Rings and groups.

Ya. Sysak

1 Noetherian rings

Let R be a ring. A (right) R-module M is called *noetherian* if it satisfies the maximum condition for its submodules. In other words, if

$$M_1 \subseteq \ldots \subseteq M_i \subseteq M_{i+1} \subseteq \ldots$$

is an ascending chain of submodules of M, then there exists a positive integer n such that $M_n = M_{n+i}$ for every $i \geq 1$. Obviously the submodules and the factor modules of a noetherian R-module are also noetherian.

Lemma 1.1. *An R-module M is noetherian if and only if every submodule of M is finitely generated.*

Proof. Let N be a submodule of M which is not finitely generated. Then, for each $n \geq 1$ and elements $a_1, \ldots, a_n \in N$, there exists an element $a_{n+1} \in N$ which is not contained in the submodule N_n of M generated by the elements $a_1, \ldots, a_n$. Therefore the chain $N_1 \subset \ldots \subset N_n \subset N_{n+1} \subset \ldots$ is infinite and $N_n \neq N_{n+1}$ for each $n \geq 1$, so that M is not noetherian.

Conversely, if there exists such an infinite chain $N_1 \subset \ldots \subset N_n \subset N_{n+1} \subset \ldots$ of submodules of M, then their union $N = \cup_{n=1}^{\infty} N_n$ is a submodule of M which is not finitely generated because otherwise $N = N_n$ for some $n \geq 1$. $\square$

A ring R is called *right noetherian* if it is noetherian as a right R-module. Clearly if R is right noetherian, then the ring $R_{\mathfrak{u}}$ obtained by adjoining a formal unity 1 to R when R has no unity is also right noetherian.

A right ideal P of R is said to be *finitely generated* if it is finitely generated as a right R-module, i.e. if there exist finitely many elements $r_1, \ldots, r_n \in P$ such that $P = r_1 R_{\mathfrak{u}} + \ldots + r_n R_{\mathfrak{u}}$.

Theorem 1.2. (Hilbert Basis Theorem) *Let R be a right noetherian ring. Then the polynomial ring $R[x]$ is also right noetherian.*

Proof. Let P be a right ideal of $R[x]$ and, for each $n \geq 1$, let

$$P_n = \{r \in R \mid rx^n + r_1 x^{n-1} + \ldots + r_n \in P \quad \text{for some} \quad r_1, \ldots, r_n \in R\}.$$

Then P_n is a right ideal of R and $P_n \subseteq P_{n+1}$ for every $n \geq 1$.

Indeed, if $r, s \in P_n$, then either $r - s = 0 \in P_n$ or $(r-s)x^n + (r_1 - s_1)x^{n-1} + \ldots + (r_n - s_n) \in P$ and so $r - s \in P_n$. Similarly, if $t \in R$, then $rt \in P_n$. Next, $r \in P_{n+1}$ because $rx^{n+1} + r_1x^n + \ldots + r_nx \in P$.

Each right ideal P_n is generated by finitely many elements, say $r_{1n}, \ldots, r_{k_n n}$. Furthermore, there exists $m \geq 1$ such that $P_m = P_{m+1} = \ldots$. For each $1 \leq i \leq k_n$ and each $1 \leq n \leq m$, take some polynomial $f_{in}(x) = r_{in}x^n + \ldots \in P$ and denote by Q the right ideal of $R[x]$ generated by all $f_{in}(x)$. Show that $P = Q$.

Assume the contrary and let $f(x) = sx^l + \ldots$ be a polynomial of the least degree l in P such that $f(x) \notin Q$. Put $j = l$ if $l \leq m$ and $j = m$ otherwise. Since $s \in P_l = P_j$, we have $s = \sum_{i=1}^{k_j} r_{ij}t_{ij}$ for some $t_{ij} \in R_{\mathfrak{u}}$ and so

$$f(x) - \sum_{i=1}^{k_j} f_{ij}(x)t_{ij} \notin Q$$

is a polynomial of degree at most $l - 1$, contrary to the choice of $f(x)$. Thus $P = Q$ and so the theorem follows from Lemma 1.1. □

The following statement is an immediate consequence of the Hilbert Basis Theorem.

Corollary 1.3. *The polynomial ring $R[x_1, \ldots, x_n]$ in n commutative indeterminates is right noetherian if R is.*

Corollary 1.4. *If C is a noetherian commutative ring with 1, then every finitely generated commutative algebra over C is noetherian.*

Proof. If R such an algebra over C generated by n elements, then R is a homomorphic image of the polynomial ring $C[x_1, \ldots, x_n]$ and so R is noetherian by Corollary 1.3. □

Corollary 1.5. *Let R be a right noetherian ring. Then every finitely generated right R-module is noetherian.*

Proof. Indeed, every finitely generated right R-module is a factor module of a free right R-module on finitely many generators which is isomorphic to a direct sum of finitely many copies of the noetherian right R-module $R_{\mathfrak{u}}$ and so itself is noetherian. □

2 Commutative rings

Throughout this section R is a ring with 1.

2.1 Prime radical

Recall that an ideal I of a commutative ring R is called *prime* if the factor ring is a domain, i.e. $rs \in I$ for some $r, s \in R$ only if $r \in I$ or $s \in I$.

Lemma 2.1. *If R is a commutative ring and the element $r \in R$ is not nilpotent, then there exists a prime ideal P of R such that $r \notin P$.*

Proof. Let P be an ideal of R which is maximal with respect to the condition $P \cap \{r^n \mid n \geq 1\} = \emptyset$. Show that P is prime.

Indeed, let $ab \in P$ for some elements $a, b \in R \setminus P$. Then P is properly contained in $aR + P$ and $bR + P$, so that $r^l \in aR + P$ and $r^m \in bR + P$ for some positive integers l, m. But then $r^{l+m} \in (aR + P)(bR + P) \subseteq P$, contrary to the choice of P. □

If R is a ring, then the intersection of all prime ideals of R is called the *prime radical* of R.

Theorem 2.2. *Let R be a commutative ring. Then the set of all nilpotent elements of R coincides with the prime radical of R.*

Proof. Clearly every nilpotent element of R is contained in each prime ideal of R and so in the prime radical P of R. Conversely, if $r \in P$ and r is not nilpotent, then there exists a prime ideal I of R such that $r \notin I$. But then P is not contained in I, contrary to its definition. □

2.2 Integral dependence

Let R be a commutative ring and S a subring of R. An element $r \in R$ is called *integral* over S if there exit a positive integer n and elements $s_1, \ldots, s_n$ of S such that $r^n + s_1 r^{n-1} + \ldots + s_n = 0$. Obviously every element of S and nilpotent elements of R are integral over S. The ring R is *integral* over S if so is every element of R. It is a simple exercise to show that the property of R to be integral over S is inherited by factor rings and by rings of quotients.

Lemma 2.3. *Let R be a commutative ring, S its subring and $r \in R$. Then the following statements are equivalent:*

1) the element r is integral over S, and

2) the subring $S[r]$ is finitely generated as an S-module.

Proof. Let r be integral over S. Then there exists a positive integer n and a polynomial $f(x) \in S[x]$ of degree n such that $r^{n+1} = f(r)$. Therefore $S[r] = S + Sr + \ldots + Sr^n$, as desired.

Conversely, if $S[r]$ is finitely generated, then there exists elements $r_1, \ldots, r_n \in S[r]$ such that $S[r] = Sr_1 + \ldots + Sr_n$. Clearly, for each i with $1 \leq i \leq n$, there exists a polynomial $f_i(x) \in S[x]$ such that $r_i = f_i(r)$. Let m be the greatest among degrees of the polynomials $f_i(x)$. Then $r^{m+1} = s_1 r_1 + \ldots + s_n r_n = \sum_{i=1}^{n} s_i f_i(r)$ for some elements $s_1, \ldots, s_n \in S$ and hence $r^{m+1} = f(r)$ with $f(x) = \sum_{i=1}^{n} s_i f_i(x)$, so that r is integral over S. □

Lemma 2.4. *Let R be a commutative ring and S its subring. If R is a finitely generated S-module, then R is integral over S.*

Proof. Let $R = Sr_1 + \ldots + Sr_n$ for some elements $r_1, \ldots, r_n \in R$ and $r \in R$. Then $r = s_1r_1 + \ldots + s_nr_n$ for some elements $s_1, \ldots, s_n \in S$. Furthermore, for any $1 \leq i \leq j \leq n$, there exist elements $t_{ij1}, \ldots, t_{ijn} \in S$ such that $r_ir_j = t_{ij1}r_1 + \ldots + t_{ijn}r_n$. Denote by T the subring of S generated by the set $\{s_k, s_{ijl} \mid 1 \leq k, l \leq n, 1 \leq i \leq j \leq n\}$. Then the subring T is noetherian and so $T[r] \subseteq Tr_1 + \ldots + Tr_n$ is a finitely generated T-module by Corollary 1.5. Therefore the element r is integral over T and so over S by Lemma 2.3. □

Lemma 2.5. *Let R be a commutative ring and S, T its subrings. If R is integral over T and T is integral over S, then R is integral over S.*

Proof. If $r \in R$, then there exists elements $t_0, \ldots, t_n \in T$ such that $r^{n+1} = t_0 + t_1r + \ldots + t_nr^n$. Since each element t_i is integral over S, the subring $P = S[t_0, \ldots, t_n]$ is finitely generated as an S-module by Lemma 2.3. It is also clear that $P[r] = P + Pr + \ldots + Pr^n$. Therefore the subring $S[t_0, \ldots, t_n, r]$ is also finitely generated as an S-module and so r is integral over S by Lemma 2.4. □

Lemma 2.6. *Let R be a commutative ring and S its subring. If elements r, s are integral over S, then the elements $r + s$ and rs are also integral over S.*

Proof. Since s is integral over $S[r]$, the subring $S[r, s]$ is finitely generated as an $S[r]$-module and $S[r]$ is finitely generated as an S-module, so that $S[r, s]$ is a finitely generated S-module. Therefore the elements $r + s, rs \in S[r, s]$ are integral over S by Lemma 2.4. □

Thus the set of all elements of R integral over S is a subring $I(S)$ of R containing S by Lemma 2.6. This subring is called the *integral closure* of S in R. Clearly R is integral over S if $I(S) = R$. The subring S is said to be *integrally closed in* R if $I(S) = S$. A domain is called *integrally closed* if it is integrally closed in its quotient field. For example, the ring $\mathbb{Z}$ and the algebra $k[x_1, \ldots, x_n]$ of all polynomials in n commutative indeterminates over a field k are integrally closed. Moreover, if R is an integrally closed domain and T is a multiplicatively closed subset of R, then the ring of quotients $T^{-1}R$ is also integrally closed.

Lemma 2.7. *Let R be a commutative ring and S its subring. If R is integral over S, then $R^* \cap S = S^*$. In particular, if R is a field, then S is a subfield of R.*

Proof. Obviously $S^* \subseteq R^* \cap S$. Conversely, for each non-zero element $s \in R^* \cap S$, the element s^{-1} is integral over S and so $s^{-(n+1)} = s_0 + s_1s^{-1} + \ldots + s_ns^{-n}$ for some positive integer n and elements $s_0, \ldots, s_n \in S$. Therefore $s^{-1} = s_0s^n + s_1s^{n-1} + \ldots + s_n \in S$ and hence $s \in S^*$. □

2.3 The Hilbert Nullstellensatz (a weak version)

Theorem 2.8. *Let F be a field and $A = F[a_1, \ldots, a_n]$ a finitely generated algebra over F. If A is a field, then A is an algebraic extension of F.*

Proof. If $n = 1$, then $a_1^{-1} = f(a_1)$ for some polynomial $f(x) \in F[x]$ and so $a_1 f(a_1) - 1 = 0$. Therefore the element a_1 is algebraic over F and hence the field $A = F[a_1]$ is an algebraic extension of F.

Let $n > 1$, $a = a_n$ and let $E = F(a)$ be the field generated by a. Then $A = E[a_1, \ldots, a_{n-1}]$ and so A is algebraic over E by induction on n. If $E = F[a]$, then the element a is algebraic over F by proved above and so A is algebraic over F, as desired.

Assume that $E \neq F[a]$ and, for each $1 \leq i \leq n-1$, let $f_i(x) \in E[x]$ be the minimal polynomial for a_i over E. Clearly E is the field of quotients of the ring $F[a]$, so that $f_i(x) = b_i^{-1} g_i(x)$ for some non-zero element $b_i \in F[a]$ and $g_i(x) \in (F[a])[x]$. Put $b = b_1 \ldots b_{n-1}$. Then $b f_i(x) \in (F[a])[x]$ for every i. Since $F[a]b \subseteq F[a]$, it follows that $F[a] \subseteq F[a]b^{-1}$ and thus the union $B = \cup_{l=0}^{\infty} F[a]b^{-l}$ is a subring of A such that $f_i(x) \in B[x]$ for every i. Therefore the elements $a_1, \ldots, a_{n-1}$ are integral over B and hence A coincides with the integral closure of B by Lemma 2.6. Thus B is in fact a subfield of A by Lemma 2.7. Show that b is contained in the Jacobson radical J of $F[a]$.

Indeed, otherwise there exists a maximal ideal P of $F[a]$ such that $b \notin P$. It is easily seen that the union $\cup_{i=0}^{\infty} P b^{-i}$ is an ideal of B, so that either $P = 0$ or $B = \cup_{i=0}^{\infty} P b^{-i}$. Since in the second case $b \in P b^{-i}$ for some $i \geq 1$, this implies $b^{i+1} \in P$ and so $b \in P$, contrary to the choice of P. Therefore $P = 0$ which means that $F[a]$ is a field and hence $E = F[a]$, contrary to our assumption.

Thus $b \in J$ and so $(1 + b)^{-1} \in F[a]$. Therefore there exist two non-zero polynomials $f(x), g(x) \in F[x]$ such that $b = f(a)$ and $(1 + b)^{-1} = g(a)$. But then $(1 + f(a))g(a) = 0$ and hence the element a must be algebraic over F. This means that $F[a]$ is a field and so $E = F[a]$, a final contradiction. □

Corollary 2.9. *If F is a field which is finitely generated as a ring, then F is finite.*

Proof. Let F, regarded as a ring, be generated by elements $a_1, \ldots, a_n$ and let Q be the prime subfield of F. Then $F = Q[a_1, \ldots, a_n]$ is a finitely generated Q-algebra and so F is algebraic over Q by Theorem 2.8. Therefore F is finitely generated as a Q-module, i.e. there exist elements $b_1, \ldots, b_m$ such that $F = Qb_1 + \ldots + Qb_m$. Thus, if Q is finite, then F is finite, as desired.

Assume that Q is infinite, so that Q is the field of rational numbers. Then $a_i = \sum_{j=1}^{m} q_{ij} b_j$ and $b_i b_j = \sum_{k=1}^{m} p_{ijk} b_k$ for some rational numbers q_{ij}, p_{ijk}. Let P be the subring of Q generated by $\{q_{ij}, p_{ijk} \mid 1 \leq i \leq n, 1 \leq j, k \leq m\}$. It is easy to see that $F = Pb_1 + \ldots + Pb_m$. Since P is a noetherian ring by Corollary 1.4, the field F, regarded as a P-module, is noetherian by Corollary 1.5 and so every P-submodule of F is finitely generated. In particular, Q

must have this property. But then Q is finitely generated as a ring which is clearly not the case. This contradiction completes the proof. □

Corollary 2.10. *If R is a finitely generated commutative ring, then every simple R-module is finite.*

Proof. If M is a simple R-module and m a non-zero element of M, then the annihilator $\mathrm{Ann}_R(m)$ is a maximal ideal of R. Since the factor ring $R/\mathrm{Ann}_R(m)$ is a field which is finitely generated as a ring, it is finite by Corollary 2.9 and so the module $M = mR$ is also finite. □

Corollary 2.11. *Let R be a commutative ring which is finitely generated either as a ring or as an algebra over a field F. Then the Jacobson radical of R is nilpotent.*

Proof. Show first that the Jacobson radical J of R is contained in the prime radical of R and so it is a nil ideal of R.

Suppose the contrary and let $a \in J$ be a non-nilpotent element. Then there exists a prime ideal P of R such that $a \notin P$ by Lemma 2.1. Passing to the factor ring R/P, we may assume that R is a domain. Let Q be the field of quotients of R and $S = R[a^{-1}]$. If I is a maximal ideal of S, then $a \notin I$ and the factor ring S/I is a field. Moreover, S/I is finitely generated either as a ring or as an algebra over F. Hence, in the first case S/I is a finite by Corollary 2.9 and in the second case S/I is an algebraic extension of F by Theorem 2.8. Therefore the subring $(R+I)/I$ of S/I has the same property and so its element $a+I$ is invertible in $(R+I)/I$ by Lemma 2.7. On the other hand, $a+I$ is contained in $(J+I)/I$ and so in the Jacobson radical of $(R+I)/I$, which is impossible.

Thus J is a nil ideal of R. Since R is a noetherian ring by Corollary 1.4, the ideal J is finitely generated and hence there exist elements $a_1, \ldots, a_m \in J$ such that $J = a_1R + \ldots + a_mR$. As $(a_iR)^n = a_i^nR = 0$ for some positive integer n and each $1 \leq i \leq m$, every ideal a_iR is nilpotent and so J is. □

2.4 The Hilbert Nullstellensatz (a strong version)

Lemma 2.12. *Let K be an algebraic extension of a field F and C an algebraically closed field. Then each embedding $\epsilon : F \to C$ can be extended to an embedding $\bar{\epsilon} : K \to C$ such that $a^{\bar{\epsilon}} = a^{\epsilon}$ for every $a \in F$.*

Proof. It is enough to consider the case when $K = F(a)$ for some element $a \in K$. The general case can be derived from this by Zorn's lemma.

Let $f(x)$ be the minimal polynomial of a over F and I the ideal of the polynomial algebra $F[x]$ generated by $f(x)$. Then K is isomorphic to the factor ring $F[x]/I$. Clearly the embedding $\epsilon : F \to C$ can be extended to the embedding $F[x] \to C[x]$ and the polynomial $f^{\epsilon}(x)$ is irreducible over F^{ϵ}. Let c be a root of $f^{\epsilon}(x)$ in C. Then the mapping $x \mapsto c$ determines a homomorphism from $F[x]$ into C whose kernel coincides with I. Indeed, for $g(x) \in F[x]$, the equality $g^{\epsilon}(c) = 0$ holds if and only if $f^{\epsilon}(x)$ is a divisor

of $g^\epsilon(x)$, so that $g(x) \in I$. Therefore $F[x]/I$ is embedded in C and so the composition $K \to F[x]/I \to C$ is an embedding $\bar{\epsilon}$ from K into C. □

Lemma 2.13. *Let F be a field and A a finitely generated commutative algebra over F whose prime radical is zero. If $a \in A$ and $\bar{F}$ is the algebraic close of F, then there exists a homomorphism $\varphi : A \to \bar{F}$ such that $a^\varphi \neq 0$.*

Proof. If P is a prime ideal of A such that $a \notin P$, then the passage to the factor algebra A/P allows us to assume that A is a domain. Let Q be the field of quotients of A and $B = A[a^{-1}]$ the subalgebra of Q and I a maximal ideal of B. Then $a \notin I$ and the factor algebra B/I is algebraic over F by Theorem 2.8. Therefore there exists an embedding $B/I \to \bar{F}$ by Lemma 2.12 and hence the composition of the above homomorphisms

$$A \to A/P \to B \to B/I \to \bar{F}$$

is a homomorphism $\varphi : A \to \bar{F}$ such that $a^\varphi \neq 0$. □

If R is a commutative ring and I is an ideal of R, then the full preimage of the prime radical of the factor ring R/I is called the *root* of I in R and denoted by $\sqrt{I}$. By Theorem 2.2,

$$\sqrt{I} = \{r \in R \mid r^n \in I \quad \text{for some positive integer} \quad n\}.$$

The ideal I is said to be a *root ideal* in R if $\sqrt{I} = I$. It is easy to see that $\sqrt{I}$ is a root ideal in R for every ideal I of R.

Let F be a field, n a positive integer and F^n the space of all n-tuple over F. For a set I of polynomials of the polynomial algebra $F[x_1, \ldots, x_n]$ in n commutative indeterminates, we denote by $\mathcal{N}(I)$ the set of all common roots in F^n of all polynomials of I, i.e.

$$\mathcal{N}(I) = \{(a_1, \ldots, a_n) \in F^n \mid f(a_1, \ldots, a_n) = 0 \quad \text{for every} \quad f(x_1, \ldots, x_n) \in I\}.$$

Conversely, if S is a subset of F^n, then $\mathcal{P}(S)$ denotes the set of all polynomials of $F[x_1, \ldots, x_n]$ each of which vanishes every n-tuple of S, i.e.

$$\mathcal{P}(S) = \{f(x_1, \ldots, x_n) \mid f(a_1, \ldots, a_n) = 0 \quad \text{for every} \quad (a_1, \ldots, a_n) \in S\}.$$

It is easy to see that $\mathcal{P}(S)$ is an ideal of the polynomial ring $F[x_1, \ldots, x_n]$.

Theorem 2.14. (Hilbert Nullstellensatz) *Let F be an algebraic closed field and I an ideal of the polynomial ring $F[x_1, \ldots, x_n]$. Then*

$$\mathcal{P}(\mathcal{N}(I)) = \sqrt{I}.$$

In the other words, if I is a set of polynomials of $F[x_1, \ldots, x_n]$ and S is the set of all common roots in F^n of all polynomials of I, then for each polynomial $f \in F[x_1, \ldots, x_n]$ which vanishes every n-tuple of S there exist polynomials $f_1, \ldots, f_m \in I$ and $g_1, \ldots, g_n \in F[x_1, \ldots, x_n]$ and a positive integer k such that

$$f^k = f_1 g_1 + \ldots + f_m g_m$$

for some $m \geq 1$.

Proof. Clearly $\sqrt{I} \subseteq \mathcal{P}(\mathcal{N}(I))$. To prove the converse inclusion it suffices to look for each polynomial $f \in F[x_1, \ldots, x_n]$ which is not contained in $\sqrt{I}$ a vector $(a_1, \ldots, a_n) \in \mathcal{N}(I)$ such that $f(a_1, \ldots, a_n) \neq 0$.

Let $A = F[x_1, \ldots, x_n]/\sqrt{I}$ and $\bar{f} = f + \sqrt{I} \in A$. We show that every homomorphism $\varphi : A \to F$ such that $\bar{f}^{\varphi} \neq 0$ determines such an n-tuple. Indeed, if $\epsilon : F[x_1, \ldots, x_n] \to A$ is the natural homomorphism and $a_i = x_i^{\epsilon\varphi}$, then the n-tuple $(a_1, \ldots, a_n)$ has a desired property. In fact, $f(a_1, \ldots, a_n) = f(x_1^{\epsilon\varphi}, \ldots, x_n^{\epsilon\varphi}) = f(x_1, \ldots, x_n)^{\epsilon\varphi} = \bar{f}^{\varphi} \neq 0$. On the other hand, if $g \in I \subseteq \sqrt{I}$, then $g(a_1, \ldots, a_n) = g(x_1^{\epsilon\varphi}, \ldots, x_n^{\epsilon\varphi}) = g(x_1, \ldots, x_n)^{\epsilon\varphi} = \bar{g}^{\varphi} = 0$ because $\bar{g} = 0$.

Finally, since A is finitely generated algebra over F whose prime radical is zero, there exists a homomorphism $\varphi : A \to F$ such that $\bar{f}^{\varphi} \neq 0$ by Lemma 2.13. □

2.5 Algebraic sets

A subset S of F^n is called an *algebraic set* if there exists a subset I of $F[x_1, \ldots, x_n]$ such that $S = \mathcal{N}(I)$. It is easy to see that a subset $S \subseteq F^n$ is algebraic if and only if $S = \mathcal{N}(\mathcal{P}(S))$. Indeed, if $S = \mathcal{N}(I)$, then $S \subseteq \mathcal{N}(\mathcal{P}(S)) \subseteq \mathcal{N}(I) = S$ because $I \subseteq \mathcal{P}(S)$.

Examples.

1) The empty set $\emptyset$ and the set F^n are algebraic because $\emptyset = \mathcal{N}(F[x_1, \ldots, x_n])$ and $F^n = \mathcal{N}(0)$.

2) If S_i, $i \in \mathcal{I}$, is a collection of algebraic sets of F^n, then the intersection $S = \bigcap_{i \in \mathcal{I}} S_i$ is also an algebraic set in F^n.

   Indeed, for each $i \in \mathcal{I}$, let I_i be a subset of $F[x_1, \ldots, x_n]$ such that $S_i = \mathcal{N}(I_i)$. Then $S = \mathcal{N}(\bigcup_{i \in \mathcal{I}} I_i)$.

3) If S_i, $i \in \mathcal{I}$, is a finite collection of algebraic sets of F^n, then their union $T = \bigcup_{i \in \mathcal{I}} S_i$ is an algebraic set in F^n.

   Indeed, put $T = \mathcal{N}(\{\prod_{i \in \mathcal{I}} f_i \mid f_i \in I_i\})$. Obviously $T \subseteq \mathcal{N}(\{\prod_{i \in \mathcal{I}} f_i \mid f_i \in I_i\})$. Conversely, if $(a_1, \ldots, a_n)$ belongs to $\mathcal{N}(\{\prod_{i \in \mathcal{I}} f_i \mid f_i \in I_i\})$ and $(a_1, \ldots, a_n) \notin T$, then for each $i \in \mathcal{I}$ there exists a polynomial $f_i \in I_i$ such that $f_i(a_1, \ldots, a_n) \neq 0$. Therefore their product $\prod_{i \in \mathcal{I}} f_i$ does not vanish $(a_1, \ldots, a_n)$. On the other hand, the polynomial $\prod_{i \in \mathcal{I}} f_i$ belongs to the set $\{\prod_{i \in \mathcal{I}} f_i \mid f_i \in I_i\}$ and so it should vanish the element $(a_1, \ldots, a_n)$. This contradiction shows that $T = \mathcal{N}(\{\prod_{i \in \mathcal{I}} f_i \mid f_i \in I_i\})$.

4) Every element $(a_1, \ldots, a_n) \in F^n$, regarded as an one-element set, is an algebraic set because $\{(a_1, \ldots, a_n)\} = \mathcal{N}(\{x_1 - a_1, \ldots, x_n - a_n\})$.

Examples 1) - 3) show that the collection of all algebraic sets of F^n can be viewed as that of *closed subsets* of a topological space. The topology on F^n determined by this collection is called the *Zariski topology.*

Lemma 2.15. *Let F^n be viewed as a topological space with the Zariski topology.*

1) If the field F is infinite and M, N are non-empty open sets of F^n, then $M \cap N \neq \emptyset$. In particular, the Zariski topology is not separated.

2) The space F^n satisfies the minimum condition for the closed subsets and so the maximum condition for the open subsets.

Proof. 1) Assume that $M \cap N = \emptyset$. Then $F^n = (F^n \setminus M) \cup (F^n \setminus N)$ and both sets $F^n \setminus M$ and $F^n \setminus N$ are proper closed subsets of F^n, so that they are proper algebraic subsets of F^n. Therefore there exist non-zero subsets I_M and I_N of $F[x_1, \ldots, x_n$ such that $F^n \setminus M = \mathcal{N}(I_M)$ and $F^n \setminus N = \mathcal{N}(I_N)$. As it has been shown in Example 3), this implies that $F^n = \mathcal{N}(\{fg \mid f \in I_M, g \in I_N\})$ and so a non-zero polynomial $fg = h(x_1, \ldots, x_n)$ vanishes every element of F^n. In particular, if $a_2, \ldots, a_n$ are non-zero elements of F, then the polynomial $h(x_1, a_2, \ldots, a_n)$ in one indeterminate x_1 is non-zero and has infinitely many roots in F which is impossible. Thus $M \cap N \neq \emptyset$.

2) Let $S_1 \supseteq S_2 \supseteq \ldots \supseteq S_m \supseteq \ldots$ be a descending chain of closed subsets of F^n. For each $i \geq 1$, we put $I_i = \mathcal{P}(S_i)$. Then I_i is an ideal of $F[x_1, \ldots, x_n]$ such that $S_i = \mathcal{N}(I_i)$ and $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_m \subseteq \ldots$. By Corollary 1.3, there exists an integer $l \geq 1$ such that $I_l = I_{l+1} = \ldots$ and therefore $S_l = S_{l+1} = \ldots$. □

Note that for a finite field F the statement 1) of Lemma 2.15 does not hold because in this case the space F^n is finite and so every subset of F^n is open.

Clearly every set M contained in F^n becomes a topological space with a Zariski topology induced by the Zariski topology on F^n. This means in particular that, for each closed subset N of M, there exists a closed subset A of F^n such that $N = A \cap M$. A subset N of M is said to be *irreducible* if N is not a union of two proper closed subsets of N. Obviously M is irreducible if and only if the intersection of any two non-empty open subsets of M is non-empty. In other words, M is connected as a topological space with Zariski topology. In particular, the topological space F^n is irreducible for every infinite field F by Lemma 2.15.1).

Theorem 2.16. *Let S be a closed subset of F^n. If S is irreducible, then the ideal $I = \mathcal{P}(S)$ of $F[x_1, \ldots, x_n]$ is prime. Conversely, if the field F is infinite and I is prime, then S is irreducible.*

Proof. If S is irreducible and f, g are polynomials of $F[x_1, \ldots, x_n]$ such that $fg \in I$, then $S = (\mathcal{N}(f) \cap S) \cup (\mathcal{N}(g) \cap S)$, so that one of the closed subsets $\mathcal{N}(f) \cap S$ or $\mathcal{N}(g) \cap S$ coincides with S. Therefore f or g belongs to I and hence I is a prime ideal of $F[x_1, \ldots, x_n]$.

Conversely, let F be an infinite field and I a prime ideal of $F[x_1, \ldots, x_n]$. If $S = S_1 \cup S_2$ for some closed subsets S_1 and S_2 of F^n, then $I \subseteq \mathcal{P}(S_1) \cap \mathcal{P}(S_2)$. Assume that $\mathcal{P}(S_1) \neq I \neq \mathcal{P}(S_2)$ and put $f = gh$ for some polynomials $g \in \mathcal{P}(S_1) \setminus I$ and $h \in \mathcal{P}(S_2) \setminus I$. Since F is infinite, it follows that $f \in I$ and

hence either g or h must belong to I because I is prime. This contradiction shows that one of the ideals $\mathcal{P}(S_1)$ or $\mathcal{P}(S_2)$ coincides with I and thus S_1 or S_2 coincides with S, as desired. □

An irreducible subset N of M is said to be *maximal* in M if N is not a proper subset of an irreducible set of M.

Theorem 2.17. *Let $M \subseteq F^n$ be a topological space with a Zariski topology. Then M has finitely many maximal irreducible subsets M_1, ..., M_k. Moreover, $M = M_1 \cup \ldots \cup M_k$ and every subset M_i is closed in M.*

Proof. Note first that M satisfies the minimal condition for its closed subsets by Lemma 2.15. Show next that M is a union of finitely many closed and irreducible subsets of M.

Indeed, otherwise there exists a closed subset N of M which is minimal with respect to the condition that N cannot be represented as a union of finitely many closed irreducible subsets of M. In particular, N cannot be irreducible, so that $N = N_1 \cup N_2$ for two proper subsets N_1 and N_2 of N closed in M. Since both N_1 and N_2 are unions of finitely many closed irreducible subsets of M, so is N, contrary to its choice.

Thus, there exists a least positive integer k such that $M = M_1 \cup \ldots \cup M_k$ for some subsets $M_1, \ldots, M_k$ of M each of which is closed and irreducible. Clearly, for any $i \neq j$, the subset M_i is not contained in M_j. Let L be an irreducible subset of M which contains M_i. As $L = (L \cap M_1) \cup \ldots \cup (L \cap M_k)$, this means that $L = L \cap M_j$ for some j and so $M_i \subseteq L \subseteq M_j$. Therefore $i = j$ and hence the irreducible subset $M_i = L$ is maximal in M. □

Let K be an extension of a field F. A set of elements $a_1, \ldots, a_n$ of K are called *algebraically independent* over F if there exists no non-zero polynomial $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ such that $f(a_1, \ldots, a_n) = 0$. A subset A of K is algebraically independent over F if so is every finite subset of A. It follows from Zorn's lemma that K contains a maximal algebraically independent subset and any of such subsets is called a *transcendence basis* of K over F. It is well-known that every two transcendence bases have the same cardinal number which is called the *transcendence degree* of K over F and denoted by $\text{t.d.}(K/F)$.

Theorem 2.18. *Let R be a finitely generated commutative algebra over F. If P and Q are prime ideals of R such that $P \subsetneqq Q$, then the transcendence degree of the field of quotients of the factor algebra R/Q over F is strictly less than that of the factor algebra R/P over F. In particular, if R is generated by m elements for some positive integer m, then every chain of distinct prime ideals of R is of length at most m.*

Proof. Clearly without loss of generality we may suppose that $P = 0$, so that R is a domain. It is easily seen that there exists a transcendence basis of the field of quotients of the factor algebra R/Q over F which consists from elements of R/Q. Let $b_1, \ldots, b_k$ be such a basis and, for each i, let a_i be a preimage

of b_i in R. Take a non-zero element a_{k+1} of Q and show that the elements $a_1, \ldots, a_k, a_{k+1}$ are algebraically independent over F.

Assume the contrary and let $f(x_1, \ldots, x_{k+1})$ be a non-zero polynomial of $F[x_1, \ldots, x_{k+1}]$ of the least degree such that $f(a_1, \ldots, a_{k+1}) = 0$. Since $f(x_1, \ldots, x_{k+1}) = g(x_1, \ldots, x_k) + h(x_1, \ldots, x_{k+1})x_{k+1}$ for some polynomial $g(x_1, \ldots, x_k)$ and $h(x_1, \ldots, x_{k+1})$ over F, it follows that $g(a_1, \ldots, a_k) = -h(a_1, \ldots, a_{k+1})a_{k+1} \in Q$ and so $g(b_1, \ldots, b_k) = 0$ in R/Q. Therefore the polynomial $g(x_1, \ldots, x_k)$ is identically equal to zero and so $h(a_1, \ldots, a_{k+1})a_{k+1} = 0$. Hence $h(a_1, \ldots, a_{k+1}) = 0$ because R is a domain. However this contradicts to the choice of $f(x_1, \ldots, x_{k+1})$ because the degree of $h(x_1, \ldots, x_{k+1})$ is less than that of $f(x_1, \ldots, x_{k+1})$. □

Let M be an irreducible algebraic set in F^n and $I = \mathcal{P}(M)$. Then the ideal I of $F[x_1, \ldots, x_n]$ is prime by Theorem 2.16 and so the factor ring $R = F[x_1, \ldots, x_n]/I$ is a domain. Let K be the field of quotients of R. The transcendence degree of K over F is called the *dimension* of M over F and denoted by $\dim_F(M)$. The following statement is an immediate consequence of Theorem 2.18.

Corollary 2.19. *If $M \subsetneqq N$ are two distinct irreducible algebraic subsets of F^n, then $\dim_F(M) < \dim_F(N)$. In particular, every chain of distinct irreducible algebraic subsets of F^n is of length at most n.*

3 Algebraic groups

As above, throughout this section F denotes an infinite field and, for $n \geq 1$, the space F^n is viewed as an algebraic set or, equivalently, as a topological space with the Zariski topology. Recall that, for a subset S of F^n, the set of all polynomials of $F[x_1, \ldots, x_n]$ vanishing every element of S is an ideal of $F[x_1, \ldots, x_n]$ denoted by $\mathcal{P}(S)$. The factor algebra $F[x_1, \ldots, x_n]/\mathcal{P}(S)$ can be viewed as an *algebra of polynomial functions* on S and it will be denoted by $F[S]$. In fact, if $f \in F[S]$ and $a = (a_1, \ldots, a_n) \in S$, then $f = f(x_1, \ldots, x_n) + \mathcal{P}(S)$ for some polynomial $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ and the element $f(a) = f(a_1, \ldots, a_n) \in F$ depends only on f and not on the choice of $f(x_1, \ldots, x_n)$. Thus every element $f \in F[S]$ is in fact a polynomial function $f : S \to F$ defined on S and with values in F. Moreover, it is easy to see that if $a \neq b$ are two elements of S, then there exists a function $f \in F[S]$ with $f(a) \neq f(b)$.

For subsets $T \subseteq S$ and $I \subseteq F[S]$, we define the annihilator of T in $F[S]$ by

$$\mathrm{Ann}_{F[S]}(T) = \{f \in F[S] \mid f(b) = 0 \quad \text{for all} \quad b \in T\}$$

and the annihilator of I in S by

$$\mathrm{Ann}_S(I) = \{b \in S \mid f(b) = 0 \quad \text{for all} \quad f \in I\}.$$

Clearly $\mathrm{Ann}_{F[S]}(T) = \mathcal{P}(T)/\mathcal{P}(S)$, so that T is closed in S if and only if $T = \mathrm{Ann}_S(\mathrm{Ann}_{F[S]}(T))$.

3.1 Polynomial maps

If $A \subseteq F^m$ and $B \subseteq F^n$ are two algebraic sets, then a mapping $\phi : A \to B$ is called a *polynomial map* or a *morphism* of A into B if for every $g \in F[B]$ there exists $f \in F[A]$ such that $f(a) = g(a^\phi)$ for every $a \in A$. In other words, the diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & F \\ & {\scriptstyle\phi}\searrow \quad \nearrow {\scriptstyle g} & \\ & B & \end{array}$$

must be commutative. Clearly the mapping ϕ is polynomial, provided that there exist n polynomials $\phi_1(x_1, \ldots, x_m), \ldots, \phi_n(x_1, \ldots, x_m)$ of $F[x_1, \ldots, x_m]$ such that

$$a^\phi = (\phi_1(a_1, \ldots, a_m), \ldots, \phi_n(a_1, \ldots, a_m))$$

for every $a = (a_1, \ldots, a_m) \in A$.

Indeed, if $\phi_1, \ldots, \phi_n$ are corresponding polynomial functions of $F[A]$, then $g(\phi_1, \ldots, \phi_n)$ is also a polynomial function of $F[A]$ and $g(a^\phi) = g(\phi_1(a), \ldots, \phi_n(a))$ for every $a \in A$, so that we can take $f = g(\phi_1, \ldots, \phi_n)$.

We shall say that ϕ is an *isomorphism* from A onto B if ϕ is bijective and the converse mapping $\phi^{-1} : B \to A$ is also a polynomial map.

Every polynomial map $\phi : A \to B$ determines the mapping $\hat{\phi} : F[B] \to F[A]$ given by $g^{\hat{\phi}} = \phi \circ g$ for every $g \in F[B]$. It is easy to see that $\hat{\phi}$ is even an algebra homomorphism from $F[B]$ into $F[A]$ because $\phi \circ (f + g) = \phi \circ f + \phi \circ g$ and $\phi \circ (fg) = (\phi \circ f)(\phi \circ g)$ for every $f, g \in F[A]$. This homomorphism $\hat{\phi} : F[B] \to F[A]$ will be called the associated algebra homomorphism.

Examples. Let $m \geq n$ and let F^m, F^n be viewed as algebraic sets.

1) If $\iota : F^n \to F^m$ is the embedding of F^n into F^m given by

$$(a_1, \ldots, a_n)^\iota = (a_1, \ldots, a_n, 0, \ldots, 0) \in F^m$$

for $(a_1, \ldots, a_n) \in F^n$, then ι determines a projection $\hat{\iota}$ of $F[x_1, \ldots, x_m]$ onto $F[x_1, \ldots, x_n]$ with $f(x_1, \ldots, x_m)^{\hat{\iota}} = f(x_1, \ldots, x_n, 0, \ldots, 0)$, so that ι is a polynomial map.

2) If $\pi : F^m \to F^n$ is the projection of F^m onto F^n given by

$$(a_1, \ldots, a_m)^\pi = (a_1, \ldots, a_n) \in F^n$$

for every $(a_1, \ldots, a_m) \in F^m$, then π determines an identity embedding $\hat{\pi} : F[x_1, \ldots, x_n] \to F[x_1, \ldots, x_m]$ and so it is a polynomial map.

Recall that a mapping $\phi : A \to B$ of topological spaces A and B is called *continuous* if, for every closed subset T of B, the full preimage $S = \{a \in A \mid a^\phi \in T\}$ of T in A is a closed subset of A.

Lemma 3.1. *Let $A \subseteq F^m$ and $B \subseteq F^n$ be two algebraic sets and $\phi : A \to B$ a polynomial map. Then the following statements hold.*

1) As a mapping of topological spaces A and B with Zariski topology, ϕ is continuous. In particular, ϕ is a homeomorphism, provided that it is an isomorphism from A onto B.

2) If S is an irreducible subset of A, then its image S^ϕ is an irreducible subset of B.

Proof. 1) If T is a closed subset of B and $I = \mathrm{Ann}_{F[B]}(T)$, then the full preimage S of T in A coincides with $\mathrm{Ann}_A(I^{\hat{\phi}})$. Indeed, if $a \in S$ and $g \in I$, then $g^{\hat{\phi}}(a) = g(a^\phi) = 0$, so that $S \subseteq \mathrm{Ann}_A(I^{\hat{\phi}})$. Conversely, if $a \in A$ and $g^{\hat{\phi}}(a) = 0$, then $g(a^\phi) = 0$ and therefore $a^\phi \in T$, so that $\mathrm{Ann}_A(I^{\hat{\phi}}) \subseteq S$. Thus $S = \mathrm{Ann}_A(I^{\hat{\phi}})$ is a closed subset of A, as desired.

2) Assume that the subset S^ϕ is not irreducible. Then there exist two closed subsets U and V of B such that $S^\phi \subseteq U \cup V$ and neither U nor V contains S^ϕ. The full preimages $\phi^{-1}(U)$ and $\phi^{-1}(V)$ of U and V in A are closed subsets of A by 1) and obviously their union $\phi^{-1}(U) \cup \phi^{-1}(V)$ contains S. Since S is irreducible, this means that S is contained either in $\phi^{-1}(U)$ or in $\phi^{-1}(V)$. But then S^ϕ is contained either in U or in V, respectively, contrary to their choice. Thus S^ϕ must be irreducible. □

Consider now the cartesian product $A \times B$ of two non-empty algebraic sets $A \subseteq F^m$ and $B \in F^n$ as the subset $\{(a, b) \in F^{m+n} \mid a \in A, b \in B\}$. It is easy to see that $\mathcal{P}(A \times B) = \mathcal{P}(A)F[x_1, \ldots, x_{m+n}] + \mathcal{P}(B)F[x_1, \ldots, x_{m+n}]$. On the other hand, if elements $a = (a_1, \ldots, a_m)$ and $b = (b_{m+1}, \ldots, b_{m+n})$ satisfy the condition that the element $(a, b) \in F^{m+n}$ is vanished by every polynomial of $\mathcal{P}(A \times B)$, then $f(a_1, \ldots, a_m) = 0 = g(b_{m+1}, \ldots, b_{m+n})$ for every $f(x_1, \ldots, x_m) \in \mathcal{P}(A)$ and every $g(x_1, \ldots, x_n) \in \mathcal{P}(B)$, so that $a \in A$ and $b \in B$. Thus $A \times B = \mathcal{N}(\mathcal{P}(A \times B))$ and so $A \times B$ is an algebraic set which is called the *direct product* of the algebraic sets A and B.

Example. As an algebraic set, the direct product $F^n \times F^m$ is isomorphic to F^{m+n}.

Recall that, for two algebras R and S over F, regarded as vector spaces over F, the tensor product $R \otimes_F S$ becomes an algebra over F if its multiplication is determined by the rule $(r \otimes s)(t \otimes u) = rt \otimes su$ for every $r, s \in R$ and $t, u \in S$. This algebra is called the *tensor product of algebras* R and S and denoted by $R \otimes S$. It is easily verified that if A and B are algebraic sets, then the algebra $F[A \times B]$ of polynomials functions on $A \times B$ is isomorphic to the tensor product $F[A] \otimes F[B]$. In fact, the mapping $\tau : F[A] \otimes F[B] \to F[A \times B]$, given by

$$(\sum_i f_i \otimes g_i)^\tau(a, b) = \sum_i f_i(a) g_i(b)$$

for all $a \in A$ and $b \in B$ with $f_i \in F[A]$ and $g_i \in F[B]$, determines such an algebra isomorphism from $F[A] \otimes F[B]$ onto $F[A \times B]$.

Lemma 3.2. *If A and B are two irreducible algebraic sets, then so is its direct product $A \times B$.*

Proof. Assume that $A \subseteq F^m$ and $B \subseteq F^n$, so that $A \times B \subseteq F^{m+n}$. For brevity, let $F[X] = F[x_1, \ldots, x_m]$, $F[Y] = F[x_{m+1}, \ldots, x_{m+n}]$ and $F[X,Y] = F[x_1, \ldots, x_{m+n}]$. Furthermore, put also $P = \mathcal{P}(A)$, $Q = \mathcal{P}(B)$ and $I = \mathcal{P}(A \times B)$. By Theorem 2.16, P and Q are prime ideals of $F[X]$ and $F[Y]$, respectively, and $I = PF[X,Y] + QF[X,Y]$. We have to show that I is also a prime ideal of $F[X,Y]$, i.e. if $f, g \in F[X,Y]$ and $fg \in I$, then either $f \in I$ or $g \in I$.

Since $F[X,Y]$ can be viewed as the polynomial algebra over $F[X]$ in indeterminates Y, there exists a positive integer k such that the polynomials f and g can uniquely be written in the form $f = \sum_{i=0}^{k} f_i r_i$ and $g = \sum_{i=0}^{k} g_i s_i$ for some polynomials $f_i, g_j \in F[X]$ and some monomials $r_i, s_j \in F[Y]$ with $1 \leq i, j \leq k$. Furthermore, it is also clear that $I = PF[Y] + F[X]Q$, so that there exists a positive integer l such that the polynomial $fg \in I$ can be written in the form $fg = \sum_{i=0}^{l}(p_i t_i + u_i q_i)$ for some polynomials $p_i \in P$ and $q_i \in Q$ and some monomials $t_i, u_j \in F[Y]$ with $1 \leq i, j \leq l$ and this representation is uniquely modulo PQ. On the other hand, $fg = \sum_{i=0,j=0}^{k}(f_i g_j)(r_i s_j)$ and therefore each summand $(f_i g_j)(r_i s_j)$ modulo PQ coincides either with $p_h t_h$ or with $u_h q_h$ for some $1 \leq h \leq l$, so that either $f_i g_j = p_h \in P$ or $r_i s_j = q_h \in Q$.

Assume that both polynomials f and g are not contained in I. Then there exist indexes i and j such that $f_i r_i \notin I$ and $g_j s_j \notin I$. But then $f_i, g_j \notin P$ and $r_i, s_j \notin Q$, contrary to the above. Thus the ideal I is prime and so $A \times B$ is an irreducible algebraic set by Theorem 2.16. □

3.2 Affine algebraic groups

Let A be an algebraic subset of F^n whose elements form a group under a multiplicative operation $\mu : A \times A \to A$. If both mappings μ and $\nu : A \to A$, given by $a^\nu = a^{-1}$ for every $a \in A$, are polynomial maps of algebraic sets $A \times A$ and A into A, respectively, then A is called an *algebraic F-group*. As it follows from Lemma 3.1.1), every algebraic group is also a topological group with Zariski topology.

Examples. 1. Let $n = 1$ and F^+ be the additive group of F. Then F^+ is an algebraic F-group.

Indeed, since the mappings $\mu : F \times F \to F$ and $\nu : F \to F$ are given by $(a,b)^\mu = a + b$ and $a^\nu = -a$ for every $a, b \in F$, they are determined by the polynomials $\mu(x,y) = x + y \in F[x,y]$ and $\nu(x) = -x \in F[x]$, respectively, so that μ and ν are polynomial maps.

2. Let $n = 2$ and F^* be the multiplicative group of F. Then F^* is an algebraic F-group.

Indeed, identify F^* with the subset $A = \{(a,b) \in F^2 \mid ab = 1,\ a, b \in F\}$ of F^2. Then $A = \mathcal{N}(xy - 1)$ is an algebraic subset of F^2 and the mappings $\mu : A \times A \to A$ and $\nu : A \to A$ are given by $((a,b),(c,d))^\mu = (ac, bd)$ and $(a,b)^\nu = (b,a)$ for every $(a,b), (c,d) \in A$. Therefore μ and ν are determined by the polynomials $\mu_1(x,y,z,u) = xz$ and $\mu_2(x,y,z,u) = yu$ of $F[x,y,z,u]$

and by $\nu_1(x,y) = y$ and $\nu_2(x,y) = x$ of $F[x,y]$, respectively, so that μ and ν are polynomial maps.

3. The group $G = SL(n,F)$ of all $(n \times n)$-matrices over F whose determinant is equal to 1 is an algebraic F-group.

Indeed, each $(n \times n)$-matrix (a_{ij}) over F can be viewed as an element of the space F^{n^2}, so that G coincides with the set of all roots of the polynomial $\det(x_{ij}) - 1$ of the polynomial algebra $F[x_{ij} \mid 1 \le i,j \le n]$ and thus it is an algebraic set. Furthermore, the rules of multiplication of two matrices and taking the inverse matrix imply that the mappings $\mu : G \times G \to G$ and $\nu : G \to G$ are polynomial.

4. The group $G = GL(n,F)$ of all invertible $(n \times n)$-matrices over F is an algebraic F-group.

Indeed, identify G with the subset of all $(n+1 \times n+1)$-matrices of the form $\begin{pmatrix} A & 0 \\ 0 & \det A \end{pmatrix}$ where $A = (a_{ij})$ is an $(n \times n)$-matrix. Then G is the set of all roots of the polynomials $\{x_{n+1\,n+1}\det(x_{ij}) - 1,\ x_{i\,n+1},\ x_{n+1\,j} \mid 1 \le i,j \le n\}$ of the polynomial algebra $F[x_{ij} \mid 1 \le i,j \le n+1]$ and so it is an algebraic set. By the same reason as above, the mappings $\mu : G \times G \to G$ and $\nu : G \to G$ are polynomial.

If A is an algebraic group, then the subgroup B of A is algebraic if and only if it is a closed subset of A, regarded as a topological group with Zariski topology. This means that there exists a subset S of the algebra $F[A]$ of polynomial functions on A such that $B = \mathrm{Ann}_A(S)$. Every closed subgroup of the group $GL(n,F)$, regarded as an algebraic group, is called a *linear algebraic group*.

If A and B are two algebraic groups, then the direct product $A \times B$, regarded simultaneously as the direct product of the algebraic sets A and B, is an algebraic group whose algebra polynomial functions $F[A \times B]$ is isomorphic to $F[A] \otimes F[B]$. For instance, the space F^n, regarded as an additive algebraic group, is isomorphic to the direct sum $F \oplus \ldots \oplus F$ of n copies of the algebraic group F^+.

Lemma 3.3. *Let A be an algebraic group, B its non-empty closed subset and $a \in A$. Then the subsets aB, Ba and $a^{-1}Ba$ are closed in A.*

Proof. Clearly $\{a^{-1}\} \times A$ is a closed subset of $A \times A$. Let $\bar{\mu}$ be the restriction of the polynomial map $\mu : A \times A \to A$ on $\{a^{-1}\} \times A$. Then $\bar{\mu}$ is a continuous mapping from $\{a^{-1}\} \times A$ onto A by Lemma 3.1. It is easy to see that the full preimage of B under $\bar{\mu}$ coincides with the set $\{a^{-1}\} \times \{aB\}$. Therefore this set is closed in $\{a^{-1}\} \times A$. Since the embedding $A \to \{a^{-1}\} \times A$ given by $c \mapsto (a^{-1}, c)$ for every $c \in A$ is also continuous, the set aB is closed in A because it is the full preimage of $\{a^{-1}\} \times \{aB\}$. By symmetry, Ba and so $a^{-1}Ba$ are also closed subsets of A. □

For an algebraic group A, the maximal irreducible subsets of the algebraic set A are called *connected components* of A because they are maximal connected subsets of A, regarded as a topological space with Zariski topology. Every connected component of A is a closed subset in A by Theorem 2.17.

Theorem 3.4. *Let A be an affine algebraic group. Then A contains a connected closed normal subgroup A_0 of finite index in A and all connected components of A are precisely the cosets of A_0 in A. Moreover, A_0 is a unique connected closed subgroup of finite index in A.*

Proof. Since A is a union of its finitely many connected components by Theorem 2.17, there exists such a component A_0 which contains the neutral element 1 of A. If M is an arbitrary connected component of A containing 1, then the product A_0M is a connected subset of A.

Indeed, A_0 and M are connected algebraic sets, so that their direct product $A_0 \times M$ is also connected by Lemma 3.2. As A_0M is the image of $A_0 \times M$ under the polynomial map $\mu : A \times A \to A$, it is connected by Lemma 3.1.

Thus $A_0M = A_0 = M$ because $A_0 \subseteq A_0M$ and $M \subseteq A_0M$. Next, A_0^{-1}, regarded as the image of A_0 under the polynomial map $\nu : A \to A$, is a connected subset of A containing 1. Therefore $A_0^{-1} \subseteq A_0$ and hence A_0 is a closed subgroup of A. For each element $a \in A$, the coset A_0a is a connected subset of A because it is the image of the direct product of irreducible algebraic sets A_0 and $\{a\}$. If $A_0a \subseteq M$ for some connected component M of A, then $A_0 \subseteq Ma^{-1}$ and so $A_0 = Ma^{-1}$ because Ma^{-1} is connected. Hence every coset Aa is a connected component of A and thus there exists only finitely many such cosets. This means that A_0 is a subgroup of finite index in A.

Let B be a connected closed subgroup of finite index in A. Then $B \subseteq A_0$ and so A_0 is the disjoint union of finitely many cosets of B in A_0. Since A_0 is connected and every coset Ba is a closed in A by Lemma 3.3, we have $B = A_0$ and thus A_0 is the unique connected closed subgroup of finite index in A. In particular, $a^{-1}A_0a = A_0$ and so A_0 is normal in A. □

If A is an algebraic group, then its unique connected closed subgroup of finite index will always be denoted by A_0.

Corollary 3.5. *Let A be an algebraic group and B its closed subgroup. Then the following statements are equivalent.*

1) $A_0 \subseteq B$;

2) B is of finite index in A;

3) B is open.

Proof. Clearly statement 1) implies 2). If statement 2) holds, then A is the disjoint union of finitely many cosets of B in A. Since every coset aB of B in A is closed by Lemma 3.3, the union of all these cosets distinct from B is a closed subset C of A such that $A = B \cup C$ and $B \cap C = \emptyset$. Therefore B is open. Finally, if statement 3) holds, then the intersection $A_0 \cap B$ is a

non-empty open closed subgroup of A_0. As A_0 is a connected subgroup of A, this implies that $A_0 = A_0 \cap B$ and so $A_0 \subseteq B$. □

Lemma 3.6. *Let A be an algebraic group and $b \in A$. Then the mappings*

$$a \mapsto ba, \quad a \mapsto b^{-1}ab, \quad a \mapsto a^{-1}ba \quad \text{and} \quad a \mapsto [a,b] = a^{-1}b^{-1}ab$$

with $a \in A$ are polynomial maps from A into A. In particular, the conjugacy class $b^{A_0} = \{a^{-1}ba \mid a \in A_0\}$ of b under A_0 is an connected subset of A.

Proof. Clearly the mapping $\mu_b : a \mapsto ba$ with $a \in A$ is a composition of two polynomial maps $A \to \{b\} \times A \to A$ first of which is the embedding given by $a \mapsto (b,a)$ for $a \in A$ and the second is the restriction of the multiplication $\mu : A \times A \to A$ on $\{b\} \times A$, so that μ_b is a polynomial map. Similarly, the mapping $a \mapsto b^{-1}ab$ is a composition of corresponding polynomial maps $A \to \{b^{-1}\} \times A \times \{b\} \to A$. Therefore the embedding $A \to A \times A$ given by $a \mapsto (a^{-1}, a^{\mu_b})$ for $a \in A$ is also a polynomial map and hence $a \mapsto a^{-1}ba$ is so because $a^{-1}ba = (a^{-1}, a^{\mu_b})^{\mu}$. In particular, as b^{A_0} is the image of A_0 under this map, it is connected by Lemma 3.1.2). Finally, the mapping $a \mapsto [a,b]$ is a polynomial map because $[a,b] = (a^{-1}, b^{-1}ab)^{\mu}$. □

Corollary 3.7. *Let A be an algebraic group whose connected closed normal subgroup A_0 is of finite index k in A. Then every finite conjugacy class of elements of A contains at most k elements each of which centralizers A_0.*

Proof. If $a \in A$ and the conjugacy class a^A is finite, then the subset $a^{A_0} = \{a\}$ by Lemma 3.6 and so $A_0 \subseteq C_A(a)$. Therefore there are at most k conjugates of a in A. □

If B and C are subsets of a group A, then we denote by $[B,C]$ the subgroup of A generated by all group commutators $[b,c]$ with $b \in B$ and $c \in C$.

Lemma 3.8. *Let A be an algebraic group. If B and C are non-empty connected subsets of A, then the subgroup $[B,C]$ is connected. In particular, the derived subgroup A' of A is connected if A is so.*

Proof. Note first that the mapping $A \times A \to A$ given by $(a,b) \mapsto [a,b]$ with $a, b \in A$ is a polynomial map because $[a,b] = (a^{-1}, b^{-1}ab)^{\mu}$ and $(a,b) \mapsto (a^{-1}, b^{-1}ab)$ is a polynomial map from $A \times A$ into $A \times A$. Put next $D = \{[b,c] \mid b \in B, c \in C\}$ and let $D_n = \{d_1 \dots d_n \mid d_i \in D, 1 \le i \le n\}$. Then D is an connected subset of A by Lemma 3.2. Therefore D_n is so for every $n \ge 1$ by Lemma 3.1.2) because it is the polynomial image of the connected algebraic set $D \times \dots \times D$ with n factors. As $[B,C] = \bigcup_{n=1}^{\infty} D_n$ and since the union of an ascending chain of connected subsets of A is also connected, the proof is completed. □

It is easy to verify that the group $T(n,F)$ of all upper triangular $n \times n$-matrices over F is a connected closed subgroup of the algebraic group $GL(n,F)$

and it is soluble of derived length n. The following theorem which is due to Kolchin may be viewed as a converse of this assertion.

Theorem 3.9. (Kolchin) *Let the field F be algebraic closed and A a soluble connected subgroup of $GL(n,F)$. Then A is conjugate in $GL(n,F)$ with a subgroup of $T(n,F)$.*

Proof. Obviously the theorem holds for $n=1$. If $n>1$ and the vector space F^n has a proper subspace of dimension $m \geq 1$ which is invariant under A, then there exist a matrix $g \in GL(n,F)$ and two mappings $\rho : A \to GL(m,F)$ and $\sigma : A \to GL(n-m,F)$ such that, for each $a \in A$, the equality

$$g^{-1}ag = \begin{pmatrix} a^\rho & * \\ 0 & a^\sigma \end{pmatrix}$$

holds. Clearly both mappings ρ and σ are polynomial, so that the groups A^ρ and A^σ are connected by Lemma 3.1.2). By induction on n, there exist matrices $h_1 \in GL(m,F)$ and $h_2 \in GL(n-m,F)$ such that $h_1^{-1}A^\rho h_1 \subseteq T(m,F)$ and $h_2^{-1}A^\rho h_2 \subseteq T(n-m,F)$. Then $h = \begin{pmatrix} h_1 & 0 \\ 0 & h_2 \end{pmatrix} \in GL(n,F)$ and $(gh)^{-1}A(gh) \subseteq T(n,F)$.

Suppose now that F^n has no non-zero proper subspaces which are invariant under A, i.e. the action of A on F^n is irreducible. Since the derived subgroup A' of A is connected by Lemma 3.8, we may assume that $g^{-1}A'g \subseteq T(n,L)$ for some $g \in GL(n,F)$ by induction on the derived length of A. Let v be a common eigenvector for the matrices of A', so that $vb = k_b v$ for each $b \in A'$ and some $k_b \in F$ depending on b. Then, for each $a \in A$, it follows that $(va)b = (v(aba^{-1}))a = (k_{\{aba^{-1}\}}v)a = k_{\{aba^{-1}\}}(va)$ because $aba^{-1} \in A'$. As A is irreducible on F^n, this implies that there exists a basis of F^n whose elements are common eigenvectors for A'. Therefore we can choose the matrix g such that the subgroup $g^{-1}A'g$ consists of diagonal matrices. Since the eigenvalues of two conjugate matrices coincide, the conjugacy class b^A of any matrix $b \in A'$ must be finite and hence b centralizes A by Corollary 3.7. Thus A' is a central subgroup of A and so it consists only of scalar matrices because $(va)b = k_b(va)$ for every $a \in A$. Furthermore, every matrix $b \in A'$ has determinant 1 because b is a product of commutator matrices. Therefore $k_b^n = 1$ and hence A' is of order at most n. Being connected, $A' = 1$ and so A is abelian. Since A is irreducible on F^n, this implies that $n = 1$ because every commutative set of square matrices over F has a common eigenvalue. Thus A is triangular. □

Lemma 3.10. *Let A be an algebraic group and B its closed subset. Then the normalizer $N_A(B) = \{a \in A \mid a^{-1}Ba = B\}$ of B in A is closed. In particular, the centralizer of every subset of A is closed.*

Proof. For every $b \in B$, put $N_b = \{a^{-1}ba \in B\}$. Then N_b is the full preimage of B under τ_b and so N_b is a closed subset of A by Lemma 3.1.1). Therefore the intersection $N_1 = \cap_{b\in B} N_b = \{a \in A \mid a^{-1}Ba \subseteq B\}$ is closed. By the same

reason, the subset $N_2 = \{a \in A \mid aBa^{-1} \subseteq B\}$ and hence $N_A(B) = N_1 \cap N_2$ is also closed. In particular, for every $a \in A$, the centralizer $C_A(a) = \{c \in A \mid c^{-1}ac = a\}$ of a in A is closed. Since the centralizer of a subset of A coincides with the intersection of the centralizers of its elements, the proof is completed. □

If A is an algebraic set, regarded as a topological space with Zariski topology, and S a subset of A, then the intersection of all closed subsets of A containing S is called a *closure* of S in A and denoted by $\bar{S}$.

Lemma 3.11. *Let A be an algebraic group and B a subgroup of A. Then the closure $\bar{B}$ is also a subgroup of A. Moreover, if B is normal in A, then $\bar{B}$ is.*

Proof. Since $B^{-1} = \{b^{-1} \mid b \in B\} = B$ and the mapping $\nu : a \mapsto a^{-1}$ for $a \in A$ is continuous, the subset $\bar{B}^{-1}$ as the full preimage of $\bar{B}$ under ν is closed an contains B, so that $\bar{B} \subseteq \bar{B}^{-1}$. By symmetry, $\bar{B}^{-1} \subseteq \bar{B}$ and thus $\bar{B}^{-1} = \bar{B}$.

Next, for each $b \in B$, we have $bB = B$ and the subset $b^{-1}\bar{B}$ is closed by Lemma 3.3. Therefore $\bar{B} \subseteq b^{-1}\bar{B}$ and hence $b\bar{B} \subseteq \bar{B}$. Furthermore, if $a \in \bar{B}$, then $a^{-1} \in \bar{B}$ and thus $Ba^{-1} \subseteq B\bar{B} \subseteq \bar{B}$. This implies that $B \subseteq \bar{B}a$ and so $\bar{B} \subseteq \bar{B}a$. Thus $\bar{B}\bar{B} \subseteq \bar{B}$, i.e. $\bar{B}$ is a subgroup of A.

Finally, if B is normal in A, then $a^{-1}Ba = B$ for every $a \in A$ and the subset $a^{-1}\bar{B}a$ is closed by Lemma 3.3. Therefore $\bar{B} \subseteq a^{-1}\bar{B}a$ and similarly $\bar{B} \subseteq a\bar{B}a^{-1}$. Thus $a^{-1}\bar{B}a = \bar{B}$, as desired.

Lemma 3.12. *Let A be an algebraic group, B and C its non-empty subsets and let D be a subgroup of A. If $[B, C] \subseteq D$, then $[\bar{B}, \bar{C}] \subseteq \bar{D}$.*

Proof. Let $c \in C$. Since the mapping $a \mapsto [a, c]$ for $a \in A$ is continuous by Lemma 3.6, the full preimage of the subgroup $\bar{D}$ in A is closed and contains B. Therefore it contains $\bar{B}$ and hence $[\bar{B}, c] \subseteq \bar{D}$. Next, for each $b \in \bar{B}$, the mapping $a \mapsto [b, a] = [a, b]^{-1}$ with $a \in A$ is also continuous. Thus the full preimage of $\bar{D}$ in A under this mapping contains C and so $\bar{C}$. Therefore $[\bar{B}, \bar{C}] \subseteq \bar{D}$. □

Theorem 3.13. *Let A be an algebraic group and B a subgroup of A. Then*

1) the subgroup $\bar{B}$ is soluble of derived length n if and only if B is, and

2) the subgroup $\bar{B}$ is nilpotent of class n if and only if B is.

Proof. Put $B = B^{(0)}$ and $B^{(i+1)} = [B^{(i)}, B^{(i)}]$ for every $i \geq 0$. Then $\bar{B}^{(i)} \subseteq \overline{B^{(i)}}$ by Lemma 3.12 and so $\bar{B}^{(i)} = \overline{B^{(i)}}$. In particular, $B^{(n)} = 1$ if and only if $\bar{B}^{(n)} = 1$, so that statement 1) holds.

Similarly, $\underbrace{[\bar{B}, \ldots, \bar{B}]}_{n \text{ times}} = \underbrace{[B, \ldots, B]}_{n \text{ times}}$ and this implies statement 2). □

Recall that a group G is called *linear* if it is isomorphic to a subgroup of the group $GL(n, K)$ of all non-singular $(n \times n)$-matrices over a field K. Clearly, if

$\bar{K}$ is the algebraic closure of K, then $GL(n,K)$ can be viewed as a subgroup of the group $GL(n,\bar{K})$. The group G is said to be *triangularizable*, if it is conjugate in $GL(n,\bar{K})$ with a subgroup of the group $T(n,\bar{K})$ of all upper triangular $(n\times n)$-matrices over $\bar{K}$.

Corollary 3.14. *Every soluble linear group G contains a triangularizable subgroup of finite index.*

Proof. Let $\bar{G}$ be the closure of G in the algebraic group $GL(n,\bar{K})$. Then $\bar{G}$ is a soluble algebraic group by Theorem 3.13. Therefore its connected component $\bar{G}_0$ containing 1 is a closed connected subgroup of finite index in $\bar{G}$ by Theorem 3.4. Since $\bar{G}_0$ is triangularizable by Theorem 3.9, the intersection $G\cap\bar{G}_0$ is a triangularizable subgroup of finite index in G. □

4 Polynomial homomorphisms of algebraic groups

In what follows the field F will be algebraically closed.

Lemma 4.1. *Let A and B be algebraic sets and $\phi: A\to B$ a polynomial map. Then the associated algebra homomorphism $\hat{\phi}: F[B]\to F[A]$ is injective if and only if $\overline{A^\phi}=B$.*

Proof. If $\hat{\phi}$ is injective and $g\in \mathrm{Ann}_{F[B]}(A^\phi)$, then, for every $a\in A$, we have $0=g(a^\phi)=g^{\hat{\phi}}(a)$, so that $g^{\hat{\phi}}=0$ and thus $g=0$. Conversely, if $\overline{A^\phi}=B$ and $g^{\hat{\phi}}=0$, then $g(a^\phi)=0$ and so $g\in\mathrm{Ann}_{F[B]}(A^\phi)$. As $\mathrm{Ann}_B(\mathrm{Ann}_{F[B]}(A^\phi))=\overline{A^\phi}=B$, this means that $\mathrm{Ann}_{F[B]}(A^\phi)=0$ and so $g=0$. □

Lemma 4.2. *Let R be a commutative ring with 1 and S a subring of R containing 1. If R is a finitely generated S-module and I is a proper ideal of S, then $IR\neq R$.*

Proof. Suppose the contrary and let $R=r_1S+\ldots+r_nS$ for some elements $r_1,\ldots,r_n\in R$. Then $R=RI=r_1I+\ldots+r_nI$ and so there exists elements $a_{ij}\in I$ for all $1\le i,j\le n$ such that $r_i=\sum_{j=1}^n a_{ij}r_j$. Therefore $\sum_{j=1}^n(a_{ij}-\delta_{ij})r_j=0$ for all $1\le j\le n$. If $a=\det(a_{ij}-\delta_{ij})$, then $ar_i=0$ for all $1\le i\le n$ by Cramer's rule, so that $aR=0$. Hence $a=0$ and thus $1\in I$ because $a\in 1+I$. But then $I=S$, contrary to the hypothesis of the lemma. □

Lemma 4.3. *Let A and $B\subseteq F^n$ be algebraic sets and $\phi: A\to B$ a polynomial map. If the associated algebra homomorphism $\hat{\phi}: F[B]\to F[A]$ is injective and the algebra $F[A]$ is integer over $F[B]^{\hat{\phi}}$, then $A^\phi=B$, i.e. the polynomial map ϕ is surjective.*

Proof. For each $1 \leq i \leq n$ and every $b = (b_1, \ldots, b_n) \in B$, let f_i be the function of $F[B]$ such that $f_i(b) = b_i$. Then

$$\mathrm{Ann}_{F[B]}(b) = (f_1 - b_1)F[B] + \ldots + (f_n - b_n)F[B]$$

and $b \in A^\phi$ if and only if the ideal

$$I_b = (f_1^{\hat{\phi}} - b_1)F[A] + \ldots + (f_n^{\hat{\phi}} - b_n)F[A]$$

of $F[A]$ is properly contained in $F[A]$.

Indeed, if $b = a^\phi$ for some $a \in A$, then $(f_i^{\hat{\phi}} - b_i)(a) = f_i^{\hat{\phi}}(a) - b_i = f_i(b) - b_i = 0$ for every i and so $a \in \mathrm{Ann}_A(I_b)$. This implies that $\mathrm{Ann}_A(I_b) \neq \emptyset$ and so $I_b \neq F[A]$. Conversely, if $I_b \neq F[A]$, then $\mathrm{Ann}_{F[A]}(\mathrm{Ann}_A(I_b)) = \sqrt{I_b} \neq F[A]$ by the Hilbert Nullstellensatz and therefore $\mathrm{Ann}_A(I_b) \neq \emptyset$. Thus, for $a \in \mathrm{Ann}_A(I_b)$, we have $0 = f_i^{\hat{\phi}}(a) - b_i = f_i(a^\phi) - b_i$ for every i and hence $a^\phi = b$.

Thus, if $A^\phi \neq B$, there exists $b \in B$ with $I_b = F[A]$. On the other hand, $I_b = \mathrm{Ann}_{F[B]}(b)^{\hat{\phi}} F[A]$. Since $F[A]$ is integer over $F[B]^{\hat{\phi}}$, it is a finitely generated $F[B]^{\hat{\phi}}$-module and therefore $\mathrm{Ann}_{F[B]}(b) = F[B]$ by Lemma 4.2, which is impossible. □

If A is an irreducible closed subset of F^n, then the factor ring $F[A] = F[x_1, \ldots, x_n]/\mathcal{P}(M)$ is a domain by Theorem 2.16. Let $F(A)$ denote the field of quotients of $F[A]$. Every element $q \in F(A)$ can be written in the form $q = f^{-1}g$ for some elements $f = f(x_1, \ldots, x_n) + \mathcal{P}(A)$ and $g = g(x_1, \ldots, x_n) + \mathcal{P}(A)$ of $F[A]$ with $f(x_1, \ldots, x_n) \notin \mathcal{P}(A)$. For an element $a = (a_1, \ldots, a_n) \in A$, we shall say that q is *defined at* a if $f(a_1, \ldots, a_n) \neq 0$. Clearly in this case the element $q(a) = f(a_1, \ldots, a_n)^{-1} g(a_1, \ldots, a_n) \in F$ depends only on q and not on the choice of polynomials $f(x_1, \ldots, x_n)$ and $g(x_1, \ldots, x_n)$. Thus the elements of $F(A)$ can be viewed as *rational functions* on A although they are not defined everywhere on A.

Lemma 4.4. *Let A be an irreducible closed subset of F^n. If an element $q \in F(A)$ is defined at every element of A, then $q \in F[A]$ and so there exists a polynomial $p(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ such that $q(a) = p(a_1, \ldots, a_n)$ for every $a = (a_1, \ldots, a_n) \in A$.*

Proof. Let $q = f^{-1}g$ for some $f, g \in F[A]$ with $f = f(x_1, \ldots, x_n) + \mathcal{P}(A) \neq \mathcal{P}(A)$ and let I be the ideal of $F[x_1, \ldots, x_n]$ generated by $f(x_1, \ldots, x_n)$ and $\mathcal{P}(A)$. Assume that $I \neq F[x_1, \ldots, x_n]$. Then $\sqrt{I} \neq F[x_1, \ldots, x_n]$ and obviously $\mathcal{N}(I) \subseteq A$. Since $\mathcal{P}(\mathcal{N}(I)) = \sqrt{I}$ by the Hilbert Nullstellensatz, there exists an element $b = (b_1, \ldots, b_n) \in A$ such that $f(b_1, \ldots, b_n) = 0$. But then the element q is not defined at b, contrary to the hypothesis of the lemma. Thus $I = F[x_1, \ldots, x_n]$ and so $q \in F[A]$. Therefore $q = p(x_1, \ldots, x_n) + \mathcal{P}(A)$ for some $p(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ and clearly the polynomial $p(x_1, \ldots, x_n)$ is desired. □

The following assertion is basic for the theory of algebraic groups.

Theorem 4.5. *Let A be an algebraic subset of F^n. If $\phi : A \to F^n$ is a polynomial map, then the image A^ϕ of A in F^n contains a non-empty open subset of its algebraic closure $\overline{A^\phi}$.*

Proof. Put $B = \overline{A^\phi}$ an assume first that A is irreducible with $\dim_F(A) = 1$. As $\phi : A \to B$, the associated algebra homomorphism $\hat{\phi} : F[B] \to F[A]$ is injective by Lemma 4.1, so that it can next be assumed that $F[B] \subseteq F[A]$. Furthermore, the algebra $F[A]$ is a domain by Theorem 2.16 and its field of quotients $F(A)$ is of transcendence degree 1 over F. Since A^ϕ and so B is an irreducible set by Lemma 3.1.2), we may suppose that $F[B] \neq F$. Then the fields of quotients $F(B)$ of $F[B]$ is also of transcendence degree 1 over F and so $F[A]$ is algebraic over $F(B)$. If $f_1, \ldots, f_m$ are generators of $F[A]$, then there exists elements $g_1, \ldots, g_m \in F[B]$ such that each $f_i g_i$ is integer over $F[B]$. Put $g = g_1 \ldots g_m$. Then it is easy to see that the algebra $F[A]$ is integer over the subalgebra $F[B][g^{-1}]$ of the field of quotients $F(B)$ and so the algebra $F[A][g^{-1}]$ is also integer over $F[B][g^{-1}]$.

Clearly the subset $B \setminus \mathrm{Ann}_B(g)$ of B is open in B. The mapping $\psi : B \setminus \mathrm{Ann}_B(g) \to B \times F^1$ given by $b^\psi = (b, g(b)^{-1})$ identifies this subset with the closed subset $B_g = \{(b, v) \mid b \in B, v \in F^1, g(b)v = 1\}$ of the algebraic set $B \times F^1$. It is clear that the algebra $F[B \times F^1]$ is isomorphic to the polynomial algebra $F[B][y]$ in one indeterminate y over $F[B]$. If $F[B] = F[X]/\mathcal{P}(B)$ with $X = \{x_1, \ldots, x_n\}$ and $g(X)$ be a polynomial of $F[X]$ such that $g = g(X) + \mathcal{P}(B)$, then $\mathcal{P}(B_g) = \mathcal{P}(B)F[X, y] + (g(X)y - 1)F[X, y]$ in the polynomial algebra $F[X, y]$ in $n+1$ indeterminates X and y. Since the rational function $g^{-1} \in F(B)$ is defined at every element of B_g, it belongs to $F[B_g]$ by Lemma 4.4, so that the algebra $F[B_g]$ is isomorphic to the subalgebra $F[B][g^{-1}]$ of the field of quotients $F(B)$. Similarly, the open subset $A \setminus \mathrm{Ann}_A(g)$ of A is identified with the closed subset $A_g = \{(a, v) \mid a \in A, v \in F^1, g(a)v = 1\}$ of the algebraic set $A \times F^1$ and the algebra $F[A_g]$ is isomorphic to $F[A][g^{-1}]$.

Clearly the polynomial map $\phi : A \to B$ induces the polynomial map $\bar{\phi} : A \times F^1 \to B \times F^1$ by the rule $(a, v)^{\bar{\phi}} = (a^\phi, v)$ with $a \in A$ and $v \in F^1$ whose restriction on A_g is a polynomial map of A_g into B_g. Since the associated algebra homomorphism $\hat{\bar{\phi}} : F[B][g^{-1}] \to F[A][g^{-1}]$ is injective and $F[A][g^{-1}]$ is integer over $F[B][g^{-1}]$, the polynomial map $\bar{\phi} : A_g \to B_g$ is surjective by Lemma 4.3, so that $A_g^{\bar{\phi}} = B_g$. This means that $(A \setminus \mathrm{Ann}_A(g))^\phi = B \setminus \mathrm{Ann}_B(g)$ and thus the open set $B \setminus \mathrm{Ann}_B(g)$ is contained in A^ϕ. □

The followin important concequence of Theorem 4.5 shows that every polynomial homomorphism of an algebraic group A is a closed continuous mapping. In other words, the image of a closed subgroup of A is closed.

Corollary 4.6. *Let A be an algebraic group and $\phi : A \to GL(n, F)$ a polynomial homomorphism of A into $GL(n, F)$. Then the image A^ϕ is a closed subgroup of $GL(n, F)$.*

Proof. Let B be the closure of A^ϕ in $GL(n, F)$. Then B is a closed subgroup in $GL(n, F)$ by Lemma 3.11. The subgroup A^ϕ contains an non-empty open

set U of B by Theorem 4.5. Clearly, for every $b \in B$, the set bU is open in B because its complement $B \setminus bU = b(B \setminus U$ in B is closed by Lemma 3.3. Thus, if A is connected, then B is and so the intersection $U \cap bU$ is non-empty. Therefore $b \in UU^{-1} \subseteq (A^\phi)(A^\phi)^{-1} = A^\phi$ and hence $A^\phi = B$. In the general case, if A_0 is the connected component of A containing 1, then A_0^ϕ is a closed subgroup of $GL(n, F)$ and so the subgroup $A^\phi = \cup_{a \in A^\phi} A_0^\phi$ is also closed because A_0 is of finite index in A by Theorem 3.4. □

A subset S of an algebraic set A is called *locally closed* in A if it is open in its closure in A. In other words, S is the intersection of an open set and a closed set of A. A subset of A is called *constructible* in A if it is a union of finite number of locally closed subsets of A. It is easy to see that every constructible subset of a constructible subset of A is also constructible in A.

Lemma 4.7. (Chevalley)*Let A and B be algebraic sets and $\phi : A \to B$ a polynomial map. Then A^ϕ is a constructible subset in B. More generally, if C is a constructible set in A, then C^ϕ is such a set in B.*

Proof. It is easy to see that the second statement follows from the first. To prove first it suffices to consider the case when both A and B are irreducible. Then A^ϕ and so its closure $\overline{A^\phi}$ in B is also irreducible. Using induction on $\dim_F(B)$, we can assume that the result holds if $\dim_F(\overline{A^\phi}) < \dim_F(B)$. Let $\dim_F(\overline{A^\phi}) = \dim_F(B)$, so that $\overline{A^\phi} = B$. Then A^ϕ contains an non-empty open set U of B. Let $C_1, \ldots, C_n$ be the irreducible components of the set $B \setminus U$ and, for each $1 \leq i \leq n$, let $A_{i1}, \ldots, A_{im_i}$ be the irreducible components of the full preimage A_i of C_i under ϕ. Then $\dim_F(C_i) < \dim_F(B)$ and therefore, for each restriction $\phi_{ij} : A_{ij} \to C_i$ of ϕ on A_{ij}, the image $A_{ij}^{\phi_{ij}}$ is a constructible subset in C_i. Since $A^\phi = U \cup (\cup_{ij} A_{ij}^{\phi_{ij}})$, the set A^ϕ is also constructible. □

Corollary 4.8. *If A is an algebraic set and B is a constructible subset in A, then B contains a dense open subset of its closure $\bar{B}$.*

Proof. The set B is the union of a finitely many closed irreducible subsets of B, say, $B_1, \ldots, B_n$. Then each B_i is also a constructible subset of A and $\bar{B} = \cup_i \bar{B}_i$. If $U_i \subseteq B_i$ is a dense open set of $\bar{B}_i$, then $\cup_i U_i$ is such a set in $\bar{B}$. Thus we may assume that B and so $\bar{B}$ is irreducible. Since B is a union of finitely many locally closed subsets of A, say, $C_1, \ldots, C_m$, we have $\bar{B} = \cup_i \bar{C}_i$ and therefore $\bar{B} = \bar{C}_i$ for some i. By definition C_i is open $\bar{C}_i$, so that C_i is dense and open in $\bar{B}$. □

Lemma 4.9. *Let A be an algebraic group and B its subgroup which is a constructible subset of A. Then B is a closed subgroup of A.*

Proof. The subgroup B contains a dense and open subset U of its closure $\bar{B}$ in A. Since $\bar{B}$ is a subgroup of A by Lemma 3.11, for every $b \in \bar{B}$ the subset bU is dense and open in $\bar{B}$. Therefore $U \cap bU \neq \emptyset$ and hence $b \in UU^{-1} \subseteq BB^{-1} = B$, so that $B = \bar{B}$. □

Lemma 4.10. *Let A be an algebraic group and let B and C be a closed subgroup of A. If the closure $\overline{BC}$ is a subgroup of A, then $\overline{BC} = BCB = CBC$. In particular, if $BC = CB$, then BC is a closed subgroup of A.*

Proof. Since BC is the image of the algebraic set $B \times C$ under the polynomial map $B \times C \to A$ given by $(b, c)^\mu = bc$ with $b \in B$ and $c \in C$, it is a constructible subset of A by Lemma 4.7. Therefore BC contains a dense open subset U of the closure $\overline{BC}$. Therefore $U \cap aU \neq \emptyset$ for each $a \in \overline{BC}$ and so $a \in UU^{-1} \subseteq (BC)(CB) = BCB$. Hence $\overline{BC} = BCB$ and, by symmetry, $\overline{BC} = CBC$. □

Recall that every linear group A can be viewed as a subgroup of an algebraic linear group. If A_0 is the connected component of A containing 1, then $A_0 = A \cap \bar{A}_0$.

Lemma 4.11. *Let the linear group $A = BC$ be the product of two subgroups B and C. If A_0, B_0 and C_0 are the connected components containing 1 of A, B and C, respectively, then $A_0 \subseteq \bar{B}_0\bar{C}_0$.*

Proof. Clearly the subgroups B_0 and C_0 are contained in A_0 and there exist elements $b_1, \ldots, b_n \in B$ and $c_1, \ldots, c_n \in C$ such that

$$A = \bigcup_{i=1}^{n} b_i B_0 C_0 c_i.$$

It is easy to see that, for each i, either $A_0 \cap b_i B_0 C_0 c_i = \emptyset$ or $b_i B_0 C_0 c_i \subseteq A_0$. Therefore

$$A_0 = \bigcup_{j=1}^{m} b_{i_j} B_0 C_0 c_{i_j}$$

and hence

$$\bar{A}_0 = \bigcup_{j=1}^{m} b_{i_j} \overline{B_0 C_0} c_{i_j}.$$

As $\bar{A}_0 = (\bar{A})_0$, this implies that $\bar{A}_0 = \overline{B_0 C_0}$. Obviously $b_{i_j} \bar{B}_0 \bar{C}_0 c_{i_j} \subseteq \bar{A}_0$ and either

$$b_{i_j} \bar{B}_0 \bar{C}_0 c_{i_j} \cap b_{i_k} \bar{B}_0 \bar{C}_0 c_{i_k} = \emptyset$$

or

$$b_{i_j} \bar{B}_0 \bar{C}_0 c_{i_j} = b_{i_k} \bar{B}_0 \bar{C}_0 c_{i_k}.$$

By Theorem 4.5, the set $\bar{B}_0\bar{C}_0$ contains a non-empty open subset U of its closure $\overline{\bar{B}_0\bar{C}_0} = \overline{B_0 C_0} = \bar{A}_0$. Since the intersection $U \cap bUc$ is non-empty for all $b, c \in \bar{A}_0$ and the subgroup $\bar{A}_0$ is connected, it follows that $b_{i_j} \bar{B}_0 \bar{C}_0 c_{i_j} = \bar{B}_0 \bar{C}_0$ for every j and so

$$A_0 = \bigcup_{j=1}^{m} b_{i_j} B_0 C_0 c_{i_j} \subseteq \bigcup_{j=1}^{m} b_{i_j} \bar{B}_0 \bar{C}_0 c_{i_j} = \bar{B}_0 \bar{C}_0,$$

as claimed. □

A group G is called *abelian-by-finite* if G has an abelian normal subgroup of finite index and G is *metabelian* if the derived subgroup of G is abelian.

Theorem 4.12. *Let the linear group $A = BC$ be the product of two abelian-by-finite subgroups B and C. Then A contains a metabelian subgroup of finite index.*

Proof. Since the connected component containing 1 has no subgroups of finite index, the subgroups B_0 and C_0 are abelian. Therefore the closed subgroups $\bar{B}_0$ and $\bar{C}_0$ are also abelian and their product $\bar{B}_0\bar{C}_0$ contains A_0 by Lemma 4.11. Hence the subgroup A_0 must be metabelian. This can be proved by arguments which were used by Itô in proving the theorem that every group of the form $G = HK$ with abelian subgroups H and K is metabelian. See Theorem 2.1.1 in the monograph "Product of groups" of B. Amberg, S.Franciosi and F. de Giovanni, Clarendon Press, Oxford, 1992. □