi-simplicité des produits tensoriels de représentations de groupes, *Invent. math.* **116** (1994), 513–530.

[S2] J.-P. Serre, Semisimplicity and tensor products of group representations: converse theorems, *J. Algebra* **194** (1997), 496–520 (with an appendix by W. Feit).

[S3] J.-P. Serre, Exemples de plongements des groupes $\mathrm{PSL}_2(\mathbb{F}_p)$ dans des groupes de Lie simples, *Invent. math.* **124** (1996), 525–562.

[S4] J.-P. Serre, *Galois Cohomology*, Springer-Verlag (1997).

[Sp1] T. Springer, Some arithmetical results on semi-simple Lie algbras, *Publ. Math I.H.E.S.* **30**, (1966),115-141.

[Sp2] T. Springer, Regular elements of finite reflection groups, *Invent. math.* **25** (1974), 159–198.

[SpSt] T. Springer, R. Steinberg, Seminar on algebraic groups and related finite groups: conjugacy classes, algebraic groups, *Lect. Notes in Math* **131**, Springer-Verlag (1970).

[St] R. Steinberg, Regular elements of semisimple algebraic groups, *Publ. Math. IHES* **25** (1965), 49–80 (= Coll. Papers no. 20).

[Te] D. Testerman, The construction of the maximal A_1's in the exceptional algebraic groups. *Proc. A.M.S* **161**, 635-644 (1993).

[T1] J. Tits, Buildings of spherical type and finite BN-pairs, *Lect. Notes in Math.* **386**, Springer-Verlag (1974).

[T2] J. Tits, Résumé de cours au Collège de France, (1997-1998), 93-98.