1. Algebraic groups

In the first two weeks, we describe the theory of linear algebraic groups.

1.1. **Linear algebraic groups.** If a scheme $G_{/B}$ as a functor induces a covariant functor from $ALG_{/B}$ into the category GP of groups, G is called a *group scheme*. If it has values in abelian groups AB, we call it a commutative group scheme. We present here a functorial view point of group schemes. A main reference is [RAG].

1.2. **Affine algebraic groups.** We start with examples. Let G be an affine scheme over a ring B. Thus G is a covariant functor from B–algebras $ALG_{/B}$ to $SETS$. If the functor $R \mapsto G(R)$ for all B–algebras R factors through the subcategory GP of groups in $SETS$, (i.e., $G(R)$ is a group and $\phi_* : G(R) \to G(R')$ for any B–algebra homomorphism $\phi : R \to R'$ is a group homomorphism), G is called an *affine group scheme* or an affine algebraic group defined over B. The group functor μ_N sending each B-algebra R to its N-th root of unity $\mu_N(R)$ is given by S_A for $A = B[X]/((1+X)^N - 1) - 1)$ and is an example of finite flat (equivalently, locally free of finite rank) affine group schemes.

Exercise 1.1. *Prove that* $\mu_N(R) = \mathrm{Hom}_{ALG_{/B}}(B[X]/((1+X)^N - 1) - 1), R)$ *is in bijection to* $\{\zeta \in R^\times | \zeta^N = 1\}$ *by sending* $\phi : B[X]/((1+X)^N - 1) - 1) \to R$ *to* $\phi(X) = \zeta$.

Similarly if an affine scheme $\mathcal{R}_{/B}$ is a covariant functor from the category of B-algebras into the category of rings, $\mathcal{R}$ is called an *affine ring scheme*. For two affine algebraic group G, G' defined over B, we define

$$\begin{aligned} \mathrm{Hom}_{B\text{-alg gp}}(G, G') &= \mathrm{Hom}_{GSCH_{/B}}(G, G') \\ &:= \left\{ \phi \in \mathrm{Hom}_{SCH_{/B}}(G, G') \middle| \phi_R \text{ is a group homomorphism for all } R \right\}. \end{aligned} \tag{1.1}$$

For simplicity, we write S_A for $\mathrm{Spec}(A)_{/B}$.

Example 1.1.

(1) Let $A = B[X_1, \ldots, X_n]$. Then $\mathbb{G}_a^n(R) := S_A(R) = R^n$, which is an additive group. Since
$$\phi_*(r_1, \ldots, r_n) = (\phi(r_1), \ldots, \phi(r_n))$$
for each algebra homomorphism $\phi : R \to R'$, ϕ_* is a homomorphism of additive groups/rings. Thus $\mathbb{G}_a^n$ is an additive group/ring scheme.

(2) More generally, we can think of $C = B[X_{ij}]$ for n^2 variables. Then $S_C(R) = M_n(R)$, and S_C is not just a group scheme but is a ring scheme. This ring scheme is written often as M_n. As additive group schemes (ignoring ring structure), M_n is isomorphic to $\mathbb{G}_a^{n^2}$.

(3) Consider $A = B[t, t^{-1}]$. Then $S_A(R) = \mathrm{Hom}_{ALG_{/B}}(A, R) = R^\times$ by sending $\phi \in S_A(R)$ to $\phi(t) \in R$. Thus this is a group scheme, denoted by $\mathbb{G}_m$ and called the *multiplicative group*. Note that if $\phi : \mathbb{G}_m \to \mathbb{G}_m$ is a scheme morphism, then $\phi^*(t) = b \cdot t^n$ for $b \in B^\times$ as $B[t, t^{-1}]^\times = B^\times \times t^{\mathbb{Z}}$. If further ϕ induces a group homomorphism $\mathbb{G}_m \to \mathbb{G}_m$, the constant b has to be 1. Thus $\mathrm{Hom}_{GSCH_{/B}}(\mathbb{G}_m, \mathbb{G}_m) = \mathbb{Z}$ by $\phi \mapsto n$ if $\phi^*(t) = t^n$. Consider the group algebra

$B[\mathbb{Z}]$ of the additive group $\mathbb{Z}$. Then $B[t,t^{-1}] \cong B[\mathbb{Z}]$ by $t^n \leftrightarrow [n] \in B[\mathbb{Z}]$, so $\mathbb{G}_m = \mathrm{Spec}(B[\mathrm{End}_{GSCH_{/B}}(\mathbb{G}_m)])$.

(4) Let L be a free $\mathbb{Z}$-module of rank n with basis $e_1,\dots,e_n$. Consider the functor $R \mapsto R^\times \otimes_{\mathbb{Z}} L$, where $R^\times$ is considered to be an abelian group and $R^\times \otimes_{\mathbb{Z}} L$ is a usual tensor product of two abelian groups. Write this functor as $\mathbb{G}_m \otimes_{\mathbb{Z}} L$. Then $R^\times \otimes_{\mathbb{Z}} L \cong (R^\times)^n$ by sending $\sum_i a_i \otimes e_i$ to $(a_1,\dots,a_n)$. Thus we have $\mathbb{G}_m \otimes_{\mathbb{Z}} L \cong \mathbb{G}_m^n$. Since $\mathrm{End}_{GSCH_{/B}}(\mathbb{G}_m) = \mathbb{Z}$, we have $L^* = \mathrm{Hom}_{\mathbb{Z}}(L,\mathbb{Z}) \cong \mathrm{Hom}_{GSCH_{/B}}(\mathbb{G}_m \otimes_{\mathbb{Z}} L, \mathbb{G}_m) =: X^*(L)$ (the character group of $\mathbb{G}_m \otimes L$) by sending $t \otimes \ell$ to $t^{\ell^*(\ell)}$ for $\ell^* \in L^*$. In other words, we have $\mathbb{G}_m \otimes_{\mathbb{Z}} L = \mathrm{Spec}(\mathbb{Z}[L^*])$ for the group algebra $\mathbb{Z}[L^*]$ of the additive group L^*. Put $X_*(\mathbb{G}_m \otimes_{\mathbb{Z}} L) = \mathrm{Hom}_{GSCH_{/B}}(\mathbb{G}_m, \mathbb{G}_m \otimes_{\mathbb{Z}} L)$. We call it the cocharacter group of $\mathbb{G}_m \otimes_{\mathbb{Z}} L$. We have a pairing $(\cdot,\cdot) : X_*(\mathbb{G}_m \otimes_{\mathbb{Z}} L) \times X^*(\mathbb{G}_m \otimes_{\mathbb{Z}} L) \to \mathrm{End}_{GSCH_{/B}}(\mathbb{G}_m) = \mathbb{Z}$ by $(\phi,\chi) = \chi \circ \phi$. Plainly this pairing is perfect. The group of the form $\mathbb{G}_m \otimes_{\mathbb{Z}} L$ is often called a *B-split torus*.

(5) Consider the ring $D = B[X_{ij}, \frac{1}{\det(X)}]$ for n^2 variables X_{ij} and the variable matrix $X = (X_{ij})$. Then $S_D(R) = GL_n(R)$ and S_D is a group scheme under matrix multiplication, which is a subscheme of S_C because $GL_n(R) \subset M_n(R)$ for all R. This group scheme S_D is written as $GL(n)$. In particular, $S_{B[t,t^{-1}]} = GL(1)$ is equal to $\mathbb{G}_m$.

(6) For a given B–module X free of rank n, we define $X_R = X \otimes_B R$ (which is R–free of the same rank n) and

$$GL_X(R) = \left\{\alpha \in \mathrm{End}_R(X_R) \middle| \text{there exists } \alpha^{-1} \in \mathrm{End}_R(X_R)\right\}.$$

Then GL_X is isomorphic to $GL(n)_{/B}$ by choosing a basis of X; so, GL_X is an affine group scheme defined over a ring B. We can generalize this to a locally free B–module X, but if X is not free, it is slightly more demanding to prove that GL_X is an affine scheme.

(7) We can then think of $E = B[X_{ij}]/(\det(X)-1)$. Then

$$S_E(R) = \{x \in GL_n(R) | \det(x) = 1\}.$$

This closed subscheme of M_n (and also of $GL(n)$) is written as $SL(n)$ and is a group scheme (under matrix multiplication) defined over B.

(8) Let X is a free B–module of finite rank. We fix a nondegenerate bilinear form $S : X \times X \to B$. Then we consider

$$G(R) = \{\alpha \in GL_X(R) | S_R(x\alpha, y\alpha) = S_R(x,y) \text{ for all } x,y \in X_R\},$$

where $S_R(r \otimes x, s \otimes y) = rsS(x,y)$ for $r,s \in R$ and $x,y \in X$.

To see that this G is an affine algebraic group defined over B, we fix a base $x_1,\dots,x_n$ of X over B and define a matrix S by $S = (S(x_i,x_j)) \in M_n(B)$. Then every (ij) entry $s_{ij}(X)$ of the matrix $XS\cdot {}^tX - S$ ($X = (X_{ij})$) is a quadratic polynomial with coefficients in B. Then we consider $L = B[X_{ij}, \det(X)^{-1}]/(s_{ij}(X))$. By definition,

$$S_L(R) = \left\{\alpha \in GL_X(R) \middle| \alpha S^t \alpha = S\right\} \cong G(R).$$

We find $\alpha S {}^t\alpha = S \Rightarrow S = \alpha^{-1} S \cdot {}^t\alpha^{-1}$; so, the inverse exists, and G is an affine algebraic group. If $X = B^n$ and $S(x,y) = xS{}^t y$ for a non-degenerate symmetric matrix S, G as above is written as $O_{S/B}$ and is called the *orthogonal group* of S. If $X = Y \times Y$ and S is non-degenerate skew symmetric of the form $S((y,y'),(z,z')) = T(y,z') - T(z,y')$ for a symmetric bilinear form $T : Y \times Y \to B$, we write $G = Sp_{T/B}$. In particular, if $S(x,y) = x \left(\begin{smallmatrix} 0 & -1_n \\ 1_n & 0 \end{smallmatrix}\right) {}^t y$, the group G is written as $Sp_{n/B}$ and is called the *symplectic group* of genus n.

(9) We consider a quadratic polynomial $f(T) = T^2 + aT + b \in \mathbb{Z}[T]$. Then define $S_f(R) = \mathbb{G}_a(R)[T]/(f(T))$. As a scheme $S_f \cong \mathbb{G}_a^2$ but its value is a ring all the time. If $\phi : R \to R'$ is an algebra homomorphism, $\phi_*(r + sT) = \phi(r) + \phi(s)T$; so, it is a ring homomorphism of $S_f(R) = R[T]/(f(T))$ into $S_f(R') = R'[T]/(f(T))$. Thus S_f is a ring scheme, and writing O for the order of the quadratic field $\mathbb{Q}[\sqrt{a^2 - 4b}]$ generated by the root of $f(T)$, we have $S_f(R) \cong R \otimes_{\mathbb{Z}} O$.

(10) Since any given number field F is generated by one element, we know $F = \mathbb{Q}[T]/(f(T))$ for an irreducible monic polynomial $f(T)$. For any $\mathbb{Q}$–algebra R, define $S_f(R) = R[T]/(f(T))$. Then in the same way as above, S_f is a ring scheme defined over $\mathbb{Q}$ such that $S_f(R) = F \otimes_{\mathbb{Q}} R$.

(11) Let G be an affine algebraic group defined over a number field F. Then we define a new functor G' defined over $\mathbb{Q}$–algebras R by $G'(R) = G(S_f(R)) = G(F \otimes_{\mathbb{Q}} R)$. We can prove that G' is an affine group scheme defined over $\mathbb{Q}$, which we write $G' = \mathrm{Res}_{F/\mathbb{Q}} G$ (see Exercise 1.2 (3)).

(12) Assume that f is a quadratic polynomial in $\mathbb{Q}[T]$. Then $S_f(\mathbb{Q}) = F$ is a quadratic extension with $\mathrm{Gal}(F/\mathbb{Q}) = \{1, \sigma\}$. Let X be a finite dimensional vector space over $\mathbb{Q}$ and let $\mathrm{Gal}(F/\mathbb{Q})$ act on $X_F = F \otimes_{\mathbb{Q}} X$ through F. We suppose to have a hermitian form $H : X_F \times X_F \to F$ such that $H(x,y) = \sigma(H(y,x))$. Then for $\mathbb{Q}$–algebra R

$$U_H(R) = \left\{ \alpha \in GL_X(S_f(R)) \middle| H_{S_f(R)}(x\alpha, y\alpha) = H_{S_f(R)}(x,y) \right\}$$

is an affine algebraic group, which is called the unitary group of H. Note that U_H is defined over $\mathbb{Q}$ (not over F).

Exercise 1.2.

(1) *Prove that if* $\phi \in \mathrm{Hom}_{GSCH_{/B}}(\mathbb{G}_m, \mathbb{G}_m) =: \mathrm{End}(\mathbb{G}_m)$*, the corresponding algebra homomorphism* $\phi^* : B[t,t^{-1}] \to B[t,t^{-1}]$ *satisfies* $\phi(t) = t^n$ *for an integer* n *(so,* $\mathrm{End}(\mathbb{G}_m) \cong \mathbb{Z}$*).*

(2) *Let* F *be a number field with the integer ring* O*. Is there any affine ring scheme* S *defined over* $\mathbb{Z}$ *such that* $S(R) = O \otimes_{\mathbb{Z}} R$*?*

(3) *Let* $S : X \times X \to B$ *is a bilinear form for a* B*–free module* X *of finite rank* n*, and suppose that* $X \cong \mathrm{Hom}_B(X, B)$ *by* S*. Prove that the matrix of* S *is in* $GL_n(B)$ *for any choice of basis of* X *over* B*.*

(4) *For an affine algebraic group* G *over a number field* F *(that is, a finite extension of* $\mathbb{Q}$*), prove that* $\mathrm{Res}_{F/\mathbb{Q}} G$ *is an affine algebraic group defined over* $\mathbb{Q}$*.*

(5) *Show that the unitary group* U_H *over* $\mathbb{Q}$ *as above is an affine algebraic group.*

More generally than the above Exercise 1.2 (4), we start with an affine group scheme H over a ring R'. For a subalgebra R of R', if the covariant functor $C \mapsto H(C \otimes_R R')$ defined

on the category of R-algebras is isomorphic to a scheme $H'_{/R}$, we write $H'_{/R} = \mathrm{Res}_{R'/R}H$ and call it the *Weil restriction* of H with respect to R'/R (this is not changing the base ring of $H_{/R'}$ to the subalgebra R).

Theorem 1.3. *Let the notation and the assumption be as above. If R'/R is locally R-free of finite rank, the group functor $\mathrm{Res}_{R'/R}H$ is an affine group scheme over R.*

For a proof, see [NMD] 7.6, Theorem 4.

1.3. **Basic diagrams.** The group structure of a group scheme gives rise to morphisms of schemes by Yoneda's lemma, for example, the group multiplication induces the multiplication morphism $m : G \times G \to G$ and the existence of identity can be formulated to be the existence of a closed immersion $\mathrm{Spec}(B) \to G$, which satisfies the group law. For example, associativity is equivalent to the commutativity of the following diagram

$$\begin{array}{ccc} G \times_{S_B} G \times_{S_B} G & \xrightarrow{(x,y,z)\mapsto(xy,z)} & G \times_{S_B} G \\ {\scriptstyle (x,y,z)\mapsto(x,yz)}\downarrow & & \downarrow{\scriptstyle m} \\ G \times_{S_B} G & \xrightarrow[m]{} & G. \end{array}$$

If $G = S_A$ is affine, the dual of this commutative diagram is

$$\begin{array}{ccc} A \otimes_B A \otimes_B A & \xleftarrow{\underline{m}\otimes\mathrm{id}} & A \otimes_B A \\ {\scriptstyle \mathrm{id}\otimes\underline{m}}\uparrow & \circlearrowleft & \uparrow{\scriptstyle \underline{m}} \\ A \otimes_B A & \xleftarrow[\underline{m}]{} & A. \end{array}$$

The B-algebra homomorphism $\underline{m}$ is called *co-multiplication*. Similarly, the identity e_R of the group $G(R)$ induces functor morphism

$$e_R : S_B(R) = \{\text{the structure morphism } \iota_R : B \to R\} \ni \iota_R \mapsto e_R \in G(R).$$

If $G = S_A$ is affine, the dual B-algebra homomorphism $\underline{e} : A \to B$ is called the *co-identity*. The group inverse map $i : G(R) \to G(R)$ induces an involution $\underline{i}$ of $\mathcal{O}_G$ (or A if $G = S_A$) called *co-inverse*. These maps makes the following diagram commutative:

$$\begin{array}{ccc} A & \xrightarrow{\underline{e}} & B \\ {\scriptstyle \underline{m}}\downarrow & & \downarrow{\scriptstyle \iota_A} \\ A \otimes_B A & \xrightarrow[\mathrm{id}_A\otimes\underline{i}]{} & A, \end{array} \quad \text{and} \quad \begin{array}{ccc} A & \xrightarrow{\underline{e}} & B \\ {\scriptstyle \underline{m}}\downarrow & & \downarrow{\scriptstyle \iota_A} \\ A \otimes_B A & \xrightarrow[\underline{e}\otimes\mathrm{id}_A]{} & B \otimes_B A = A, \end{array}$$

A B-algebra A with co-multiplication, co-inverse and co-identity (satisfying the above commutative diagrams) is called a *B-bialgebra* (or Hopf B-algebra). Once we take a dual $A^* = \mathrm{Hom}_B(A, B)$, A^* is also a bialgebra under the dual maps, as long as A is locally free of finite rank over B. The bialgebra A^* is called the *dual B-bialgebra* of a B-bialgebra A. We write $BIALG_{/B}$ for the category of B-bialgebras whose morphisms are B-algebra homomorphisms compatible with co-multiplication, co-inverse and co-identity. The category of group schemes $GSCH_{/B}$ is a subcategory of $SCH_{/B} \subset \mathcal{C}_B$ made up of B-schemes

having values in the category of groups, whose morphisms are B-scheme morphisms preserving the group structure. The association $A \mapsto S_A$ induces a contravariant functor of $BIALG_{/B}$ into $GSCH_{/B}$ which gives rise to an (anti-)equivalence of categories between $BIALG_{/B}$ and the full subcategory of affine group schemes in $GSCH_{/B}$.

Exercise 1.4. *Consider* $\mathbb{G}_m = \mathrm{Spec}(B[t, t^{-1}])$. *Let*

$$\underline{m} \in \mathrm{Hom}_{ALG_{/B}}(B[t, t^{-1}], B[t, t^{-1}] \otimes_B B[t, t^{-1}])$$

with $\underline{m}(t) = t \otimes t$. *Show that the corresponding morphism* $m : \mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m$ *is given by* $m(a, b) = ab$ *for* $a, b \in \mathbb{G}_m(R) = R^\times$.

2. Representation of Lie algebras

Here is a summary of the results we used on representation of Lie algebra. If we replace representations of a Lie algebra $\mathfrak{g}$ by representations of a group G on a finite dimensional vector space, the exposition is close to the one given in [MFG] Section 2.1. In other words, the results presented here are also valid for group representations once we replace the statement for Lie algebras by the corresponding statements for groups. As for books on Lie algebras, see [REP] for representations on a $\mathbb{C}$ vector space, [LAG] III for Lie algebras over general fields and [BLI] for more general cases.

2.1. **Algebras.** Let R be an algebra (which can be non-commutative). The algebra R is called *simple* if there are no two-sided ideals of R except for $\{0\}$ and R. An R–module M is called *irreducible* or *simple* if $M \neq 0$ and any R–submodule $N \subsetneq M$ is trivial. Thus M is irreducible $\Leftrightarrow M \cong R/\mathfrak{m}$ for a maximal left ideal $\mathfrak{m}$ of R.

Let M be an R–module of finite type. Then for any given proper R–submodule M_0 of M, we consider the set S of all proper R–submodules of M containing M_0. Here the word "proper" means that $M_0 \neq M$. If X is an ordered subset of S, then $M_X = \bigcup_{N \in X} N$ is an R–submodule of M. Here the "ordered" mean that if $N, N' \in X$, we can find $N'' \in X$ such that $(N \cup N') \subset N''$. If $M_X = M$, we find an element N of X such that $M = N$ because M is finitely generated over R. This contradicts to our assumption that S is made of proper submodules. Thus we have $M_X \neq M$ and $M_X \in S$. Namely any ordered sequence in S has a upper bound in S. Then by Zorn's lemma, S has a maximal element. This shows the existence of maximal proper R–submodule containing a given M_0.

Let $J(M)$ (*radical* of M) be the intersection of all proper maximal R–submodules of M. Then if M is of finite type over R, $J(M) = M$ implies that $M = 0$. Let $J = J(R)$ be the intersection of all maximal left ideals of R, which is called the *radical* of R. Then $R \neq J$. If M is irreducible, then the annihilator $\mathrm{Ann}(M) = \{r \in R | rM = 0\}$ of M is a maximal left ideal of R, because $R/\mathrm{Ann}(M) \cong M$ via $r \mapsto rm$ for any $0 \neq m \in M$. Thus $J \subset \bigcap_{M:\text{irreducible}} \mathrm{Ann}(M)$. Pick r in the intersection. Then $r(R/\mathfrak{m}) = 0$ for any maximal left ideal $\mathfrak{m}$, since $M = R/\mathfrak{m}$ for a maximal left ideal $\mathfrak{m}$ is irreducible. Thus $r \in rR \subset \mathfrak{m}$, and hence we have

$$J = \bigcap_{M:\text{irreducible}} \mathrm{Ann}(M). \tag{2.1}$$

Since $rM = 0$ implies $rxM = 0$ for all $x \in R$, $Jx \subset \cap_{M:\text{irreducible}} \mathrm{Ann}(M) = J$. Thus J is a two-sided ideal. We claim

$$\text{For every } r \in J,\ 1 - r \in R^\times. \tag{2.2}$$

Proof. Since $xr \in J$ for $x \in R$ and $r \in J$, we prove $1 - xr \in R^\times$ in place of $1 - r \in R^\times$. Suppose on the contrary that $1-xr$ does not even have left inverse. Then $R(1-xr) \neq R$, and hence, there exists a maximal left ideal $\mathfrak{m} \supset R(1 - xr)$. Thus $1 - xr \in \mathfrak{m}$ and $xr \in J \subset \mathfrak{m}$, which shows $1 = 1 - xr + xr \in \mathfrak{m}$, a contradiction. Thus $1 - xr$ has a left inverse. In particular, we find $s \in R$ such that $s(1-r) = 1$. Then $s = 1+sr = 1-(-s)r$. Applying the above argument for $x = -s$, we find $t \in R$ such that $ts = t(1-(-s)r) = 1$. Then $t = t(s(1 - r)) = (ts)(1 - r) = 1 - r$. This shows that $(1 - r)s = ts = 1$ and $1 - r \in R^\times$. □

Suppose that $\mathfrak{a} \subset R$ is a two-sided ideal with the property that $r \in \mathfrak{a} \Rightarrow 1 - r \in R^\times$. If $\mathfrak{a} \not\subset J$, then there exists a maximal left ideal $\mathfrak{m}$ such that $\mathfrak{a} \not\subset \mathfrak{m}$. Then $\mathfrak{a}+\mathfrak{m} = R$, and $a + m = 1$ for $a \in \mathfrak{a}$ and $m \in \mathfrak{m}$. Then $\mathfrak{m} \supset Rm = R(1 - a) = R$ because $1 - a \in R^\times$. This is a contradiction. Thus $\mathfrak{a} \subset J$. We thus have

$$\textit{If } a \in \mathfrak{a} \Rightarrow 1 - a \in R^\times \textit{ for a left (resp. right, two-sided) ideal } \mathfrak{a}, \textit{ then } \mathfrak{a} \subset J. \tag{2.3}$$

By (2.3), we conclude

$$J = \bigcap_{\mathfrak{m}:\text{maximal right ideals}} \mathfrak{m} = \bigcap_{\mathfrak{m}:\text{maximal two-sided ideals}} \mathfrak{m}. \tag{2.4}$$

Lemma 2.1 (Krull–Azumaya, Nakayama)**.**

1. *Let M be an R-module of finite type. If $M = JM$, then $M = 0$.*
2. *Let A be a commutative local ring and M be an A–module. If either the A–module M is of finite type or $\mathfrak{m}_A^N M = 0$ for a sufficiently large integer N, then $M = \mathfrak{m}_A M$ implies $M = 0$.*

This follows from the two facts: (i) $J(M) = M \Rightarrow M = 0$ and (ii) $JM \subset J(M)$ under the assumption of the lemma (cf. [CRT] Theorem 2.2).

Corollary 2.2. *Let A be a local ring. Let M and N be A–modules and $f : M \to N$ be an A–linear map. Suppose either that $\mathfrak{m}_A$ is nilpotent or that N is an A–module of finite type. Then if f induces a surjection $\overline{f} : M/\mathfrak{m}_A M \to N/\mathfrak{m}_A N$, then f itself is surjective.*

Proof. Consider $X = N/f(M)$. By assumption, $X/\mathfrak{m}_A X = \mathrm{Coker}(\overline{f}) = 0$. Thus $X = \mathfrak{m}_A X$ and hence by Lemma 2.1, $X = 0$. □

2.2. **Modules over Lie algebras.** Let E be a field of characteristic 0. A *Lie algebra* $\mathfrak{g}$ over E is a vector space over E with E-linear Lie bracket map $[\cdot,\cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ satisfying $[x, y] = -[y, x]$ and $[x, [y, z]] + [z, [x, y]] + [y, [z, x]] = 0$ for all $x, y, z \in \mathfrak{g}$.

Let $\mathfrak{g}$ be a finite dimensional Lie algebra over E with E-linear Lie bracket $[\cdot,\cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$. For an E-vector space V of finite dimension n, a representation $\rho : \mathfrak{g} \to \mathrm{End}_E(V)$ is an E-linear map with $\rho([x, y]) = \rho(x)\rho(y) - \rho(y)\rho(x)$ for all $x, y \in \mathfrak{g}$. A representation $\rho : \mathfrak{g} \to \mathrm{End}_E(V)$ is called *reducible* if $V = V(\rho)$ has a proper non-trivial subspace stable under $\mathfrak{g}$. A representation is called *irreducible* if it is not reducible. An

irreducible representation with coefficients in E can be reducible as a representation into $\mathrm{End}_L(V \otimes_E L)$ for a field extension L/E. A representation $\rho : \mathfrak{g} \to \mathrm{End}_E(V)$ is called *absolutely irreducible* if $\rho_{\overline{E}}$ on $V(\rho) \otimes_E \overline{E}$ is irreducible for an algebraic closure $\overline{E}/E$.

Let $R = R(\rho)$ be the E–subalgebra of the E–linear endomorphism algebra of $V = V(\rho)$ generated over E by $\rho(\sigma)$ for all $\sigma \in \mathfrak{g}$. Then $R \subset \mathrm{End}_E(V) \cong M_n(E)$, and hence R is a finite dimensional algebra over E; so, it is artinian and noetherian. Let $J = J(R)$. Then the sequence $\{J^n\}_n$ stabilizes for a sufficiently large $n = N$. From Nakayama's lemma (Lemma 2.1), we conclude $J^N = \{0\}$. Thus $\bigcap_{\mathfrak{m}:\text{max. two-sided}} \mathfrak{m}^N \subset J^N = 0$. For a maximal two-sided ideal $\mathfrak{m}$ and an ideal $\mathfrak{a} \not\subset \mathfrak{m}$, we see $\mathfrak{m} + \mathfrak{a} = R$, and hence $\mathfrak{m}^j + \mathfrak{a}^j = R$ for all $j > 0$. Applying the Chinese remainder theorem ([CRT] Theorem 1.4), we have $R = \prod_{\mathfrak{m}} R/\mathfrak{m}^N$ for sufficiently large N, where $\mathfrak{m}$ runs over all maximal two-sided ideals of R. We write $R_{\mathfrak{m}}$ for $R/\mathfrak{m}^N$. If V is irreducible, then $J = \mathfrak{m}$ for a single maximal two-sided ideal. Then $V \neq \mathfrak{m}V$ again by Lemma 2.1. Therefore $\mathfrak{m}V = 0$. Since R acts faithfully on V, we conclude $\mathfrak{m} = 0$. Thus R is a simple algebra over E. We have shown that

$$V \text{ is irreducible} \Rightarrow R \text{ is simple.}$$

Thus the study of irreducible $\mathfrak{g}$-modules is reduced to the study of R-modules for a simple E-algebra R.

2.3. **Semi-simple algebras.** To study modules over simple algebras, we start slightly more generally. Here we only assume R to be an artinian algebra. An R–module V is called *completely reducible* if it is a direct sum of irreducible modules. The algebra R is called *semi-simple* if its radical $J = J(R)$ vanishes. Since maximal left ideals of $R/J(R)$ corresponds bijectively to maximal left ideals of R by the homomorphism theorem, we see that $J(R/J(R)) = 0$. This shows that the quotient $R/J(R)$ is semi-simple. Now the following three statements are equivalent:

(SS1) R is semi-simple;
(SS2) The left R–module R is completely reducible;
(SS3) Every R–module V of finite length is completely reducible.

Proof. We first prove the implication: (SS1)⇒ (SS2): Let Ω be the set of all maximal left ideals of R. Then $\mathfrak{m} + \mathfrak{n} = R$ for two distinct elements $\mathfrak{m}, \mathfrak{n} \in \Omega$. Then by the Chinese remainder theorem, $\bigcap_{\mathfrak{m}\in\Omega} \mathfrak{m} = J(R) = 0$ implies that $R \cong \bigoplus_{\mathfrak{m}\in\Omega} R/\mathfrak{m}$. Since R is artinian, Ω is a finite set. By the homomorphism theorem, R–submodules of $R/\mathfrak{m}$ correspond bijectively to left ideals between $\mathfrak{m}$ and R. This shows $R/\mathfrak{m}$ is irreducible, since $\mathfrak{m}$ is a maximal left ideal.

(SS2)⇒(SS3): Since $R \cong \bigoplus_{\mathfrak{m}\in\Omega} R/\mathfrak{m}$, we have minimal left ideals $I_{\mathfrak{m}}$ indexed by $\mathfrak{m} \in \Omega$ such that $R = \bigoplus_{\mathfrak{m}\in\Omega} I_{\mathfrak{m}}$ with $I_{\mathfrak{m}} \cong R/\mathfrak{m}$ as left R–modules. Then $1 = \oplus_{\mathfrak{m}\in\Omega} e_{\mathfrak{m}}$ for $e_{\mathfrak{m}} \in I_{\mathfrak{m}}$. Multiplying the left-hand-side and the right-hand-side by $a \in I_{\mathfrak{m}}$, we get $I_{\mathfrak{m}} \ni a = a1 = \oplus_{\mathfrak{m}\in\Omega} a e_{\mathfrak{m}}$, and therefore $a e_{\mathfrak{n}} = \delta_{\mathfrak{m},\mathfrak{n}} a$, where $\delta_{\mathfrak{m},\mathfrak{n}} = 1$ or 0 according as $\mathfrak{m} = \mathfrak{n}$ or not. Thus $I_{\mathfrak{m}} = R e_{\mathfrak{m}}$. Replacing a by $e_{\mathfrak{m}}$, we get $e_{\mathfrak{m}}^2 = e_{\mathfrak{m}}$ and $e_{\mathfrak{m}} e_{\mathfrak{n}} = 0$ if $\mathfrak{m} \neq \mathfrak{n}$. Consider an R–linear map $\varphi : I_{\mathfrak{m}} \to I_{\mathfrak{m}} v$ given by $\varphi(i) = iv$ for $v \in V$. Since $\mathrm{Ker}(\varphi)$ is R–submodule of $I_{\mathfrak{m}}$, the irreducibility of $I_{\mathfrak{m}}$ tells us that either $\mathrm{Ker}(\varphi) = 0$ or $\mathrm{Ker}(\varphi) = I_{\mathfrak{m}}$. Thus either $I_{\mathfrak{m}} v \cong I_{\mathfrak{m}}$ or $I_{\mathfrak{m}} v = 0$. In particular, if $I_{\mathfrak{m}} v \neq 0$, then $\sum_{\mathfrak{m}\in\Omega} e_{\mathfrak{m}} v = v \in \sum_{\mathfrak{m}\in\Omega} I_{\mathfrak{m}} v$. From this, we conclude $V = \sum_{v\in V-\{0\}} \sum_{\mathfrak{m}\in\Omega} I_{\mathfrak{m}} v$. Then

we can find $\mathfrak{m}_j$ and v_j such that $I_{\mathfrak{m}_j}v_j \neq 0$ and $V = \bigoplus_j I_{\mathfrak{m}_j}v_j \cong \bigoplus_j I_{\mathfrak{m}_j}$ as R–modules, since V is of finite length.

(SS3)⇒(SS1): By (SS3), R is the direct sum of irreducible R–submodules $I_{\mathfrak{m}}$. By Lemma 2.1, $I_{\mathfrak{m}} \neq J(R)I_{\mathfrak{m}}$. Since $I_{\mathfrak{m}}$ is irreducible, $J(R)I_{\mathfrak{m}} = 0$. Then $J(R) = J(R)R = \bigoplus_{\mathfrak{m}} J(R)I_{\mathfrak{m}} = 0$. □

We now decompose $\Omega = \Omega_1 \bigsqcup \cdots \bigsqcup \Omega_\lambda$ so that $\mathfrak{m}, \mathfrak{n} \in \Omega_j \iff I_{\mathfrak{m}} \cong I_{\mathfrak{n}}$ as left R–modules. Then we write $R_j = \bigoplus_{\mathfrak{m}\in\Omega_j} I_{\mathfrak{m}}$. If $\mathfrak{m} \in \Omega_j$, $I_{\mathfrak{m}}a$ for $a \in R$ is either isomorphic to $I_{\mathfrak{m}}$ or 0, and therefore it has to be inside R_j. Thus $R_jR \subset R_j$ and hence R_j is a two-sided ideal, and $R = \bigoplus_j R_j$ is an algebra direct sum. Returning to the original setting and applying the above argument to $R/J(R)$, we have

(S) *An artinian algebra R has only one maximal two-sided ideal if and only if there is a unique isomorphism class of irreducible R-modules,*

since the set of maximal two-sided ideals of R naturally corresponds to that of $R/J(R)$ bijectively. We now claim that the following three assertions are equivalent (a theorem of Wedderburn):

(S1) R is a simple algebra;
(S2) R is a direct sum of mutually isomorphic minimal left ideals;
(S3) $R \cong M_n(D)$ for a division algebra D,

where a *division algebra* D is an algebra such that $D - \{0\} = D^\times$.

Proof. (S1) ⇒ (S2) follows from (S) because minimal left ideals are all irreducible.

(S2) ⇒ (S3): Let V be the minimal left ideal of R. Then $R \cong V^n$ as a left R–module. Then $\mathrm{End}_R(R) \cong M_n(\mathrm{End}_R(V))$. Pick $\phi : V \to V \in \mathrm{End}_R(V)$. Then $\mathrm{Ker}(\phi) = 0$ or V and $\mathrm{Im}(\phi) = V$ or 0 because of irreducibility of V. This shows ϕ is either bijective or the zero map; hence $D = \mathrm{End}_R(V)$ is a division algebra. On the other hand, it is easy to see that $\phi \mapsto \phi(1)$ induces $\mathrm{End}_R(R) \cong R$, because $\phi_a(x) = xa$ gives an element in $\mathrm{End}_R(R)$ with $\phi_a(1) = a$.

(S3) ⇒ (S1): Let $\mathfrak{a}$ be a two-sided ideal of R. If $\mathfrak{a}$ has non-zero element a, multiplying a by elementary matrices from left and right, we may assume that $a = dE_{ij}$ for $0 \neq d \in D$ with the elementary matrix E_{ij} having nontrivial (i, j)–entry. Thus $E_{ij} = d^{-1}a \in \mathfrak{a}$. Then again multiplying E_{ij} by elementary matrices, we find $E_{ij} \in \mathfrak{a}$ for all (i, j). Thus $\mathfrak{a} = R$. □

Let R be a simple artinian algebra. Let $\overline{E}$ be the center of R. Then by (S3), $\overline{E}$ is a field, which is the center of D. Suppose that $\overline{E}$ is algebraically closed. Then for any $x \in D$, $\overline{E}[x] \subset D$ is a finite field extension of $\overline{E}$. Thus $\overline{E} = \overline{E}[x]$ and $x \in \overline{E}$. This shows that $\overline{E} = D$ and

(S4) *If R is a finite dimensional simple algebra over an algebraically closed field $\overline{E}$, then $R \cong M_n(\overline{E})$.*

Recall that $\mathfrak{g}$ is a Lie algebra. Let $\rho : \mathfrak{g} \to M_n(E)$ be an absolutely irreducible representation for a field E. Let R be the E–subalgebra of $M_n(E)$ generated by $\rho(g)$ for all $g \in \mathfrak{g}$. By absolute irreducibility, $R \otimes_E \overline{E}$ remains simple for an algebraic closure $\overline{E}$ of E. Since there is no simple algebra except for matrix algebras over an algebraically

closed field, $R\otimes_E \overline{E}\cong M_{n'}(\overline{E})$ for some $n'\le n$ if ρ is absolutely irreducible. Pick $x\neq 0$ in V. We consider a map $f: R\otimes_E \overline{E}\to V\otimes_E \overline{E}$ induced by $r\mapsto rx$. Then $Ker(f)$ is a maximal left ideal of $M_{n'}(\overline{E})$, and hence $V\otimes_E \overline{E}\cong \overline{E}^{n'}$. This shows that $n=n'$, and $R\cong M_n(E)$. We record here what we have proven:

Proposition 2.3. *Suppose that $\rho:\mathfrak{g}\to M_n(E)$ for a field E is absolutely irreducible. Let R be a E–subalgebra of $M_n(E)$ generated by $\rho(g)$ for all $g\in\mathfrak{g}$. Then*

1. (Burnside) *$R\cong M_n(E)$ for $n=\dim_E V$;*
2. (Schur) *If a linear map $f: V\to V$ commutes with ρ, then f is induced by a scalar multiplication.*

The second assertion follows from the first as a linear endomorphism of E^n commuting with all matrices in $M_n(E)$ is a scalar. This proposition also applies to an absolutely irreducible group representation $\rho: G\to M_n(E)$ for a group G.

This result shows that $V(\rho)\otimes_E X$ (or $\rho:\mathfrak{g}\to M_n(X)$) remains irreducible for an arbitrary field extension X/E if ρ is absolutely irreducible.

Let H be a closed subgroup of a profinite group G. Let $\rho: G\to GL_n(A)$ be a representation. Consider the following condition

(AI_H) $\qquad\qquad \overline{\rho}|_H$ *is absolutely irreducible.*

Of course (AI_H) implies (AI_G). We have the following generalization of Schur's lemma by Mazur.

Lemma 2.4 (B. Mazur)**.** *Suppose* (AI_G)*, and let R be an A–subalgebra of $M_n(A)$ generated by* $\mathrm{Im}(\rho)$*. Then $R=M_n(A)$, and in particular, if $T\rho(\sigma)=\rho(\sigma)T$ for all $\sigma\in G$ and $T\in M_n(A)$, T is a scalar matrix.*

Proof. We consider the A–subalgebra R generated by $\rho(G)$ over A inside $M_n(A)$. We only need to show that $R=M_n(A)$, because then its center is scalar. We have the inclusion map $\iota: R\hookrightarrow M_n(A)$, which induces a surjection $\overline{\iota}: R/\mathfrak{m}_A R\to M_n(E)$ by Proposition 2.3. Then by Corollary 2.2, ι is surjective. This shows $R=M_n(A)$. □

2.4. **Induced representations.** Let G be a group. Fix a subgroup H of finite index, and pick an A–free module V of rank n. Suppose that H acts on V A–linearly (such a module, we call an (A,H)–module). If one fixes a base of V, the action of H is given by a homomorphism $\rho_H: H\to GL_n(A)$. Such a homomorphism is called a representation of H of degree n with coefficients in A. Two such representations φ and φ' are *equivalent* if the two underlying H–modules are isomorphic, that is, we have an A–linear isomorphism $T: V\to V'$ such that $hT(x)=T(hx)$ for all $h\in H$. In particular, two choices of basis on V give rise to a unique isomorphism class of ρ_H.

Formal linear combinations $\sum_g a_g g$ form a free A–module $A[G]$, which is an A–algebra by $\sum_g a_g g\cdot\sum_h b_h h=\sum_{g,h} a_g b_h gh$. This algebra is called the *group algebra* of G. If V is an (A,H)–module, it automatically becomes $A[H]$–module by $\left(\sum_g a_g g\right)\cdot v=\sum_g a_g(gv)$. Thus the representation ρ_H extends uniquely to an algebra representation of $A[H]$ into the matrix ring $M_n(A)$.

We consider a space of formal linear combinations $\sum_{g\in G/H} v_g g$ for the coset space G/H. Thus $V[G/H]$ is an A–free module of rank $n[G:H]$, and $V[G/H]=A[G/H]\otimes_A V$

by $\sum_g v_g g \mapsto \sum_g (g \otimes v_g)$. We have another identification: $W = W_{G/H} = A[G] \otimes_{A[H]} V$. Here the tensor product is taken by using the right $A[H]$–module structure on $A[G]$ given by $\left(\sum_g a_g g\right) \cdot h = \sum_g a_g (gh)$. Then again $\left(\sum_g a_g g\right) \otimes v \mapsto \sum_g a_g v\overline{g}$ for $\overline{g} = gH$ gives an isomorphism: $W_{G/H} \cong V[G/H]$. This expression of $V[G/H]$ has a natural left action of G given by that on $A[G]$: $g \cdot \left(\sum_{g'} a_{g'} g' \otimes v\right) = \sum_{g'} a_{g'} gg' \otimes v$. The module $V[G/H]$ contains naturally V by $v \mapsto v1_G$, which corresponds to $1_G \otimes V$ in $W_{G/H}$ and $h(1 \otimes v) = h \otimes v = 1 \otimes hv$ for $h \in H$ by the property of the tensor product over $A[H]$: $xh \otimes y = x \otimes hy$ for $h \in A[H]$. Thus H acts on $V \subset V[G/H]$ through the original action; so, $V \hookrightarrow V[G/H]$ is an inclusion of H–modules. In this sense, $V[G/H]$ is an extension of ρ_H. We choose a base of $V[G/H]$ over A and get an isomorphism class $\mathrm{Ind}_H^G \rho_H$ of a representation of G. This is called the *induced representation* of ρ_H which has degree $n[G:H]$.

For our later use, we record the following characterization of induced representations:

Lemma 2.5. *Let $\rho : G \to GL_n(B)$ be a continuous representation for a local ring B. Suppose that $\overline{\rho} = \rho \bmod \mathfrak{m}_B : G \to GL_n(\mathbb{F})$ is absolutely irreducible. Let $\chi : G \to B^\times$ be a continuous character of order r prime to p. Then $\rho \cong \rho \otimes \chi$ if and only if there exist a B-free local algebra B' with $\mathrm{rank}_B B' \le r$ and a representation $\varphi : H \to GL_m(B')$ for $H = \mathrm{Ker}(\chi)$ such that $(G:H)m = n$ and $\rho \cong \mathrm{Ind}_H^G \varphi$ in $GL_n(B')$.*

Proof. Suppose that $\rho = \mathrm{Ind}_H^G \varphi$ for a representation $\varphi : H \to GL_m(B')$. Note that the representation space of ρ is given by

$$V(\varphi) \otimes_{B'} B'[\Delta].$$

Then from the isomorphism $B'[\Delta] \cong B'[\Delta] \otimes \chi$ induced by the group character: $\sigma \mapsto \chi(\sigma)\sigma$ of $\Delta = G/H$ into $B[\Delta]^\times$, it is obvious that the induced representation ρ satisfies $\rho \cong \rho \otimes \chi$. Conversely we assume $\rho \cong \rho \otimes \chi$. We also write $V = V(\rho)$ for the representation space of ρ. Then by definition, we can find $C \in GL_n(B)$ such that $C(\chi(\sigma)\rho(\sigma))C^{-1} = \rho(\sigma)$ for all $\sigma \in G$. Then $C^r \rho(\sigma) C^{-r} = \rho(\sigma)$ for all σ. This combined with the absolute irreducibility of $\overline{\rho}$ shows that C^r is a scalar in $B^\times$ (Lemma 2.4). We take a local factor B' of $B[X]/(X^r - C^r)$, extend the scalar to B' and consider $V' = V \otimes_B B'$. Then C acts semi-simply on V'. Fixing an eigenvalue c of C on V', all other eigenvalues of C are given by ζc for an r-th root of unity ζ. Note that B contains all r-th roots of unity because χ has values in B. Let $V[c\zeta]$ be the $c\zeta$-eigenspace of C, which is a direct summand of V since r is prime to p. If $v \in V'[c\zeta]$, then we see from $\rho \cong \rho \otimes \chi$ that $C\rho(\sigma)v = \chi(\sigma)^{-1} c\zeta \rho(\sigma) v$. Thus G permutes $V'[c\zeta]$ and then $V' = \oplus_{\sigma \in \Delta} \rho(\sigma) V'[c]$. From this, it is easy to construct an $B[G]$–isomorphism $V' \cong \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], V'[c]) \cong B'[G] \otimes_{B'[H]} V'[c]$ sending $\sigma V'[c]$ to $\sigma \otimes V'[c]$, which proves the desired assertion. □

2.5. **Differential of group representations.** Let $G_{/E} = \mathrm{Spec}(\mathcal{O}_G)$ be a connected affine algebraic group and $\mathfrak{g}_{/E}$ be the Lie algebra of G. Consider E-derivations $\partial, \delta : \mathcal{O}_G \to \mathcal{O}_G$. By computation, we verify that $\Delta := [\partial, \delta] = \partial \circ \delta - \delta \circ \partial$ satisfies the derivation relation $\Delta(ab) = a\Delta(b) + b\Delta(a)$. Thus $Der_E(\mathcal{O}_G) = Der_E(\mathcal{O}_G, \mathcal{O}_G)$ is a Lie algebra. The multiplication $x \mapsto gx$ induces by pull-back a ring automorphism

$g^* : \mathcal{O}_G \to \mathcal{O}_G$. If $\partial \circ g^* = g^* \circ \partial$, we call ∂ a left invariant derivation. Since $[\partial, \delta]$ is left invariant if ∂ and δ are left invariant, we define the Lie algebra $\mathfrak{g}$ of G to be the Lie algebra of left invariant derivations. By evaluation at the identity $1 \in G$, we may (and do) identify $\mathfrak{g}$ with the tangent space at 1 of $\mathfrak{g}$.

There is another way of defining $\mathfrak{g}$ as the kernel of the homomorphism $G(E[\epsilon]) \to G(E))$ induced by the projection $E[\epsilon] \twoheadrightarrow E$, where $E[\epsilon] = E[x]/(x^2)$ (for the polynomial ring $E[x]$) with $\epsilon = x \mod (x^2)$. Indeed, writing $\underline{1} : \mathcal{O}_G \to E$ for the co-identity, for any $P \in \mathrm{Hom}_{ALG_{/E}}(\mathcal{O}_G, E[\epsilon]) = G(E[\epsilon])$ projecting down to $1 \in G(E)$, $P(a)$ for $a \in \mathcal{O}_G$ has the form $\underline{1}(a) + \partial(a)\epsilon$. We verify $\partial(ab) = \underline{1}(a)\partial(b) + \underline{1}(b)\partial(a)$ from $P(ab) = P(a)P(b)$, and hence ∂ is in the tangent space at 1. Similarly, if P projects down to $x \in G(E)$, writing $P(a) = \underline{x}(a) + \partial_x(a)\epsilon$, ∂_x is a tangent vector at x. From this, it is clear that the tangent space at 1 extends isomorphically to the Lie algebra of left invariant derivations.

Exercise 2.6. *Write down explicitly the Lie bracket $[x, y]$ for two given tangent vectors x, y at $1 \in G$ without extending x, y to vector fields over G* (cf. [LAG] §10.5).

Let G' be another connected linear algebraic group defined over E with a morphism $\rho : G \to G'$ of group schemes over E. Write $\mathfrak{g}'$ for the Lie algebra of G'. Then its *differential* $d\rho = \rho_* : \mathfrak{g} \to \mathfrak{g}'$ is a homomorphism of Lie algebras.

Exercise 2.7. *Check that $d\rho$ is a homomorphism of Lie algebras.*

An E-rational representation $\rho : G_{/E} \to GL(n)_{/E}$ is a homomorphism of E-group schemes. Write $\mathfrak{gl}_n(E)$ for the Lie algebra of $GL(n)_{/E}$. Then $\mathfrak{gl}_n(E)$ can be identified with the Lie algebra of $n \times n$ matrices $M_n(E)$ with entries in E whose Lie bracket is given by $[x, y] = xy - yx$ for the matrix product xy with $x, y \in M_n(E)$. Then $d\rho : \mathfrak{g} \to \mathfrak{gl}_n(E)$ is an E-linear representation of Lie algebras. Since ρ is complex analytic after extending scalars to $\mathbb{C}/E$ (after embedding E into $\mathbb{C}$), ρ is absolutely irreducible if and only if $d\rho$ is absolutely irreducible. Over $\mathbb{C}$, the exponential map $\exp_G : \mathfrak{g}_{/\mathbb{C}} = \mathfrak{g} \otimes_E \mathbb{C} \to G(\mathbb{C})$ given by usual formula $\exp_G(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$ converges absolutely, giving an analytic surjection of $\mathfrak{g}_{/\mathbb{C}}$ onto $G(\mathbb{C})$ whose inverse is given by $\log_G(g) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(g-1)^n}{n}$. Then we see easily that $\exp_{GL(n)}(d\rho(X)) = \rho(\exp_G(X))$ and $\log_{GL(n)}(\rho(g)) = d\rho(\log_G(g))$ for all $X \in \mathfrak{g}_{/\mathbb{C}}$ and $g \in G(\mathbb{C})$ (see [GME] §4.3.3 for a p-adic version of this). From this, the above equivalence on absolute irreducibility of ρ and $d\rho$ is clear.

3. Lie Algebras over p-Adic Ring

We describe Lie theory over adic rings.

3.1. **Logarithm and exponential.** Let $\mathfrak{gl}_n(A)$ be $M_n(A)$ for a commutative ring A regarded as a Lie algebra over A under the standard Lie bracket $[X, Y] = XY - YX$. We call a ring A a *p-adic ring* if $A = \varprojlim_n A/p^n A$ for a prime p. In particular, a p-profinite ring A is a p-adic ring, since we have

$$A = \varprojlim_n A_n = \varprojlim_n \varprojlim_m A_n/p^m A_n = \varprojlim_m \varprojlim_n A_n/p^m A_n = \varprojlim_m A/p^m A,$$

where A_n is a finite ring with p-power order. Let A be a p-adic local ring flat over $\mathbb{Z}_p$. Write $\mathbf{p} = 4$ if $p = 2$ and otherwise $\mathbf{p} = p$. Consider the exponential and logarithm

power series

$$\log(1+X)=\sum_{n=1}^{\infty}(-1)^{n+1}\frac{X^n}{n} \quad \text{and} \quad \exp(X)=\sum_{n=0}^{\infty}\frac{X^n}{n!}.$$

As is well known, the power series $\log(X)$ (resp. $\exp(X)$) converge p-adically over $1+p\cdot M_n(A)$ (resp. $p\cdot\mathfrak{gl}_n(A)$) giving rise to a p-adic analytic function (see [LFE] §1.3):

$$\log_p : 1+p\cdot M_n(A)\to \mathfrak{gl}_n(A) \text{ and } \exp_p : p\cdot\mathfrak{gl}_n(A)\to 1+p\cdot M_n(A).$$

We have an *adjoint action* Ad of $GL_n(A)$ on $\mathfrak{gl}_n(A)$ given by $Ad(x)(X)=xXx^{-1}$ which commutes with $\log_p$ and $\exp_p$.

In the rest of this subsection, we suppose

(a) A is a p-profinite noetherian local ring flat over $\mathbb{Z}_p$ with the total quotient ring $Q(A)$;
(g) $G\subset SL_n(A)$ is a profinite subgroup.

Put $\Gamma_A(\mathfrak{a})=\{g\in SL_n(A)|g-1\in\mathfrak{a}M_n(A)\}$ for an ideal $\mathfrak{a}$ of A. Let

$$\mathfrak{sl}_n(A)=\{X\in\mathfrak{gl}_n(A)|\mathrm{Tr}(X)=0\}$$

which is a Lie A-subalgebra of $\mathfrak{gl}_n(A)$ and the Lie algebra of $SL_n(A)$.

Lemma 3.1. *Assume* (a). *Then* $\log_p$ *and* $\exp_p$ *give rise to* p*-adic analytic maps*

$$\log_p : \Gamma_A(\mathbf{p})\to \mathbf{p}\cdot\mathfrak{sl}_n(A) \quad \textit{and} \quad \exp_p : \mathbf{p}\cdot\mathfrak{sl}_n(A)\to\Gamma_A(\mathbf{p}) \tag{3.1}$$

with $\log_p\circ\exp_p=\mathrm{id}_{\mathbf{p}\cdot\mathfrak{sl}_n(A)}$ *and* $\exp_p\circ\log_p=\mathrm{id}_{\Gamma(\mathbf{p})}$, *where* $\Gamma_A(\mathfrak{a})=SL_n(A)\cap(1+\mathfrak{a}M_n(A))$ *for an ideal* $\mathfrak{a}$ *of* A. *Similarly* $\exp_P$ *and* $\log_P$ *are* P*-adic analytic maps*

$$\log_P : 1+P\cdot\mathfrak{sl}_n(\widehat{A}_P)\to P\cdot\mathfrak{sl}_n(\widehat{A}_P), \quad \exp_P : P\cdot\mathfrak{sl}_n(\widehat{A}_P)\to 1+P\cdot\mathfrak{sl}_n(\widehat{A}_P)$$

for a prime $P\in\mathrm{Spec}(A)$ *with characteristic* 0 *residue field.*

We write simply $\Gamma(\mathfrak{a})$ for $\Gamma_A(\mathfrak{a})$ if confusion is unlikely.

Proof. Analyticity of the maps is plain by definition; so, we only need to prove that log has values in $\mathfrak{sl}_n$ and exp has values in SL_n. Since the proof is the same for p and P, we give a proof for $\exp_p$ and $\log_p$. For an upper triangular $n\times n$ matrix Δ with diagonal entry $\delta_1,\dots,\delta_n$, if $\log_p(\Delta)$ (resp. $\exp_p(\Delta)$) is well defined, it is upper triangular with diagonal entries $\log_p(\delta_1),\dots,\log_p(\delta_n)$ (resp. $\exp_p(\delta_1),\dots,\exp_p(\delta_n)$). Thus we conclude $\det(\exp_p(\Delta))=\prod_j\exp_p(\delta_j)=\exp_p(\mathrm{Tr}(\Delta))$ and $\mathrm{Tr}(\log_p(\Delta))=\sum_j\log_p(\delta_j)=\log_p(\det(\Delta))$. If A is a domain, over a finite flat extension of A (which is still p-profinite), we can bring any matrix to an upper-triangular form, we have $\det(\exp_p(X))=\exp_p(\mathrm{Tr}(X))$ and $\mathrm{Tr}(\log_p(X))=\log_p(\det(X))$. Thus if A is a domain, we get the desired assertion; i.e., $\log_p(\Gamma(\mathbf{p}))\subset\mathbf{p}\cdot\mathfrak{sl}_n(A)$ and $\exp_p(\mathbf{p}\cdot\mathfrak{sl}_n(A))\subset\Gamma(\mathbf{p})$. The corresponding power series identity proves

$$\log_p\circ\exp_p=\mathrm{id}_{\mathbf{p}\cdot\mathfrak{sl}_n(A)} \quad \text{and} \quad \exp_p\circ\log_p=\mathrm{id}_{\Gamma(\mathbf{p})}.$$

Under (a), by [CRT] Theorem 29.4, we have a surjective ring homomorphism $R\to A$ for a regular complete noetherian local p-profinite domain R of characteristic 0, which induces the surjective ring homomorphism $\pi : M_n(R)\to M_n(A)$. By definition, $\log_p(\pi(X))=\pi(\log_p(X))$ and $\exp_p(\pi(X))=\pi(\exp_p(X))$ as long as these maps are

well defined for $X \in M_n(R)$. Since R is a domain, we have on $M_n(R)$, $\det(\exp_p(X)) = \exp_p(\mathrm{Tr}(X))$ and $\mathrm{Tr}(\log_p(X)) = \log_p(\det(X))$. Thus we conclude the same identity for any A satisfying (a). This finishes the proof. □

3.2. **Lie Algebras of p-Profinite Subgroups of $SL(2)$.** If A is a p-profinite ring of characteristic p, obviously the power series $\log(1+X)$ and $\exp(X)$ do not make much sense; so, the relation between closed subgroups in $SL_n(A)$ and Lie subalgebras of $\mathfrak{sl}_n(A)$ is not very direct. Indeed, for almost all p-profinite subgroups $\mathcal{G}$ of $\Gamma_\Lambda(\mathbf{p})$, $\log_p(\mathcal{G})$ may not be a Lie algebra (over $\mathbb{Z}_p$). There are good criteria in [GAN] for $\log_p(\mathcal{G})$ to be a Lie $\mathbb{Z}_p$-subalgebra of $\mathfrak{sl}_n(A)$, but it would be fair to say that they are effective only when A is finite flat over $\mathbb{Z}_p$. Thus we need a different way to cover characteristic 0 and p profinite rings uniformly.

The *principal congruence subgroup*

$$\Gamma_A(\mathfrak{a}) = \{x \in SL_2(A) | x \equiv 1 \mod \mathfrak{a}\}$$

for an A-ideal $\mathfrak{a}$ plays an important role in this chapter, which can be written as $SL_2(A) \cap (1 + \mathfrak{a} \cdot \mathfrak{gl}_2(A))$. Note that $\mathfrak{a} \cdot \mathfrak{gl}_2(A)$ is a Lie algebra.

To study a general p-profinite subgroup $\mathcal{G}$ of $SL_2(A)$, we somehow want to have an explicit relation between p-profinite subgroups $\mathcal{G}$ of the form $SL_2(A) \cap (1+X)$ and Lie $\mathbb{Z}_p$-subalgebras $X \subset \mathfrak{gl}_2(A)$. Under the condition that $p > 2$, Pink found a functorial explicit relation between closed p-profinite subgroups in $SL_2(A)$ and Lie subalgebras X of $\mathfrak{gl}_2(A)$ (valid even for A of characteristic p). We call subgroups of the form $SL_2(A) \cap (1 + X)$ *basic subgroups* following Pink's terminology.

We prepare some notation to quote here the result in [P]. A ring is called *semi-local* if it has only finitely many maximal ideals. Let A be a semi-local p-profinite ring (not necessarily of characteristic p and not necessarily noetherian). Since Pink's result allows semi-local p-profinite algebras, we do not assume A to be local in the exposition of his result. (but we assume it to be local in any of the proof).

Exercise 3.2. *Let q be a p-power. Then prove $|SL_2(\mathbb{F}_q)| = (q+1)(q-1)q$. In particular, the p-Sylow subgroup of $SL_2(\mathbb{F}_q)$ is $U(\mathbb{F}_q) = \{\left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right) | u \in \mathbb{F}_q\}$.*

Let $\mathcal{G} \subset SL_2(A)$ be a p-profinite subgroup. Then its image in $SL_2(A/\mathfrak{m}_A) = SL_2(\mathbb{F}_q)$ is in p-Sylow subgroup. By Exercise 3.2, any $x \in \mathcal{G}$ has trace modulo $\mathfrak{m}_A$ equal to the trace of unipotentn element; so, $\mathrm{Tr}(x) \equiv 2 \mod \mathfrak{m}_A$ for all $x \in \mathcal{G}$. Hereafter, we assume $p > 2$. Define $\Theta : SL_2(A) \to \mathfrak{sl}_2(A)$ and $C : SL_2(A) \to Z(A)$ for the center $Z(A)$ of $M_2(A)$ by

$$\Theta(x) = x - \frac{1}{2}\mathrm{Tr}(x)1_2 \quad \text{and} \quad \zeta(x) = \frac{1}{2}(\mathrm{Tr}(x) - 2)1_2$$

for $1_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Since $x \mod \mathfrak{m}_A$ is unipotent for $x \in \mathcal{G}$, replacing $\mathcal{G}$ by its conjugate in $SL_2(A)$, we may assume that $(\mathcal{G} \mod \mathfrak{m}_A) \subset U(A/\mathfrak{m}_A)$; so, $\Theta(x) \mod \mathfrak{m}_A$ is upper nilpotent; so, $\Theta(x)\Theta(y) \equiv 0 \mod \mathfrak{m}_A$ for $x, y \in \mathcal{G}$. Define L by the closed additive subgroup of $\mathfrak{sl}_2(A)$ (topologically) generated by $\Theta(x)$ for all $x \in \mathcal{G}$. Since $\Theta(x)\Theta(y) \equiv 0 \mod \mathfrak{m}_A$ for $x \in \mathcal{G}$, we have $L \cdot L \subset \mathfrak{m}_A M_2(A)$. Then we put $C = \mathrm{Tr}(L \cdot L) \subset \mathfrak{m}_A$. Here $L \cdot L$ is the closed additive subgroup of $M_2(A)$ generated by $\{xy | x, y \in L\}$ for the matrix product xy; similarly, L^n is the closed additive subgroup generated by n times iterated products of elements in L. We then define $L_1 = L$ and inductively

$L_{n+1} = [L, L_n] \subset \mathfrak{m}_A^n \mathfrak{sl}_2(A)$; so, $L_2 = [L, L]$, where $[L, L_n]$ is the closed additive subgroup generated by Lie bracket $[x, y] = xy - yx$ for $x \in L$ and $y \in L_n$. By an easy computation we will do later, we get

$$[x, y] = [\Theta(x), y] = [x, \Theta(y)] = [\Theta(x), \Theta(y)] \text{ and } [x, y] = \Theta(xy) - \Theta(yx).$$

From this we get $[\Theta(x), \Theta(y)] = \Theta(xy) - \Theta(yx)$ and hence $[L, L] \subset L$. We will verify

$$[L, L] \subset L,\ C \cdot L \subset L,\ L = L_1 \supset \cdots \supset L_n \supset L_{n+1} \supset \cdots \quad \text{and} \quad \bigcap_{n\geq 1} L_n = \bigcap_{n\geq 1} L^n = 0. \tag{3.2}$$

In particular, L is a Lie $\mathbb{Z}_p$-subalgebra of $\mathfrak{sl}_2(A)$. Put

$$\mathcal{M}_n(\mathcal{G}) = C \cdot 1_2 \oplus L_n \subset M_2(A) = \mathfrak{gl}_2(A),$$

which is a closed Lie $\mathbb{Z}_p$-subalgebra by (3.2). In particular, we write $\mathcal{M}(\mathcal{G})$ for $\mathcal{M}_2(\mathcal{G})$. Define

$$\mathcal{H}_n = \{x \in SL_2(A) | \Theta(x) \in L_n,\ \mathrm{Tr}(x) - 2 \in C\} \text{ for } n \geq 1.$$

If $x \in \mathcal{H}_n$, then $x = \Theta(x) + \zeta(x) + 1_2$, thus $\mathcal{H}_1 \subset SL_2(A) \cap (1 + \mathcal{M}_n(\mathcal{G}))$. If we pick $x \in SL_2(A) \cap (1 + \mathcal{M}_n(\mathcal{G}))$, then $x = 1 + c \cdot 1 + y$ with $y \in L_n$ and $c \in C$. Thus $\mathrm{Tr}(x) - 2 = 2c \in C$ and $\Theta(x) = 1_2 + c \cdot 1_2 + y - \frac{1}{2}(2 + 2c) \cdot 1_2 = y$. This shows

$$\mathcal{H}_n = SL_2(A) \cap (1 + \mathcal{M}_n(\mathcal{G})) \text{ in particular, } \mathcal{H}_2 = SL_2(A) \cap (1 + \mathcal{M}(\mathcal{G})).$$

By (3.2), $\mathcal{H}_1$ is a group containing $\mathcal{G}$. For $x, y \in \mathcal{G}$, write $x = a + \Theta(x)$ and $y = b + \Theta(y)$; so, $a, b \in A$ (in the center of $M_2(A)$). Then $xy = ab + a\Theta(y) + b\Theta(x) + \Theta(x)\Theta(y)$; so, $\Theta(xy) = a\Theta(y) + b\Theta(x) + \Theta(x)\Theta(y)$ and $1 + \zeta(xy) = ab$. Thus shows $L^2 \subset L$. We can prove that $\mathcal{H}_n$ are p-profinite subgroups of $SL_2(A)$. We will see this after stating the main result of Pink (Theorem 3.3 combined with Theorem 2.7 in [P]):

Theorem 3.3 (Pink)**.** *Let the notation be as above. Suppose $p > 2$, and A be a semi-local p-profinite algebra. Let $\mathcal{G} \subset SL_2(A)$ be a p-profinite subgroup. Then we have*

1. *$\mathcal{G}$ is a normal closed subgroup of $\mathcal{H}_1$,*
2. *$\mathcal{H}_{n+1}$ $(n \geq 1)$ is a subgroup of $SL_2(A)$ given by $\mathcal{H}_{n+1} = (\mathcal{H}_1, \mathcal{H}_n)$ (which is the closed subgroup topologically generated by commutators (x, y) with $x \in \mathcal{H}_1$ and $y \in \mathcal{H}_n$),*
3. *$\{\mathcal{H}_n\}_{n\geq 2}$ coincides with the descending central series of $\{\mathcal{G}_n\}_{n\geq 2}$, where $\mathcal{G}_{n+1} = (\mathcal{G}, \mathcal{G}_n)$ starting with $\mathcal{G}_1 = \mathcal{G}$.*

In short, we have

(P) *The topological commutator subgroup $\mathcal{G}'$ of $\mathcal{G}$ is the subgroup given by $SL_2(A) \cap (1 + \mathcal{M}(\mathcal{G}))$ for the closed Lie subalgebra $\mathcal{M}(\mathcal{G}) \subset \mathfrak{gl}_2(A)$ defined as above.*

We refer the proof of this technical theorem to [GME] §4.3.12.

Put $\mathcal{M}_j^0(\mathcal{G}) = \mathcal{M}_j(\mathcal{G}) \cap \mathfrak{sl}_2(A)$ and $\mathcal{M}^0(\mathcal{G}) = \mathcal{M}_2(\mathcal{G}) \cap \mathfrak{sl}_2(A)$. By the expression given before stating the theorem, the association $\mathcal{G} \mapsto \mathcal{M}_j(\mathcal{G})$ (resp. $\mathcal{G} \mapsto \mathcal{M}_j^0(\mathcal{G})$) is a covariant functor from p-profinite subgroups of $SL_2(A)$ into closed Lie $\mathbb{Z}_p$-subalgebras of $\mathfrak{gl}_2(A)$ (resp. $\mathfrak{sl}_2(A)$). In particular, $\mathcal{M}_j(\mathcal{G})$ and $\mathcal{M}_j^0(\mathcal{G})$ are stable under the adjoint action $x \mapsto gxg^{-1}$ of $\mathcal{G}$. For an A-ideal $\mathfrak{a}$, writing $\overline{\mathcal{G}}_{\mathfrak{a}} = (\mathcal{G} \mod \mathfrak{a}) = (\mathcal{G} \cdot \Gamma_A(\mathfrak{a}))/\Gamma_A(\mathfrak{a})$,

$\mathcal{M}_j(\overline{\mathcal{G}}_{\mathfrak{a}}) \subset \mathfrak{gl}_2(A/\mathfrak{a})$ (resp. $\mathcal{M}^0_j(\overline{\mathcal{G}}_{\mathfrak{a}}) \subset \mathfrak{sl}_2(A/\mathfrak{a})$) is the surjective image of $\mathcal{M}_j(\mathcal{G})$ (resp. $\mathcal{M}^0_j(\mathcal{G})$) under the reduction map $x \mapsto (x \mod \mathfrak{a})$. Since $\mathcal{H}_1$ is almost equal to $\mathcal{G}$ with $\mathcal{H}_1/\mathcal{G}$ abelian, we call $\mathcal{H}_1$ the *basic closure* of $\mathcal{G}$. If $\mathcal{G}$ is normalized by an element of $GL_2(A)$, by construction, the basic closure $\mathcal{H}_1$ is also normalized by the same element. Thus the normalizer of $\mathcal{G}$ in $GL_2(A)$ is contained in the normalizer of $\mathcal{H}_1$ in $GL_2(A)$. By the above theorem, any p-profinite subgroup of $SL_2(A)$ is basic up to abelian error.

To show that $\mathcal{H}_n$ are groups, we prepare

Lemma 3.4. *We have the following relation between 2×2 matrices $x, y \in \mathfrak{gl}_2(A)$ in the Lie algebra $\mathfrak{gl}_2(A)$:*

(1) $[x,y] = [\Theta(x), y] = [x, \Theta(y)] = [\Theta(x), \Theta(y)]$,
(2) $[x,y] = \Theta(xy) - \Theta(yx)$,
(3) $2\cdot\Theta(xy) = [\Theta(x), \Theta(y)] + \mathrm{Tr}(x)\cdot\Theta(y) + \mathrm{Tr}(y)\cdot\Theta(x)$,
(4) $2\cdot\mathrm{Tr}(xy) = 2\cdot\mathrm{Tr}(\Theta(x)\Theta(y)) + \mathrm{Tr}(x)\cdot\mathrm{Tr}(y)$,
(5) $(\mathrm{Tr}(x))^2 = 4\cdot\det(x) + 2\cdot\mathrm{Tr}(\Theta(x)^2)$,
(6) $x, y \in \mathfrak{sl}_2(A) \Rightarrow \mathrm{Tr}(xy)1_2 = xy + yx$,
(7) $x \in SL_2(A) \Rightarrow \Theta(x^{-1}) = -\Theta(x)$,
(8) $x \in SL_2(A) \Rightarrow \mathrm{Tr}(x^{-1}) = \mathrm{Tr}(x)$,
(9) $x \in SL_2(A) \Rightarrow \mathrm{Tr}(x)\cdot\Theta(y) = \Theta(xy) + \Theta(x^{-1}y)$,

and for $x, y, u, v \in \mathfrak{sl}_2(A)$,

(a) $4\cdot\mathrm{Tr}(xy)\cdot[u,v] = [y,[x,[u,v]]] + [x,[y,[u,v]]] + [[x,v],[y,u]] + [[y,v],[x,u]]$.

Proof. The first 9 formulas are easy. Recall $\Theta(x) = x - \frac{1}{2}\mathrm{Tr}(x)1_2$. Since $\frac{1}{2}\mathrm{Tr}(x)1_2$ commutes with any matrix and $\mathrm{Tr}(xy) = \mathrm{Tr}(yx)$, we have (1) and (2). Since $\det(x) = ad - bc$ for $x = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and

$$2\mathrm{Tr}(\Theta(x)^2) = \frac{1}{2}\mathrm{Tr}\left(\left(\begin{smallmatrix} a-d & 2b \\ 2c & d-a \end{smallmatrix}\right)^2\right) = (a-d)^2 + 4bc,$$

we get

$$4\cdot\det(x) + 2\cdot\mathrm{Tr}(\Theta(x)^2) = 4(ad-bc) + 2(a-d)^2 + 4bc = (a+d)^2 = \mathrm{Tr}(x)^2$$

proving (5). If $x \in SL_2$, we have $x^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$; so, $\mathrm{Tr}(x^{-1}) = \mathrm{Tr}(x)$ $\Theta(x^{-1}) = -\Theta(x)$, getting (7) and (8). As for (9), for $x \in SL_2(A)$ and $y \in M_2(A)$, we note $\mathrm{Tr}(x)\cdot\Theta(y) = \Theta(xy) + \Theta(x^{-1}y)$. To see this, writing $y = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$, we see

$$\begin{aligned}\mathrm{Tr}(xy) + \mathrm{Tr}(x^{-1}y) &= (a\alpha + b\gamma + c\beta + d\delta) + (d\alpha - b\gamma - c\beta + a\delta) \\ &= \alpha\mathrm{Tr}(x) + \delta\mathrm{Tr}(x) = \mathrm{Tr}(x)\mathrm{Tr}(y).\end{aligned}$$

Then we haves

$$(\Theta(xy)+\Theta(x^{-1}y)) = xy + x^{-1}y - \frac{\mathrm{Tr}(x)\mathrm{Tr}(y)}{2}1_2 = y\mathrm{Tr}(x)1_2 - \frac{\mathrm{Tr}(x)\mathrm{Tr}(y)}{2}1_2 = \mathrm{Tr}(x)\Theta(y)$$

as desired. We leave the reader to verify the rest in (1–9).

To verify (a), we note that the two sides of (a) are skew-symmetric with respect to (u,v) and symmetric with respect to (x,y). For any symmetric bilinear pairing $S(x,y)$

on an A-module, we have

$$S(x,y)=\frac{1}{2}(S(x+y,x+y)-S(x,x)-S(y,y)).$$

Thus the symmetric pairing $S(x,y)$ is determined by its quadratic form $S(x,x)$ as long as $2\in A^\times$. By (6), we have x^2 is scalar $\frac{1}{2}\mathrm{Tr}(x^2)$. Thus to show (a), we may assume that $x=y$, which becomes

$$(*)\qquad 4x^2[u,v]=[x,[x,[u,v]]]+[[x,v],[x,u]].$$

We only need to check this formula. Since this is bilinear skew symmetric with respect to the variable (u,v), we only need to check this for

$$(u,v)=(U,V),\ (V,X)\ \text{ and }\ (X,U)$$

for $U=\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$, $V=\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)$ and $X=[U,V]=\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$. For example, if $(u,v)=(U,V)$, writing $x=\left(\begin{smallmatrix}a&b\\c&-a\end{smallmatrix}\right)$, we confirm that $x^2=\left(\begin{smallmatrix}a^2+bc&0\\0&a^2+bc\end{smallmatrix}\right)$ commutes with $X=[U,V]$,

$$[x,[x,[U,V]]]=2x^2[U,V]-2x[U,V]x=4\left(\begin{smallmatrix}bc&-ab\\-ac&-bc\end{smallmatrix}\right)$$

and

$$[[x,V],[x,U]]=\left[\left(\begin{smallmatrix}b&0\\-2a&-b\end{smallmatrix}\right),\left(\begin{smallmatrix}-c&2a\\0&c\end{smallmatrix}\right)\right]=4\left(\begin{smallmatrix}a^2&ab\\ac&-a^2\end{smallmatrix}\right).$$

Since $x^2=\left(\begin{smallmatrix}a^2+bc&0\\0&a^2+bc\end{smallmatrix}\right)$ by (6), we get the desired identity

$$4x^2[U,V]=[x,[x,[U,V]]]+[[x,V],[x,U]].$$

Verification of $(*)$ for $(u,v)=(V,X)$ and (X,U) is left to the reader. □

Proof of (3.2): The inclusion $[L,L]\subset L$) follows from the formulas Proposition 3.4 (1) and (2):

$$[\Theta(x),\Theta(y)]=\Theta(xy)-\Theta(yx).$$

As for $C\cdot L\subset L$, by Proposition 3.4 (4), we have

$$C=\mathrm{Tr}(L\cdot L)\subset\mathrm{Tr}(\mathcal{G})+\mathrm{Tr}(\mathcal{G})^2.$$

Note that Proposition 3.4 (9) implies $\mathrm{Tr}(\mathcal{G})\cdot L\subset L$; hence, $C\cdot L\subset L$, as desired. Since $\bigcap_n L^{2n}\subset\bigcap_n \mathfrak{m}_A^n M_2(A)=\{0\}$ by Krull's intersection theorem [CRT] Theorem 8.9. Thus $\bigcap_n L^n=\bigcap_n L^{2n}=\{0\}$ and $L_n\subset L^n$ shows $\bigcap_n L_n=\{0\}$. □

Lemma 3.5. *Let $p>2$. Let A be an integral domain finite flat either over $\mathbb{F}_p[[T]]$, Λ or $\mathbb{Z}_p$. If a subgroup $G\subset SL_2(A)$ contains a congruence subgroup $\Gamma_A(\mathfrak{c})$ for a non-zero A-ideal $\mathfrak{c}$, then $\alpha G\alpha^{-1}$ for $\alpha\in GL_2(Q(A))$ contains $\Gamma_A(\mathfrak{c}')$ for another non-zero A-ideal $\mathfrak{c}'$ depending on α.*

Proof. For simplicity, we write $\Gamma(\mathfrak{c})$ for $\Gamma_A(\mathfrak{c})$. We may suppose that $G=\Gamma(\mathfrak{c})$ for an ideal $\mathfrak{c}$ inside the maximal ideal of A; so, G is p-profinite. Then, we have $\mathcal{M}_1^0(G)\supset\mathfrak{c}\cdot\mathfrak{L}$ for $\mathfrak{L}=\mathfrak{sl}_2(A)$. Then we see $\mathcal{M}^0(G)=[\mathcal{M}_1^0(G),\mathcal{M}_1^0(G)]=\mathfrak{c}^2\mathfrak{L}$. Replacing α by $\xi\alpha$ for a suitable $\xi\in A\cap Q(A)^\times$ for the quotient field $Q(A)$ of A, we may assume that $\alpha\in M_2(A)\cap GL_2(Q(A))$. Then $(\alpha\mathfrak{L}\alpha^{-1}\cap\mathfrak{L})\supset\alpha\mathfrak{L}\alpha^\iota$ for $\alpha^\iota=\det(\alpha)\alpha^{-1}\in M_2(A)$. Since $\mathfrak{L}$ and $\alpha\mathfrak{L}\alpha^\iota$ are both free A-module of rank 3, $\mathfrak{L}/\alpha\mathfrak{L}\alpha^\iota$ is a torsion A-module finite type annihilated by a non-zero A-ideal $\mathfrak{c}''$. Then $\mathcal{M}(\alpha\Gamma(\mathfrak{c})\alpha^{-1}\cap SL_2(A))\supset\mathfrak{c}^2\cdot\alpha\mathfrak{L}\alpha^{-1}\supset\mathfrak{c}^2\mathfrak{c}''\mathfrak{L}$. Thus the ideal $\mathfrak{c}_\alpha:=\mathfrak{c}^2\mathfrak{c}''$ does the job (as C for G is $\mathfrak{c}^2\cdot Z(A)$). □

Let $\mathcal{B}_{/\mathbb{Z}_p} \subset GL(2)_{/\mathbb{Z}_p}$ (resp. $\mathcal{Z}_{/\mathbb{Z}_p}$) be the upper triangular Borel subgroup (resp. the center of $GL(2)_{/\mathbb{Z}_p}$) as an algebraic group. Write $\mathcal{U}_{/\mathbb{Z}_p}$ for the unipotent radical of $\mathcal{B}_{/\mathbb{Z}_p}$ and $\mathcal{ZU}$ for the radical of $\mathcal{B}$; so, $\mathcal{ZU}(A) = \mathcal{Z}(A)\mathcal{U}(A)$. Let $\mathfrak{B}_{/\mathbb{Z}_p}$ (resp. $\mathfrak{U}_{/\mathbb{Z}_p}$) be the Lie algebra of $\mathcal{B}_{/\mathbb{Z}_p}$ (resp. $\mathcal{U}_{/\mathbb{Z}_p}$). We write $\mathcal{B} = \mathbb{G}_m^2 \ltimes \mathcal{U}$ by the splitting $\mathbb{G}_m^2 \ni (t,t') \mapsto \left(\begin{smallmatrix} t & 0 \\ 0 & t' \end{smallmatrix}\right) \in \mathcal{B}$.

Lemma 3.6. *Let A be a complete discrete valuation ring with finite residue field. If $G \subset SL_2(A)$ is an open subgroup, its derived subgroup (i.e., commutator subgroup) is an open subgroup of $SL_2(A)$.*

Since we use this lemma only when A has residual characteristic > 2, we prove the lemma when $A/\mathfrak{m}_A$ has characteristic $p > 2$.

Proof. Since $G \supset \Gamma(\mathfrak{m}^m) = \Gamma_A(\mathfrak{m}^m)$ with $\mathfrak{m} = \mathfrak{m}_A$ for $m > 0$, we may assume that $G = \Gamma(\mathfrak{m}^m)$. Let G' be the derived group of $G = \Gamma(\mathfrak{m}^m)$. We claim that $G' = \Gamma(\mathfrak{m}^{2m})$. Let ϖ be the generator of $\mathfrak{m}$ and put $a = \varpi^m$. Write $(x,y) = x^{-1}y^{-1}xy$ for the commutator. Then for $X, Y \in M_2(A)$,

$$(1+aX, 1+aY) \equiv (1-aX)(1-aY)(1+aX)(1+aY) \equiv 1 \mod a^2,$$

and hence $G' \subset \Gamma(\mathfrak{m}^{2m})$. Assuming that p is odd, we prove now that $G'\Gamma(\mathfrak{m}^{2m+1})/\Gamma(\mathfrak{m}^{2m+1})$ is equal to $\Gamma(\mathfrak{m}^{2m})/\Gamma(\mathfrak{m}^{2m+1})$. Note that $\Gamma(\mathfrak{m}^{2m})/\Gamma(\mathfrak{m}^{2m+1}) \cong \mathfrak{sl}_2(\mathbb{F})$ for $\mathbb{F} = A/\mathfrak{m}$ by $1+aX \mapsto X$. Let $X = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and $Y = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$. Then we have $[X,Y] = XY - YX = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and

$$(1+aX, 1+aY) \overset{(*)}{=} (1-aX)(1-aY)(1+aX)(1+aY) \equiv 1 + a^2[X,Y] \mod a^3.$$

Note here the identity $(*)$ is an equality not just a congruence as $X^2 = Y^2 = 0$. Thus $G'\Gamma(\mathfrak{m}^{2m+1})/\Gamma(\mathfrak{m}^{2m+1})$ contains $(1+aX, 1+aY)$ which is non-trivial. By conjugation, $SL_2(A)$ acts on $G = \Gamma(\mathfrak{m}^m)$. The action factors through $SL_2(\mathbb{F})$ and induces the conjugate action of $SL_2(\mathbb{F})$ on $\mathfrak{sl}_2(\mathbb{F}) \cong \Gamma(\mathfrak{m}^{2m})/\Gamma(\mathfrak{m}^{2m+1})$. If $p > 2$, it is easy to verify this adjoint action of $SL_2(\mathbb{F})$ on $\mathfrak{sl}_2(\mathbb{F})$ is irreducible (see Exercise at the end of §3.3). Thus $G'\Gamma(\mathfrak{m}^{2m+1})/\Gamma(\mathfrak{m}^{2m+1}) = \Gamma(\mathfrak{m}^{2m})/\Gamma(\mathfrak{m}^{2m+1})$. Suppose we have proven $G'\Gamma(\mathfrak{m}^{2m+j-1})/\Gamma(\mathfrak{m}^{2m+j}) = \Gamma(\mathfrak{m}^{2m})/\Gamma(\mathfrak{m}^{2m+j})$ for $j \geq 1$. Then we have

$$\begin{aligned}(1+aX, 1+a\varpi^j Y) &= (1-aX)(1-a\varpi^j Y)(1+aX)(1+a\varpi^j Y) \\ &\equiv 1 + a^2\varpi^j[X,Y] \mod a^3\varpi^j.\end{aligned}$$

Again we find a non-trivial element

$$(1+aX, 1+a\varpi^j Y) \in G'\Gamma(\mathfrak{m}^{2m+j})/\Gamma(\mathfrak{m}^{2m+j+1}).$$

Then by induction on j, we get

$$G'\Gamma(\mathfrak{m}^{2m+j})/\Gamma(\mathfrak{m}^{2m+j+1}) = \Gamma(\mathfrak{m}^{2m})/\Gamma(\mathfrak{m}^{2m+j+1})$$

for all $j > 0$. Passing to the limit, we have

$$G' = \varprojlim_j G'\Gamma(\mathfrak{m}^{2m+j-1})/\Gamma(\mathfrak{m}^{2m+j}) = \varprojlim_j \Gamma(\mathfrak{m}^{2m})/\Gamma(\mathfrak{m}^{2m+j}) = \Gamma(\mathfrak{m}^{2m}).$$

This finishes the proof. □

3.3. **Lie Algebra and Lie Group over $\mathbb{Z}_p$.** We study here the structure of closed subgroups G of $SL_2(\mathbb{Z}_p)$. Thus in this section, we have $A = \mathbb{Z}_p$.

Lemma 3.7. *Let K be a field of characteristic 0. If $M \subset M_2(K)$ is a semi-simple quadratic extension of K, the commutant*

$$C(M) = \{x \in M_2(K) | xy = yx \text{ for all } y \in M\}$$

of M is equal to M, and for the normalizer $N(M^\times)$ of $M^\times$ in $GL_2(K)$, the quotient $N(M^\times)/M^\times$ has order 2.

Proof. Since M is semi-simple, $M_2(K)$ is a free M-module of rank 2. Write $M_2(K) = M \oplus Mx$ with $x \in GL_2(K)$. We can choose such x because

$$\{g \in M_2(K) | g \notin M\} \not\subset \{h \in M_2(K) | \det(h) = 0\}$$

as the left-hand side is a Zariski open subset of $M_2(K)$ and the right-hand side is a proper Zariski closed set of codimension 1. Any $x \in GL_2(K) \setminus M$ does the job. If x commutes with M, it commutes with all $M_2(K)$; so, it is a scalar matrix. Since M contains scalar matrices, x cannot be scalar.

If such an $x \in GL_2(K) \setminus M$ normalizes $M^\times$, it normalizes M, and the conjugation $a \mapsto xax^{-1}$ induces a non-trivial K-algebra automorphism of M; so, $N(M^\times)/M^\times$ has at most two elements. Regarding M as a two-dimensional vector space over K, we may identify $M_2(K) = \mathrm{End}_K(M)$, and we may regard $M \subset M_2(K) = \mathrm{End}_K(M)$ sending $a \in M$ to the K-linear endomorphism of M obtained from the multiplication by $a \in M$. Then the non-trivial ring automorphism $\sigma \in \mathrm{Aut}(M_{/K})$ gives rise to a nontrivial element in $GL_2(K)$ normalizing $M^\times$. □

Lemma 3.8. *Let K be a field of characteristic 0. If $M \subset M_2(K)$ is a maximal non-semisimple commutative K-subalgebra of $M_2(K)$, the commutant $C(M)$ of M is equal to M, and the normalizer of $M^\times$ in $GL_2(K)$ is $M^\times$ itself.*

Proof. Since M is not semi-simple, it has a nilradical N made of α with $\alpha^n = 0$ for $n > 1$. Thus $\det(X - \alpha) = X^2$ and therefore $\alpha^2 = 0$. Then if $\alpha \neq 0$, with respect to a basis u, v of K^2 with $\alpha v = 0$, we find $\alpha = \left(\begin{smallmatrix} 0 & t \\ 0 & 0 \end{smallmatrix}\right)$ with $t \neq 0$. Then by an explicit computation, the centralizer C is of the form

$$C = \left\{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) | a, b \in K\right\}.$$

Then $C \supset M$, and maximality of M tells us $M = C$. Then by computation again, we see $C(M) = M$ and that $N(M^\times)$ is the algebra of upper triangular matrices. □

Lemma 3.9. *Let K be an infinite field of characteristic different from 2. Let $\mathfrak{L}$ be a nontrivial proper Lie subalgebra over K in $\mathfrak{sl}_2(K)$. Then $\mathfrak{L}$ is isomorphic to one of the following three Lie K-subalgebras:*

1. $\{x \in M | \mathrm{Tr}_{M/\mathbb{Q}}(x) = 0\}$ *as an abelian Lie subalgebra for a semi-simple quadratic extension M of K.*
2. $\mathfrak{U}_{/K} = \left\{\left(\begin{smallmatrix} 0 & x \\ 0 & 0 \end{smallmatrix}\right) \middle| x \in K\right\}$.
3. $\mathfrak{B}_{/K} = \left\{\left(\begin{smallmatrix} a & x \\ 0 & -a \end{smallmatrix}\right) \middle| a, x \in K\right\}$.

In particular, $\mathfrak{sl}_2(K)$ is the smallest simple Lie K-algebra containing non-trivial nilpotent elements.

A Lie algebra $\mathfrak{L}$ over a field k is *simple* if it contains no nontrivial normal k-subalgebras $\mathfrak{L}'$ (i.e., if $[\mathfrak{L},\mathfrak{L}'] \subset \mathfrak{L}'$, then $\mathfrak{L}' = \mathfrak{L}$ or $\mathfrak{L}' = 0$).

Proof. We may suppose $0 \neq \mathfrak{L} \subsetneq \mathfrak{sl}_2(K)$. Thus $1 \leq \dim_K \mathfrak{L} \leq 2$. First suppose that $\mathfrak{L}$ contains a nontrivial nilpotent element N. Then we have $\mathfrak{L} \supset \mathfrak{n} = K \cdot N$. Since the characteristic polynomial $\det(X - N)$ of N is X^2, choosing a basis of K well, we may assume that $\mathfrak{n} = \left\{ \left(\begin{smallmatrix} 0 & x \\ 0 & 0 \end{smallmatrix}\right) \middle| x \in K \right\}$. Note that the normalizer of $\mathfrak{n}$ is equal to $\mathfrak{B} = \left\{ \left(\begin{smallmatrix} a & x \\ 0 & -a \end{smallmatrix}\right) \middle| a, x \in K \right\}$. If $\mathfrak{L} \supset \mathfrak{n}$ contains an element not in $\mathfrak{n}$ normalizing $\mathfrak{n}$, since $\mathfrak{B}$ has dimension 2 over K, we must have $\mathfrak{L} = \mathfrak{B}$. If $\mathfrak{L}$ contains a semi-simple element s outside $\mathfrak{B}$, then s has two distinct eigenvalues as $\mathrm{Tr}(s) = 0$ (and characteristic $\neq 2$). Multiplying by a scalar in K, we may assume that s has infinite order in the group $GL_2(K)$. Thus the centralizer of s in $M_2(K)$ is a semi-simple quadratic extension M over K. Then $\mathcal{T}_M := M \cap \mathfrak{sl}_2(K) = \{x \in M | \mathrm{Tr}_{M/K}(x) = 0\}$, which is one-dimensional over K; so, $\mathcal{T}_M = Ks \subset \mathfrak{L}$. Since M and $\mathfrak{n}$ do not commute (and do not normalize each other by Lemmas 3.7 and 3.8), we find $[s,\mathfrak{n}] \cap (\mathcal{T}_M + \mathfrak{n}) = \{0\}$; so, $\mathfrak{L} = [s,\mathfrak{n}] \oplus \mathcal{T}_M \oplus \mathfrak{n} = \mathfrak{sl}_2(K)$, which is impossible by our assumption that $1 \leq \dim_K \mathfrak{L} \leq 2$.

Now assume that $\mathfrak{L}$ is made up of semi-simple elements and 0, pick one nonzero $s \in \mathfrak{L}$, we have $\mathcal{T}_M \subset \mathfrak{L}$ for the centralizer M of s in $M_2(K)$. If $\mathfrak{L} \neq \mathcal{T}_M$, we have another semi-simple quadratic extension M' and $\mathcal{T}_{M'} \subset \mathfrak{L}$. Since the K-subalgebra of $M_2(K)$ generated by M and M' is $M_2(K)$, the subalgebras M and M' do not commute. Consider the adjoint representation $Ad : \mathfrak{L} \to \mathrm{End}_K(\mathfrak{L})$ given by $Ad(x)(y) = [x,y]$. This is a representation of Lie algebras by Jacobi's identity. The action of $\mathcal{T}_M$ under $Ad(x)$ is semi-simple (as $\mathcal{T}_M$ is semi-simple); so, $Ad(x)$ for generic $x \in \mathcal{T}_M$ has three distinct eigenvalues $a, 0, -a$ on $\mathfrak{sl}_2$ in an algebraic closure of K. Write V_b for the eigenspaces with eigenvalue b. The existence of $\mathcal{T}_{M'}$ in $\mathfrak{L}$ tells us $W := (V_a + V_{-a}) \cap \mathfrak{L}$ is non-zero. If a is in K, V_a is in $\mathfrak{L}$ and one verifies that V_a is a nilpotent Lie subalgebra, against semi-simplicity of $\mathfrak{L}$. If a is not K, as a is quadratic over K, W has to be two-dimensional. Since $V_0 = \mathcal{T}_M$ has dimension 1, we find $\dim \mathfrak{L} = 3$, a contradiction. □

Lemma 3.10. *Let K be a field of characteristic $\neq 2$ and L/K be a field extension. If $0 \neq \mathfrak{L} \subset \mathfrak{sl}_2(L)$ is a vector K-subspace stable under the adjoint action of $SL_2(K)$, then there exists $g \in GL_2(L)$ such that $g\mathfrak{L}g^{-1} \supset \mathfrak{sl}_2(K)$.*

Proof. Put $\mathfrak{n}(X) = \left\{ \left(\begin{smallmatrix} 0 & x \\ 0 & 0 \end{smallmatrix}\right) \in \mathfrak{sl}_2(X) \middle| x \in X \right\}$ for any intermediate extension $L/X/K$. Since adjoint action: $Y \mapsto gYg^{-1}$ ($Y \in \mathfrak{sl}_2(L)$) of $g \in SL_2(K)$ is absolutely irreducible (see the exercise at the end of this subsection), we find that $\mathfrak{L}$ spans $\mathfrak{sl}_2(L)$ over L. In particular, $\mathfrak{L} \cap \mathfrak{n}(L) \neq 0$. Let T be the diagonal torus in GL_2; so, $T(X) = \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \in GL_2(X) \middle| a, b \in K^\times \right\}$. Note that $T(X)$ acts transitively on $\mathfrak{n}(X) \setminus \{0\}$. Thus conjugating $\mathfrak{L}$ by an element of $T(L)$, we may assume that $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \in \mathfrak{L}$. Since the adjoint action of $SL_2(K)$ on $\mathfrak{sl}_2(K)$ is absolutely irreducible, $\mathfrak{L} \cap \mathfrak{sl}_2(K) \neq \{0\}$ implies $\mathfrak{L} \supset \mathfrak{sl}_2(K)$, as desired. □

Taking a basis w_1, w_2 of a semi-simple quadratic extension $M/\mathbb{Q}_p$, we can embed M into $M_2(\mathbb{Q}_p)$ by sending $\alpha \in M$ to a matrix $\rho(\alpha) \in M_2(\mathbb{Q}_p)$ given by $(\alpha w_1, \alpha w_2) = (w_1, w_2)\rho(\alpha)$. Then we write $\mathcal{T}_M$ for $\mathcal{T}_{\mathrm{Im}(\rho)}$. If we start a semi-simple element $0 \neq s \in M_2(\mathbb{Q}_p)$, the centralizer of s in $M_2(\mathbb{Q}_p)$ is just $\mathbb{Q}_p + \mathbb{Q}_p s$, and taking $(w_1, w_2) = (1, s)$, we have $\mathcal{T}_M = \mathcal{T}_{\mathrm{Im}(\rho)}$. Since $\mathrm{Aut}(M/\mathbb{Q}_p)$ has order 2, for its generator σ, if we define

$\tau \in M_2(\mathbb{Q}_p)$ by $(\sigma(w_1), \sigma(w_2)) = (w_1, w_2)\tau$, τ normalizes $\mathcal{T}_M$, and as seen in Lemma 3.7, the normalizer $\mathcal{N}_M$ of $\mathcal{T}_M$ is generated by τ and $\mathcal{T}_M$; so, $\mathcal{N}_M/\mathcal{T}_M \cong \mathrm{Aut}(M/\mathbb{Q}_p)$.

Corollary 3.11. *Suppose $p > 2$. If G is a closed subgroup of $SL_2(\mathbb{Z}_p)$ of infinite order, then G has one of the following four forms*

1. *G is an open subgroup of $SL_2(\mathbb{Z}_p)$;*
2. *G is an open subgroup of $\mathcal{N}_M$ for a semi-simple quadratic extension $M_{/\mathbb{Q}_p} \subset M_2(\mathbb{Q}_p)$;*
3. *G is isomorphic to an open subgroup of the upper triangular Borel subgroup $\mathcal{B}(\mathbb{Z}_p) \subset SL_2(\mathbb{Z}_p)$;*
4. *G is isomorphic to an open subgroup of the upper triangular unipotent subgroup $\mathcal{U}(\mathbb{Z}_p) \subset SL_2(\mathbb{Z}_p)$.*

Proof. Since $G \cap \Gamma_{\mathbb{Z}_p}(p)$ is normal of finite index in G, replacing G by $G \cap \Gamma_{\mathbb{Z}_p}(p)$, we may assume that G is p-profinite. Write $\mathcal{M}_1(G) = C \oplus \mathcal{M}_1^0(G)$ for the Lie subalgebra L of $\mathfrak{sl}_2(\mathbb{Z}_p)$ associated to G as in Theorem 3.3. Then, by Lemma 3.9, $\mathfrak{L} := \mathcal{M}_1^0(G) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is either $\mathfrak{sl}_2(\mathbb{Q}_p)$ or a Cartan subalgebra (the case (1) of Lemma 3.9) or a nilpotent subalgebra (the case (2) of Lemma 3.9) or a Borel subalgebra (the case (3) of Lemma 3.9). Since $\mathcal{M}_1^0(G)$ determines G up to abelian error by Theorem 3.3, this classification corresponds to the classification in the corollary. □

Lemma 3.12. *Suppose $p > 2$ and A be an integral domain finite flat over $\mathbb{F}_p[[T]]$. If a closed subgroup G of $SL_2(A)$ contains*

$$\overline{\mathcal{T}} := \left\{ \begin{pmatrix} (1+T)^s & 0 \\ 0 & (1+T)^{-s} \end{pmatrix} \middle| s \in \mathbb{Z}_p \right\}$$

and non-trivial upper unipotent and lower unipotent subgroups, then, up to conjugation, G contains an open subgroup of $SL_2(\mathbb{F}_p[[T]])$, and if G is p-profinite, $\mathcal{M}(G)$ contains an open submodule of $M_2(\mathbb{F}_p[[T]])$.

Proof. Replacing G by $G \cap \Gamma_A(\mathfrak{m}_A)$, we may assume that G is p-profinite. Writing $K = \mathbb{F}_p((T))$ and $L = A \otimes_{\mathbb{F}_p[[T]]} K$, L is a finite field extension of K. Consider the X-span $\mathfrak{L}_X$ of $\mathcal{M}_1^0(G)$ for $X = K, L$. Then $\dim_L \mathfrak{L}_L = 3$; so, $\mathfrak{L}_L = \mathfrak{sl}_2(L)$. Thus up to conjugation, $\mathfrak{L}_K$ contains $\mathfrak{sl}_2(K)$ (cf. Lemma 3.9) by the existence of non-trivial unipotent elements. Thus we may assume that $A = \mathbb{F}_p[[T]]$. By adjoint action of $\overline{\mathcal{T}}$, the unipotent groups $U = \mathcal{U}(\mathbb{F}_p[[T]]) \cap G$ and $U_t = {}^t\mathcal{U}(\mathbb{F}_p[[T]]) \cap G$ are non-zero $\mathbb{F}_p[[T]]$-modules; so, $[\mathcal{U}(\mathbb{F}_p[[T]]) : U] < \infty$ and $[{}^t\mathcal{U}(\mathbb{F}_p[[T]]) : U_t] < \infty$. Let $\mathfrak{u}$ (resp. $\mathfrak{u}_t$) be the Lie algebra of U (resp. U_t). Thus we find that $[\mathfrak{u}, \mathfrak{u}_t] \neq 0$ is also an $\mathbb{F}_p[[T]]$-module in $\mathcal{M}^0(G)$, and hence $\mathcal{M}^0(G)$ has rank 3 over $\mathbb{F}_p[[T]]$. Also $C = \mathrm{Tr}(\mathcal{M}^0(G) \cdot \mathcal{M}^0(G))$ as in Theorem 3.3 contains $\mathfrak{u}\mathfrak{u}_t$ regarding $\mathfrak{u}$ and $\mathfrak{u}_t$ as an ideal of $\mathbb{F}_p[[T]]$ by an obvious isomorphism $\mathfrak{U}(\mathbb{F}_p[[T]]) \cong {}^t\mathfrak{U}(\mathbb{F}_p[[T]]) \cong \mathbb{F}_p[[T]]$. Then G contains $\Gamma_{\mathbb{F}_p[[T]]}(\mathfrak{u}\mathfrak{u}_t)$ and hence is open in $SL_2(\mathbb{F}_p[[T]])$. Then plainly, $\mathcal{M}(G)$ is open in $M_2(\mathbb{F}_p[[T]])$. □

Exercise

1. Let K be a field. Prove that the adjoint action of $SL_2(K)$ on $\mathfrak{sl}_2(K)$ is absolutely irreducible if and only if the characteristic of K is different from 2.