MA 312 Commutative Algebra / Jan–April 2020

(BS, Int PhD, and PhD Programmes)

Download from : http://www.math.iisc.ac.in/patil/courses/Current Courses/...

Tel : +91-(0)80-2293 3212 / 09449076304 **E-mails :** patil@math.ac.in

Lectures : Tuesday and Thursday ; 15:30–17:00 **Venue:** MA LH-5 / LH-1

4. Algebras[1] — Substitution homomorphisms and Zeros of Polynomials*

Submit a solution of ANY ONE of the *Exercise ONLY. **Due Date : Thursday, 27-02-2020**

Complete Correct Solution of the ** Exercise carry BONUS POINTS !
Recommended to solve the violet colored ^{R} Exercises

* **Substitution homomorphisms, Zeroes, Polynomial functions etc.** Let A be a commutative ring. More often used property so-called universal property of the polynomial algebra over A can be formulated as:

For every *commutative* A-algebra B and an indexed set I, the map

$$\mathrm{Hom}_{A\text{-alg}}(A[X_i \mid i\in I], B) \longrightarrow B^I\,, \quad f \longmapsto (f(X_i))_{i\in I}$$

is bijective. For each I-tuple $x=(x_i)_{i\in I}$, the substitution A-algebra homomorphism $\varepsilon_x : A[X_i \mid i\in I] \to B$, $X_i \mapsto x_i$ is an A-algebra homomorphism with

$$\varepsilon_x(F) = F(x) = F(x_i \mid i\in I) = \textstyle\sum_{\nu\in\mathbb{N}^{(I)}} a_\nu x^\nu\,,\ F = \textstyle\sum_{\nu\in\mathbb{N}^{(I)}} a_\nu X^\nu \in A[X_i \mid i\in I].$$

The image of the substitution homomorphism ε_x is the (commutative) A-subalgebra $A[x_i \mid i\in I]$ of B generated by x_i, $i\in I$. The kernel $\mathrm{Ker}\,\varepsilon_x$ is called the relation ideal of the elements x_i, $i\in I$. By the isomorphism theorem $A[X_i \mid \in I]/\mathrm{Ker}\,\varepsilon_x \xrightarrow{\sim} A[x_i \mid i\in I]$. If the relation ideal $\mathrm{Ker}\,\varepsilon_x = 0$, i. e. the substitution A-algebra homomorphism induces an isomorphism $A[X_i \mid \in I] \xrightarrow{\sim} A[x_i \mid i\in I]$, then the family $x=(x_i)_{i\in I}$ is called algebraically independent or transcendental over A; in the other case it is caled algebraic ally dependent over A. If $|I|=1$, then we simply say that transcendental element (resp. algebraic element) over A.

Therefore an element $x\in B$ is algebraic over A if and only if there exists a polynomial $F\neq 0$ in $A[X]$ with $F(x)=0$. Moreover, if there exists a *monic* polynomial $F\in A[X]$ with $F(x)=0$, then x is said to be integral over A. The A-algebra B is called algebraic (resp. integral) over A if every element of B is algebraic (resp. integral) over A. *Every finite A-algebra is integral over A.* Over a field $A=K$ the concepts “algebraic” and “integral” are naturally coincides : If namely $\mathrm{Dim}_K B$ is

[1] **Algebra over a commutative ring.** In the concept of an algebra the ring –and module structures and combined together. Let A be a ring and $B=(B+)$ be an additive abelian group. Then B is an A-algebra if B is a ring as well as an A-module, where the addition for both the structures is the given addition on B. The only reasonable compatibility condition for both the structures is the left – and right multiplications L_x and R_y, $x,y\in B$, of the ring $(B,+,\cdot)$ are A-linear, i e. $L_x\circ\vartheta_b = \vartheta_b\circ L_x$ and $R_y\circ\vartheta_a = \vartheta_a\circ R_y$ hold or – more explicitly — $x(by)=b(xy)$ and $(ax)y=a(xy)$ for all $a,b\in A$ and $x,y\in B$. In particular, $\vartheta_a = L_{a\cdot 1_B} = R_{a\cdot 1_B}$ for all $a\in A$, i. e. $A\cdot 1_A$ is contained in the center $\mathrm{Z}(B)$ of B. With this motive, from the begining we may assume that the base ring A is commutative.

Let A be a commutative ring. An A-algebra B (or an algebra over A) is an A-module with a multiplication $\cdot : B\times B\to B$ such that the $(B,+,\cdot)$ is a ring and all left–and right multiplications L_x and R_y, $x,y\in B$, are A-linear, i. e. the compatibility conditions :

$$\text{(i)}\ \ x(by)=b(xy) \quad\text{and}\quad \text{(ii)}\ \ (ax)y=a(xy)\ \ \text{hold for all}\ \ a,b\in A\,,\ x,y\in B\,.$$

These two conditions can be combined into one condition :

$$(ax)(by)=(ab)(xy) \quad \text{for all} \quad a,b\in A\,,\ x,y\in B\,.$$

Altogether, the map $\varphi\colon A\to B$, $a\mapsto a\cdot 1_A$, is a ring homomorphism *whose image is contained in the center of* B, and is called the structure homomorphism of B. The scalar multiplication (of A) on B is uniquely determined by φ : It is $ax=(a\cdot 1_B)x=\varphi(a)x$ for all $a\in A$, $x\in B$.

A map $f\colon B\to C$ of A-algebras is called an A-algebra homomorphism if f is a ring–as well as an A-module homomorphism. The set of all A-algebrahomomorphisms $B\to C$ is denoted by $\mathrm{Hom}_{A\text{-Alg}}(B,C)$. It is a subset of $\mathrm{Hom}_A(B,C)$. The set $\mathrm{End}_{A\text{-Alg}}(B)$ of the A-algebra endomorphisms of B is a monoid with respect to the composition with unit group $\mathrm{Aut}_{A\text{-Alg}}B$.

finite, then for $x \in B$ the substitution homomorphism $\varepsilon_x \colon K[X] \to B$ can not be injective.

The residue-class algebras of the polynomial algebras over A are represented, up to isomorphism, all commutative A-algebras (and if $A = \mathbb{Z}$ then by all commutative rings). If the polynimials G_j, $j \in J$, generate the relation ideal $\operatorname{Ker} \varepsilon_x$, then we say that

$$\langle x_i,\ i \in I \mid G_j(x) = 0,\ \ j \in J \rangle$$

is a representation of the commutative A-algebra $A[x_i, i \in I]$ by generators and relations. Every such represented commutative A-algebra $A[x_i, i \in I]$ has the following universal property : *If A is an arbitrary commutative A-algebra, then the map*

$$\mathrm{Hom}_{A\text{-Alg}}(A[x_i, i \in I], B) \xrightarrow{\sim} \mathrm{V}_B(G_j, j \in J) := \{a = (a_i) \in B^I \mid G_j(a) = 0\,,\ j \in J\}$$

is bijective. Therefore to understand the (common) zero-sets $\mathrm{V}_B(G_j, j \in J) = \bigcap_{j \in J} \mathrm{V}_B(G_j)$ for arbitrary *commutative* A-algebras B , one needs to study the A-algebra $A[x_i, i \in I]$. If the index sets I and J are finite, then the representation is said to be finite. *In particular, the residue-class A-algebras of the polynomial A-algebras* $A[X_1, \ldots, X_n]$, $n \in \mathbb{N}$, *up to isomorphism, are all commutative A-algebras of finite type.*

The substitution homomorphisms $\varepsilon_x \colon A[X_i \mid i \in I] \to A$, $x \in A^I$, together define a homomorphism

$$\varepsilon \colon A[X_i, i \in I] \longrightarrow A^{A^I} = \mathrm{Maps}(A^I, A)\,, \quad F \longmapsto (x \mapsto \varepsilon_x(F) = F(x))$$

whose image is the so-called polynomial functions on A^I. Since $\varepsilon(X_i)$ is the i-th projection (= i-th coordinate function) $A^I \to A$, $x \mapsto x_i$, the A-algebra $\operatorname{Img} \varepsilon$ of the polynomial functions on A^I is generated by these coordinate function. In general, ε is not injective: *Distinct polynomial can define the equal polynomial functions.* For example, over a finite commutative ring A the monic polynomial $\prod_{a \in A}(X - a) \in A[X]$ of degree $|A|$ is the zero function on A.

4.1 Construct an example of a field K and an endomorphism $h : K \to K$ such that K is not a finite algebra over the field $h(K)$. (**Hint :** Rational function fields!)

4.2 Determine the quotient and the remainder of the division :

(a) of $f \in K[X]$ by $X^2 - a$ in $K[X]$, where K is a field.

(b) of $X^m - 1$ by $X^n - 1$ in $\mathbb{Z}[X]$ for $m, n \in \mathbb{N}^*$. (**Hint :** Use division with remainder in $\mathbb{Z}$ to write $m = qn + r$ with $q, r \in \mathbb{N}$, $0 \le r < n$. Then $X^m - 1 = X^{nq}X^r - 1$.). When exactly the ideal $\langle X^m - 1, X^n - 1 \rangle$ generated by $X^m - 1$ and $X^n - 1$ in $\mathbb{Z}[X]$ is principal? If, yes, what is its generator?

4.3 **(a)** What is the cardinality $\left|\mathrm{V}_{(\mathbb{Z}/\mathbb{Z}6)}(X^2 + X)\right|$?

(b) The polynomial $X^3 + X^2 + X + 1 \in (\mathbb{Z}/\mathbb{Z}4)[X]$ is a multiple of $X + 1$ and $X + 3$, but not of $(X + 1)(X + 3)$.

(c) Give an example of a commutative ring A such that $\mathrm{V}_A(X^2 - X)$ is infinite. .

(d) Compute the zeros in $\mathbb{Z}$ and the coefficients of X^{n-1} of the polynomial in $\mathbb{Z}[X]$ defined by the following determinant :

$$F(X) := \mathrm{Det}\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & X+1 & 1 & \cdots & 1 \\ 1 & 1 & X+2 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & X+n \end{pmatrix} \in \mathbb{Z}[X]\,.$$

(e) Let K be a field. What is the zero set $\mathrm{V}_{(K[Y]/\langle Y^2 \rangle)}(X^2)$ (in the K-algebra $K[Y]/(Y^2)$?.

4.4 Let $L\,|\,K$ be a field extension and $F,\ G \in K[X,Y]$ with $\gcd_{K[X,Y]}(F, G) = 1$. Then

$$|\mathrm{V}_L \cap \mathrm{V}_L(G)| \ \le\ \deg F \cdot \deg G.$$

4.5 Let A be an integral domain.

(a) Let $F \in A[X]$ and $n \in \mathbb{N}$. If $|\mathrm{V}_A(F)| > n$, then either $F = 0$ or $\deg F > n$.

(b) If A is *infinite*, $F, G \in A[X_i \mid i \in I]$, $F \neq 0$ and if $A^I \smallsetminus \mathrm{V}_A(F) \subseteq \mathrm{V}_A(G)$, then $G = 0$.

4.6 Let $F_1, \ldots, F_n \in A[X]$ be polynomials in one indeterminate over a commutative ring A of degrees $\leq n-2$ and let $a_1, \ldots, a_n \in A$ be arbitrary elements. Then

$$\mathrm{Det}\,\big(F_i(a_j)\big)_{1 \leq i,\, j \leq n} = 0\,.$$

4.7 Let $A \neq 0$ be a noetherian commutative ring and G_j, $j \in J$, be arbitrary family of polynomials in the polynomial algebra $A[X_1, \ldots, X_n]$. Then there exists a *finite* subset $J' \subseteq J$ with the following property : For every commutative A-Algebra B,

$$\mathrm{V}_B(G_j, j \in J) = \{x \in B^n \mid G_j(x) = 0\,,\ j \in J\} = \mathrm{V}_B(G_j, j \in J')\,.$$

(**Hint :** By Hilbert's Basis Theorem $A[X_1, \ldots, X_n]$ is also a noetherian ring.)

4.8 Let A be a commutative ring, $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ pairwise comaximal ideals in A and $\mathfrak{a} := \mathfrak{a}_1 \cdots \mathfrak{a}_m$. If $f \in A[X]$ and if $\mathrm{V}_{(A/\mathfrak{a}_i)}(f) \neq \emptyset$ for every $i = 1, \ldots, m$, then $\mathrm{V}_{(A/\mathfrak{a})}(f) \neq \emptyset$. (**Hint :** Use the following well-known *Chinese Remainder Theorem*[2].)

4.9 Let A be a commutative ring, $g \in A[X]$ be a polynomial of degree $n \geq 1$, with leading coefficient a unit and $\varepsilon_g : A[X] \to A[X]$ be the substitution homomorphism with $X \mapsto g$. Let $B = A[X]$ be the $A[X]$-algebra with the structure homomorphism ε_g. Then the $A[X]$-algebra B is free of rank n with basis $1, \ldots, X^{n-1}$. What is the kernel of the canonical $A[X]$-algebra substitution homomorphism $\varepsilon_X : (A[X])[Y] \to B$ with $Y \mapsto X$?

*__4.10__ For $m \in \mathbb{N}$, let $\mathrm{P}_m := K[X_1 \ldots, X_m]$ be the polynomial algebra in m indeterminates over the field K. If $\varphi\colon \mathrm{P}_m \to \mathrm{P}_n$ is an injective, (resp. surjective) K-algebra homomorphism, then $m \leq n$ (resp. $m \geq n$). In particular, if φ is an isomorphism, then $m = n$. (**Hint :** If $\deg \varphi(X_i) \leq d$, $i = 1, \ldots, m$, then $\deg \varphi(F) \leq d \cdot \deg F$ for all $F \in \mathrm{P}_m$. Further, use the fact that the polynomials in P_m of deg $\leq r \in \mathbb{N}$ form a K-vector space of dimension $\binom{r+m}{m}$ — In the case of that φ surjective, one can reduce to the case of that φ is injective. — One can use the concepts of derivations and module of K-derivations of K-algebras to give another proof of if φ is a K-algebra isomorphism, then $m = n$. If $m \neq n$, then P_m and P_n are not even isomorphic as rings ; because every ring isomorphism induces an automorphism of K, since $K^\times = \mathrm{P}_m^\times = \mathrm{P}_n^\times$.)

4.11 Let K be a field.

(a) The K-algebra automorphisms of $K[X]$ are precisely the substitution homomorphisms $X \mapsto aX + b$, $a, b \in K$, $a \neq 0$. The group $\mathrm{Aut}_{K\text{-Alg}} K[X]$ of the K-algebra automorphisms of $K[X]$ is anti-isomorphic and hence isomorphic to the *affine group* $\mathrm{A}_1(K) = K \rtimes K^\times$ of K. (**Remark :** The K-automorphism group of a polynomial algebra $K[X_1, \ldots, X_n]$, $n \geq 2$, is much more complicated and is still an object of active research. For an important subgroup see the next Exercise.)

(b) Let K be a field and L_i, $i \in I$, be a family of homogeneous polynomials of degree 1 in the polynomial algebra $K[Y_j]_{j \in J}$. The substitution homomorphism $K[X_i]_{i \in I} \to K[Y_j]_{j \in J}$,

[2] **Chinese Remainder Theorem.** *The canonical ring homomorphism*

$$\pi : A \longrightarrow \prod_{i=1}^{n} A/\mathfrak{a}_i,\ a \longmapsto (\pi_1(a), \ldots, \pi_n(a)),$$

where $\pi_i : A \to A/\mathfrak{a}_i$, $i = 1, \ldots, n$ *are the residue-class homomorphisms, is surjective and moreover, the kernel* $\mathrm{Ker}\,\pi$ *of* π *is the intersection* $\cap_{i=1}^{n} \mathfrak{a}_i$. *In particular,* π *induces the isomorphism* $A/\cap_{i=1}^{n} \mathfrak{a}_i \xrightarrow{\sim} \prod_{i=1}^{n} A/\mathfrak{a}_i$.

$X_i \mapsto L_i$, $i \in I$, is injective (resp. surjective, bijective) if and only if the L_i, $i \in I$, is linearly independent (resp. a generating system, a basis) over K (resp. of the K-vector space P_1 of all homogeneous polynomials of degree 1 in $K[Y_j]_{j\in J}$) In particular, in the case $I = J$, the substitution endomorphism $K[Y_j]_{j\in J} \to K[Y_j]_{j\in J}$, $Y_j \mapsto L_j$, $j \in J$, is a K-algebra automorphism if and only if its restriction to P_1 is a K-vector space automorphisms of P_1. (**Hint:** With this one can identify the general linear group $\mathrm{GL}_K(P_1) = \mathrm{Aut}_K(P_1)$ with the subgroup of $\mathrm{Aut}_{K\text{-Alg}}P$. Together with the translation automorphisms $X_i \mapsto X_i - c_i$, $c_i \in K$, $i \in I$, they generate the so-called the affine group of the K-algebra automorphisms of P.)

***4.12** **(a)** Let A be an integral domain. Then every A-algebra automorphism $\varphi : A[X] \to A[X]$ is a linear automorphism, i. e. $\varphi(X)$ is a linear polynomial. (**Hint:** We may assume that the constant term of $\varphi(X)$ is 0. Then the ideal $A[X]X$ is φ-invariant.)

(b) Let A be a commutative ring and $\varphi : A[X] \to A[X]$ be an A-algebra endomorphism. Then φ is an automorphism if and only if $\varphi(X) = a + gX$ with $a \in A$ and $g \in A[X]^\times$. (**Hint:** Suppose that φ is of the given form and $\mathfrak{a}$ be the ideal generated by the coefficients other than the constant term. Then $\mathfrak{a}$ is a nilpotent ideal by the following Exercise on the description of units in the polynomial rings[3]. Now, pass to the residue-class ring is $(A/\mathfrak{a})[X]$ and apply the following Exercise[4] See also more detailed Exercises 5.9, 5.10 and 5.12 in Exercise Set 5.)

4.13 (Identity Theorem for Polynomials) Let $F \in A[X_i \mid i \in I]$ be a *non-zero* polynomial in indeterminates X_i, $i \in I$ over an integral domain. If there are subsets $N_i \subseteq A$ with $|N_i| > \deg_{X_i} F$ for all $i \in I$, then $N := \prod_{i\in I} N_i \not\subseteq \mathrm{V}_A(F)$, i. e. there exists an element $x = (x_i)_{i\in I} \in N$ with $F(x) \neq 0$. — In particular, if A is an *infinite* integral domain, then the polynomial function $A^I \to A$, $x \mapsto F(x)$ defined by a non-zero polynomial $F \in A[X_i \mid i \in I]$ is not the zero-function.

(**Proof:** We may assume that I is a finite set and $I = \{1, \cdots, n\}$, $n \in \mathbb{N}$. The case $n = 0$ is trivial. Assume that $n \geq 1$ and that the assertion is proved for $n-1$. Write $F = \sum_{m=0}^{d} F_m(X_1, \ldots, X_{n-1})X_n^m$, where $F_0(X_1, \ldots, X_{n-1}), \ldots, F_d(X_1, \ldots, X_{n-1}) \in A[X_1, \ldots, X_{n-1}]$ and $F_d(X_1, \ldots, X_{n-1}) \neq 0$. Further, since $\deg_{X_i} \leq \deg_{X_i} F < |N_i|$ for all $i = 1, \ldots, n-1$ and hence by induction hypothesis there exists $(x_1, \ldots, x_{n-1}) \in N_1 \times \cdots \times N_{n-1}$ such that $F_d(x_1, \ldots, x_{n-1}) \neq 0$. Therefore $F(x_1, \ldots, x_{n-1}, X_n) \in A[X_n]$ is a non-zero polynomial of degree $d < |N_n|$ in X_n, and hence (since A is an integral domain), there exists $x_n \in N_n$ with $F(x_1, \ldots, x_{n-1}, x_n) \neq 0$. •)

4.14 (Isomorphism type of finite fields) Let $p \in \mathbb{P}$ be a prime number.

(a) Let F be a finite field of characteristic $p > 0$. Then $|F| = |\mathbb{F}_p^n| = p^n$ for some $n \in \mathbb{N}$, $n \geq 1$. (**Hnit:** Since F is a finite dimensional vector space over the prime field $\mathbb{F}_p$, $|F| = |\mathbb{F}_p^n| = p^n$ with $n := \mathrm{Dim}_{\mathbb{F}_p} F$.)

(b) Let $q = p^n$, $n \in \mathbb{N}$, $n \geq 1$. There exists a finite field extension $L\,|\,\mathbb{F}_p$ such that the polynomial $X^q - X$ splits into linear factors in $L[X]$. (**Hint:** This is a very special case of the following very often used important *Kronecker's Theorem*[5].)

[3] **Exercise.** Let A be a commutative ring, $\mathrm{P} := A[X_i \mid i \in I]$ be the polynomial algebra and $F = \sum_{\nu=0}^{m} a_\nu X^\nu \in \mathrm{P}$. Then F is a unit in P if and only if a_0 is a unit in A and all coefficients a_ν, $\nu \neq 0$, of F are nilpotent. (**Hint:** We may assume that $\mathrm{P} = A[X]$. Let $m := \deg F > 0$. It is enough to prove that a_m is nilpotent. But $FG = 1$ with $G = b_0 + \cdots + b_n X^n$, and so by induction $a_m^{i+1} b_{n-i} = 0$ for $i = 0, \ldots, n$. **Variant:** Pass to the ring of fractions A_S, $S := \mathrm{S}(a_m)$, and apply the degree formula.)

[4] Let A be a ring, $\mathfrak{a}$ an ideal in A and let $f : V \to W$ is an A-module homomorphism with W *free* A-module. If $\mathfrak{a}$ is *nilpotent* and if f induces an isomorphism $\overline{f} : V/\mathfrak{a}V \to W/\mathfrak{a}W$, then f itself is an isomorphism.

[5] **Kronecker's Theorem.** *Let $F_1, \ldots, F_m \in K[X]$ be polynomials of positive degrees over the field K. Then there exists a finite field extension $L\,|\,K$ such that the polynomials $F_1, \ldots, F_m$ splits into linear factors in $L[X]$.*

(c) Let L be a field of characteristic$p > 0$ and $q := p^n$, $n \in \mathbb{N}$, $n \geq 1$. Suppose that the polynomial $X^q - X$ splits into linear factors in $L[X]$. Then the zero set $K := \mathrm{V}_L(X^q - X)$ is a subfield of L with $|K| = q$.

(d) Let $q = p^n$, $n \in \mathbb{N}$, $n \geq 1$. There exists a unique field (up to isomorphism) with q elements. (**Proof :** Existence follows from (b) and (c). For the uniqueness we need to show that any two fields K and L with q elements are isomorphic. Since the unit group $K^\times$ of K has order $q-1$, $a^{q-1} = 1$ for every $a \in K$, $a \neq 0$, i. e. $a^q = a$ for every $a \in K$ and hence the polynomial $X^q - X$ splits into linear factors in $K[X]$. The same also holds for the field L. The prime fields of K and L are isomorphic to $\mathbb{F}_p$. Let $k \subseteq K$ be the prime field of K. Since $K^\times$ is cyclic (see Exercise ???), there exists $x \in K^\times$ such that every element in $K^\times$ is a power of x, i. e. $K = k[x]$. Let $\mu := \mu_{x,k} \in k[X]$ be the minimal polynomial of x over k. Then μ divides $X^q - X$ in $k[X]$, since x is a zero of $X^q - X$. As a divisor of $X^q - X$ which splits into linear factors in L, g has a zero $y \in L$. Now, the substitution k-algebra homomorphism $\varepsilon_y : k[X] \to L$, $X \mapsto y$, $\mu \in \operatorname{Ker} \varepsilon_y$. Therefore, $\operatorname{Ker} \varepsilon_y = k[X]\,\mu$ and ε_y induces a k-algebra homomorphism $K = k[x] = k[X]/k[X]\,\mu \to L$ which is injective, since K is a field. Now, it follows that it is bijective on the cardinality assumption. •)

4.15 Let A be an integral domain. Then every subgroup G of $(A^\times, \cdot)$ with $\operatorname{Exp} G \neq 0$ is cyclic and finite. In particular, every finite subgroup of $A^\times$ is cyclic. The multiplicative group of a finite field is cyclic. (**Proof :** We may assume that $A = K$ is a field (replace A by its quotient field). Note that since $\operatorname{Exp} G \neq 0$, $G \subseteq \mathrm{V}_K(X^{\operatorname{Exp} G} - 1)$ and hence G is finite with $|G| \leq \operatorname{Exp} G$. Let $|G| =: m = p_1^{\nu_1} \cdots p_r^{\nu_r}$, $p_1 < p_2 < \cdots < p_r$ prime numbers, $\nu_1, \ldots, \nu_r \in \mathbb{N}^+$, be the prime decomposition of m. For $i = 1, \ldots, r$, put $m_i := p_i^{\nu_i}$ and $n_i := m/m_i$. Then $\gcd(n_1, \ldots, n_r) = 1$ and hence there exist $b_1, \ldots, b_r \in \mathbb{Z}$ with $1 = b_1 n_1 = \cdots + b_r n_r$. For every $x \in G$, $x = x^1 = x^{b_1 n_1 = \cdots + b_r n_r} = \left(x^{b_1 n_1}\right) \cdots \left(x^{b_r n_r}\right) = x_1 \cdots x_r$, where $x_i = \left(x^{b_i n_i}\right)$, $i = 1, \ldots, r$. Note that $x_i^{m_i} = \left(x_i^{b_i n_i}\right)^{m_i} = x^{b_i m} = 1$ (by Lagrange's Theorem) for all $i = 1, \ldots, r$. Moreover, the map

$$G \longrightarrow \prod_{i=1}^{r} \mathrm{V}_K(X^{m_i} - 1)\,, \quad x \longmapsto (x_1, \ldots, x_r)\,,$$

is injective and hence bijective, since

$$|G| \;\leq\; |\prod_{i=1}^{r} \mathrm{V}_K(X^{m_i} - 1) = \prod_{i=1}^{r} |\mathrm{V}_K(X^{m_i} - 1)| \;\leq\; \prod_{i=1}^{r} m_i \;= m = |G| = m_1 \cdots m_r\,.$$

In particular,
$$\left|\mathrm{V}_K\left(X^{m_i/p_i} - 1\right)\right| \;\leq\; m_i/p_i < m_i = m_i \quad \text{for every } \; i = 1, \ldots, r.$$

Now, since
$$\left|\mathrm{V}_K\left(X^{m_i/p_i} - 1\right)\right| \;\leq\; m_i/p_i \;<\; m_i = \left|\mathrm{V}_K\left(X^{m_i/p_i} - 1\right)\right|\,,$$

we have
$$|\mathrm{V}_K\left(X^{m_i/p_i} - 1\right) \subsetneq \mathrm{V}_K(X^{m_i} - 1) \text{ for every } i = 1, \ldots, r.$$

Therefore there exist $y_1, \ldots, y_r \in G$ with $\operatorname{Ord} y_i = m_i$ for every $i = 1, \ldots, r$. Then $\operatorname{Ord}(y_1 \cdots y_r) = (\operatorname{Ord} y_1) \cdots (\operatorname{Ord} y_r) = m_1 \cdots m_r = m = |G|$ and hence $y = y_1 \cdots y_r$ is a primitive element of G, i. e. G is cyclic. •)

4.16 Let $\mathbb{F}_q$ be a finite field with q elements and let $L \,|\, \mathbb{F}_q$ a finite field extension of $\mathbb{F}_q$.

(a) For $x \in L^\times$ with $\operatorname{Ord}_{L^\times} x = d$, we have $\deg \mu_{x,\mathbb{F}_q} = \operatorname{Dim}_{\mathbb{F}_q} \mathbb{F}_q[x] = \operatorname{Ord}_{(\mathbb{Z}/Zd)^\times} q$.

(b) Let $x \in L$ and $s := \deg \mu_{x,\mathbb{F}_q}$. Then s is the smallest positive natural number with

$$x = x^{q^s} \qquad \text{and} \qquad \mu_{x,\mathbb{F}_q} = \prod_{i=0}^{s-1} (X - x^{q^i}).$$

(**Hint :** Note that the group $\operatorname{Aut}_{\mathbb{F}_q\text{-alg}} \mathbb{F}_q[x]$ is cyclic with generator $ff : \mathbb{F}_q[x] \to \mathbb{F}_q[x]$, $x \mapsto x^q$. The coefficients of the polynomial on the right-hand side are invariant under the generator of the $\operatorname{Aut}_{\mathbb{F}_q\text{-alg}} \mathbb{F}_q[x]$.)

4.17 Let $\mathbb{F}_q$ be a finite field with q elements. Let $F = a_0 + a_1 X + \cdots + a_{q-2} X^{q-2} \in \mathbb{F}_q[X]$ with $\deg \mathbb{F} = q - 2$. Find the number of distinct zeros of F in $\mathbb{F}_q$, other than 0, i. e. the cardinality $|\mathrm{V}_{\mathbb{F}_q}(F)\smallsetminus\{0\}|$. (**Hint:** Let $f:\mathbb{F}_q^{q-1}\to\mathbb{F}_q^{q-1}$ be the $\mathbb{F}_q$-linear map defined by the *circulant* matrix

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{q-2}\\ a_1 & a_2 & \cdots & a_0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{q-2} & a_0 & \cdots & a_{q-3}\end{pmatrix}\in \mathrm{M}_{q-1}(\mathbb{F}_q).$$

Then $|\mathrm{V}_{\mathbb{F}_q}(F)\smallsetminus\{0\}|=q-1-\mathrm{Rank}_{F_q} f$. For a proof of this consider the product matrix $\mathfrak{A}\cdot\mathfrak{V}$, where $\mathfrak{V}:=\mathfrak{V}(x_0,x_1,\ldots,x_{q-2})=(x_j^i)_{0\le i,\,j\le q-2}$ is the Vandermonde's matrix of the non-zero elements $x_0,x_1,\ldots,x_{q-2}$ of $\mathbb{F}_q$, and $x_j^{q-1}=1$ for all $j=0,\ldots,q-2$.

***4.18** (Polynomial functions) Let A be a commutative ring, I a (finite) indexed set and B be a commutative A-algebra. For a polynomial $F\in A[X_i \mid i\in I]$, the B-valued function $B^I\to B$, $x\mapsto F(x)$, is called the polynomial function (over A) (which is again denoted by F) corresponding to the polynomial F.

(a) The canonical map $\varepsilon : A[X_i \mid i\in I]\to \mathrm{Maps}\,(B^I,B)$ which maps polynomials to polynomial functions is an A-algebra homomorphism. Its image $\mathrm{Img}\,\varepsilon$ is called the A-algebra of the polynomial functions (over A) on B^I. The polynomial functions corresponding to the polynomial X_j, $j\in I$, is the canonical projection $\pi_j : B^I\to B$ onto the j-component. The set of projections π_j, $j\in I$, form an A-algebra generating system for A-algebra of the polynomial functions on B^I.

(b) If A is a finite ring $\neq 0$, then $\varepsilon : A[X]\to \mathrm{Maps}(A,A)$ is not injective.

(c) If I is an indexed set and if A is an *infinite* integral domain, then the canonical A-algebra homomorphism

$$\varepsilon : A[X_i \mid i\in I]\longrightarrow \mathrm{Maps}(A^I,A),\quad F\longmapsto (x\mapsto F(x)),$$

is injective. (**Hint:** Use the Identity Theorem for Polynomials, see Exercise 4.13.)

(d) Suppose that $A\neq 0$. Then $\varepsilon : A[X]\to \mathrm{Maps}(A,A)$ is surjective if and only if A is a finite field. Moreover, in this case, the kernel of ε is generated by $X^q-X=(X^{q-1}-1)X$, where $q:=|A|$.

****4.19** Let A be a noetherian commutative ring and let $\varepsilon : A[X]\to A^A$ be the canonical A-algebra homomorphism.

(a) If $\mathrm{Ker}\,\varepsilon$ contains a monic polynomial, then A is a finite ring. (**Hint:** Suppose on the contrary that A is infinite. Then by passing to the residue-class ring modulo an ideal in A which is maximal in the set of ideals with infinite residue-class rings, we may further assume that all residue-class rings of A are finite. There exist elements $a,b\in A$ with $a\neq 0$, $b\neq 0$, $ab=0$. With A/Aa and A/Ab, the residue-class ring $A/Aab=A$ is also finite. — **Remark:** Interesting to prove that the map ε is *not* injective if and only if there exists a maximal ideal $\mathfrak{m}$ in A and an element $a\neq 0$ with $a\cdot\mathfrak{m}=0$ and the residue-class field $A/\mathfrak{m}$ is finite.)

(b) (P. Samuel) For every $n\in\mathbb{N}^+$, there exist *only* finitely many ideals $\mathfrak{a}$ in A with $|A/\mathfrak{a}|\le n$ (**Hint:** Let $f:=\prod_{i=0}^{n-1}(X^n-X^i)$ and $\mathfrak{c}:=\cap\{\mathfrak{a}\mid \mathfrak{a}\in\mathfrak{J}(A)$ with $|A/\mathfrak{a}|\le n\}$. Then $f(x)\in\mathfrak{c}$ for all $x\in A$ and hence by the part (a) $A/\mathfrak{c}$ is finite. — **Remark:** The number theoretic function $\mathfrak{z}_A:\mathbb{N}_+\to\mathbb{Z}$, $n\mapsto\mathfrak{z}_A(n):=$ the number of ideals $\mathfrak{a}$ in A with $|A/\mathfrak{a}|=n$, is called the Dedekind's function of A. It is multiplicative (Proof!). The associated Dirichlet's series

$$\zeta_A=\sum_{n=1}^{\infty}\frac{\mathfrak{z}_A(n)}{n^s}$$

is a complex-analytic function (in s) and is called the Dedekind's zeta function ζ_A von A. For $A=\mathbb{Z}$, $\mathfrak{z}_{\mathbb{Z}}(n)=1$ for all $n\in\mathbb{N}^+$); and hence $\zeta_{\mathbb{Z}}$ is the Riemann's zeta function,.)

(c) If V is a noetherian module over A and if $n \in \mathbb{N}_+$, then there exist finitely many submodules of W of V with $|V/W| \leq n$.

(d) If B is a (not necessarily commutative) finitely generated A-algebra, then there exists only finitely many (left-, right-, resp. two-sided) ideals $\mathfrak{b}$ in B with $|B/\mathfrak{b}| \leq n$.

4.20 Let K be an *infinite* field and V be a K-vector space.

(a) Every linearly independent (over K) of K-linear forms $f_i \in V^* = \mathrm{Hom}_K(V,K)$, $i \in I$, is *algebraically independent*[6] in the K-algebra K^V of all K-valued functions on V.

(**Hint :** One can reduce to the case that V is finite dimensional and use the following Exercise from Linear Algebra[7] — Often K-subalgebra of K^V (of all K-valued functions on V), generated by the K-linear forms $V \to K$ is called the K-algebra of polynomial functions on V. For a *finite* index set I and the finite dimensional K-vetor space $V = K^I$, this coincides with the usual definition, See Exercise 4.18. — **Remark :** More generally, for every free A-module over the commutative ring A, the A-algebra of polynomial functions on V is the A-subalgebra of the A-algebra A^V of all A-valued functions on V generated by the A-linear forms $f \in V^* := \mathrm{Hom}_A(V,A)$. If x_i, $i \in I$, is a (finite) A-basis of V, then the A-algebra of polynomial functions on V is generated by the coordinate functions $x_i^* : V \to A$, $i \in I$. Using the A-module isomorphism $\psi : A^I \to V$, $e_i \mapsto x_i$, we get the A-algebra isomorphism $\Phi : A^V \to A^{A^I} = \mathrm{Maps}(A^I, A)$ with $f \mapsto f \circ \psi$. In particular, the restriction of Φ is an A-algebra isomorphism of the A-algebra of polynomial functions on V and the A-algebra of the polynomial function on A^I. Therefore it is enough to study the A-algebra of polynomial functions on A^I. See Exercise 4.18.)

(b) Let $L|K$ be a field extension. A family $h_i \in \mathrm{Hom}_K(V,L)$, $i \in I$, of K-linear maps $V \to L$ which is linearly independent over L is also algebraically independent (over L) in the L-algebra L^V. In particular, if B is a K-algebra, then the subset $\mathrm{Hom}_{K\text{-alg}}(B,L)$ of $\mathrm{Hom}_K(B,L)$ is algebraically independent.

4.21 Let A be a K-algebra over the field K and let $x \in A^*$ be a non-zero divisor which is algebraic over over K. Then $x \in A^\times$ is a unit A and $x^{-1} \in K[x]$. (**Hint :** The left multiplication $\lambda_x : K[x] \to K[x]$, $y \mapsto xy$, by x on the finite K-algebra $K[x]$ is injective and hence bijective.) Determine the minimal polynomial $\mu_{x^{-1},K}$ of x^{-1} over K by using the minimal polynomial $\mu_{x,K}$ of x over K. (The constant term of $\mu_{x,K}$ is $\neq 0$.) In particular, if an integral domain A is algebraic over a field K, then A is a field.

4.22 Let K be a field and $n \in \mathbb{N}$. Consider the finite product K-algebra K^n of dimension n.

(a) The minimal polynomial $\mu_{x,K}$ of $x = (x_1, \ldots, x_n) \in K^n$ over K is $(X - x_{i_1}) \cdots (X - x_{i_r})$, where $x_{i_1}, \ldots, x_{i_r}$ are the distinct components of x. What is the characteristic polynomial $\chi_x := \chi_{\lambda_x}$, where $\lambda_x : K^n \to K^n$, $y \mapsto xy$, is the left multiplication on K^n by x (which is clearly K-linear, i. e. $\lambda_x \in \mathrm{End}_K K^n$).

(b) An element $x = (x_1, \ldots, x_n) \in K^n$ generates the K-algebra K^n if and only if the components $x_1, \ldots, x_n$ of x are pairwise distinct. (**Hint :** Apply the part (a), or Use Vandermonde's matrix to check that the elements $1, x, \ldots, x^{n-1} \in K^n$ are linearly independent over K.)

[6] **Algebraically independent family in the A-algebra.** Recall that a family of elements $x := (x_i)_{i \in I}$, in the A-algebra B over the commutative ring A are algebraically independent over A if the substitution A-algebra homomorphism $\varepsilon_x : A[X_i \mid i \in I] \to B$, $X_i \mapsto x_i$, $i \in I$, is injective, i. e. $\mathrm{Ker}\,\varepsilon_x = 0$.

[7] **Exercise.** Let V be a K-vector space and let $f_1, \ldots, f_n \in V^*$ be linear forms on V. Let $f : V \to K^n$ be the homomorphism defined by $f(x) := \big(f_1(x), \ldots, f_n(x)\big)$. Then show that $\mathrm{Dim}_K(Kf_1 + \cdots + Kf_n) = \mathrm{Dim}_K(\mathrm{Im}\, f)$. In particular, $f_1, \ldots, f_n$ are linearly independent if and only if the homomorphism f is surjective. (**Hint :** Note that $\mathrm{Img}\, f$ is finite dimensional and hence $\mathrm{Rank}_K f = \mathrm{Rank}_K f^* = \mathrm{Dim}_K(Kf_1 + \cdots + Kf_n)$.)

4.23 Let $f \in \mathbb{Z}[X]$ be a polynomial of positive degree. Show that there are infinitely many prime numbers p such that the polynomial f has a zero in $\mathbb{Z}/\mathbb{Z}p$. It is even the non-zero values $\{f(x) \mid x \in \mathbb{N}^+\} \smallsetminus \{0\}$, altogether have infinitely many prime divisors. But not all $|f(x)|$, $x \in \mathbb{N}^+$ are prime numbers. In particular, there are infinitely many prime numbers $p \in \mathbb{P}$ such that $\mathrm{V}_{(\mathbb{Z}/\mathbb{Z}p)}(f) \neq \emptyset$. (**Hint :** Using *Taylor's expansion*, for $x \in \mathbb{N}^+$, there exists an integer $y \in \mathbb{Z}$ such that $f\left(x+f(x)^2\right) = f(x)+f(x)^2y = f(x)\,(1+f(x)y)$. — **Remark :** Very important consequence of this simple Exercise : *For $n \in \mathbb{N}^+$, there are infinitely many primes p with $p \equiv 1\,(\mathrm{mod}\, n)$.* For a proof use the above Exercise for $f = \Phi_n \in \mathbb{Z}[X]$ and the following observation[8]. Note that this is a very special case of the following well-known[9].)

4.24 Let K be an *infinite* field and let $L|K$, be a field extension, $f \in K[X_1,\ldots,X_n]$ be a polynomial and let

$$\mathcal{E} \ : \quad a_{i1}x_1+\cdots+a_{in}x_n = b_i\,, \quad i=1,\ldots,m\,,$$

be a system of linear equations with coefficients $a_{ij}, b_i \in K$. Suppose that the system $\mathcal{E}$ has a solution $(x_1,\ldots,x_n) \in L^n$ with $f(x_1,\ldots,x_n) \neq 0$. Then show that the system $\mathcal{E}$ also has a solution $(y_1,\ldots,y_n) \in K^n$ with $f(y_1,\ldots,y_n) \neq 0$. (**Hint :** Let $n-r$ be the rank of the system $\mathcal{E}$. The entire solution spaces $\mathrm{L}_K(\mathcal{E})$ (over K) and $\mathrm{L}_L(\mathcal{E})$ (over L) of the system $\mathcal{E}$ are determined by a solution $x=(x_1,\ldots,x_n) \in K^n$ and solutions $x^{(\rho)} = (x_1^{(\rho)},\ldots,x_n^{(\rho)}) \in K^n$, $\rho = 1,\ldots,r$, which generate the solution spaces $\mathrm{L}_K(\mathcal{E}_0)$ and $\mathrm{L}_L(\mathcal{E}_0)$ of the corresponding homogenous system $\mathcal{E}_0$ over K as well as over L. Substitute this resulting parametrization of the solution space $\mathrm{L}_L(\mathcal{E})$ in the polynomial f and use the Identity Theorem.)

4.25 Let A be a commutative ring $\neq 0$.

(a) (G-adic expansion) Let $G \in A[X]$ be a monic polynomial of degree $m \geq 1$. For every polynomial $F \neq 0$, there exist unique polynomials $P_0,\ldots,P_r$ with $P_r \neq 0$ and

$$F = P_0+P_1G+\cdots+P_rG^r\,, \ \ P_i = 0 \quad \text{or} \quad \deg P_i < m\,, \ \ i=0,\ldots r\,.$$

(**Remark :** This expansion is the analog of the g-adic expansion of natural numbers, $g \in \mathbb{N}$, $g \geq 2$, and is called the G-adic expansion of F. For $G = X-c$ of degree 1, this is handled in the *Taylor-expansion*[10] of F in c.)

(b) Let $F \in A[X]$ be polynomial of degree n and $c \in S$. The coefficients $b_0,\ldots,b_{n-1}$ of the quotient $Q = b_{n-1}+b_{n-2}X+\cdots+b_0X^{n-1}$ in the representation $F = F(c)+Q\cdot(X-c)$ are the values $F_0(c),\ldots,F_{n-1}(c)$ in the *Horner's Scheme* for computation of $F(c) = F_n(c)$.

— **Horner's Scheme.** For the calculation of the values of a polynomial in one variable

$$F = a_0+a_1X+\cdots+a_nX^n \in A[X]$$

at $a \in A$, apply the so-called Horner's-Scheme. For this recursively define a sequence of polynomials :

$$F_0 = a_n\,, \ F_1 = a_{n-1}+F_0X = a_{n-1}+a_nX\,, \ \ \ldots\ldots, \ \ F_{k+1} = a_{n-k-1}+F_kX = a_{n-k-1}+\cdots+a_{n-1}X^k+a_nX^{k+1}\,,$$

[8] **Cyclotomic Extensions.** Let $n \in \mathbb{N}^+$ and $p \in \mathbb{P}$ be a prime number with $\gcd(p,n)=1$. Further, let $\zeta_n \in \mathbb{C}$ be a primitive n-roots on unity, i. e. ζ_n is a generator of the (multiplicative) cyclic group $\mu_n := \mathrm{V}_{\mathbb{C}}(X^n-1) \subseteq \mathbb{C}^\times$,see Exercise 4.?? $\Phi_n := \mu_{\zeta_n,\mathbb{Q}}$ be the minimal polynomial of ζ_n over $\mathbb{Q}$ and $\mathbb{Q}^{(n)} := \mathbb{Q}[X]/\langle\Phi_n\rangle = \mathbb{Q}(\mu_n)$ (= the splitting field of X^n-1 over $\mathbb{Q}$). Then there is an $a \in \mathbb{Z}$ with $\Phi_n(a) \equiv 0\,(\mathrm{mod}\, p)$ if and only if $\mathrm{Ord}_n\, p := \mathrm{Ord}_{(\mathbb{Z}/\mathbb{Z}n)^\times}\, p = 1$, i. e. $p \equiv 1\,(\mathrm{mod}\, n)$. For proof use $\mathrm{Aut}_{\mathbb{Q}\text{-alg}}\, \mathbb{Q}^{(n)} \subseteq (\mathbb{Z}/\mathbb{Z}n)^\times$.

[9] **Dirichlet's Theorem.** *Let n, $m \in \mathbb{N}^+$ be relatively prime natural numbers. then there exist infinitely many prime numbers $p \in \mathbb{P}$ with $p \equiv m\,(\mathrm{mod}\, n)$.*

[10] **Taylor's expansion of F at a.** If $a \in A$, $F \in A[X]$, $F \neq 0$ and $\deg F = n \in \mathbb{N}$, then by the repeated application of the division with remainder $F = Q(X-a)+F(a)$, $Q \in A[X]$, we get the representation :

$$F = a_n(X-a)^n+a_{n-1}(X-a)^{n-1}+\cdots+a_1(X-a)+a_0$$

with uniquely determined coefficients $a_0,\ldots,a_n \in A$, $a_n \neq 0$, is the so-called Taylor's expansion of F at a.

$$\ldots\ldots\ \ldots\ \ldots,\ F_n = a_0 + F_{n-1}X = F,$$

and hence the value $F(a) = F_n(a)$ is determined by the recursion scheme

$$F_0(a) = a_n\,,\quad F_{k+1}(a) = a_{n-k-1} + F_k(a)\,a\,,\quad k = 0,\ldots,n-1.$$

This scheme can also be used to determine the value $F(a)$ for an element a in an arbitrary A-algebra.

(**Remark:** Applying this process to the polynomial Q instead of F successively one can obtain the coefficients in the Taylor-expansion of F at c.– What are the expansions of the polynomial $F = X^4 - 3X^3 + 5X^2 - X + 2 \in \mathbb{Z}[X]$ at $c = 2$ and at $c = -1$.)

4.26 (Tschirnhaus[11]-Transformation) Let $A \neq 0$ be a commutative ring and $G = c_0 + c_1X + \cdots + c_{n-1}X^{n-1} + X^n \in A[X]$ be a monic polynomial of degree $n \in \mathbb{N}^+$. Assume that n is a unit in A. In the free residue-class A-algebra $A[x] = A[X]/(G)$ of rank n, the element $\widetilde{x} := x + \frac{1}{n}c_{n-1}$ satisfies the equation $\widetilde{c}_0 + \cdots + \widetilde{c}_{n-2}\widetilde{x}^{\,n-2} + \widetilde{x}^{\,n} = 0$ with coefficients $\widetilde{c}_i$, $i = n-2,\ldots,0$, in A. In particular, $A[x] = A[\widetilde{x}] \xleftarrow{\sim} A[X]/(\widetilde{G})$, where the coefficient of X^{n-1} in the monic polynomial $\widetilde{G} := \widetilde{c}_0 + \cdots + \widetilde{c}_{n-2}X^{n-2} + X^n \in A[X]$ is 0. (The polynomial $\widetilde{G}$ obtained from the polynomial G by the (linear) Tschirnhaus(en)-Transformation.)

4.27 (Kronecker's[12] method of indeterminates) Very often used method ("Unbestimmenten-Methode") used to prove algebraic relations among elements $x_1,\ldots,x_n$ in a ring B, look for a solution of the analog of the problem for the *indeterminates* $X_1,\ldots,X_n$ in the polynomial ring $A[X_1,\ldots,X_n]$ and then by using a ring homomorphism and the substitution homomorphism $\varepsilon_x : A[X,\ldots,X_n] \to B$, $X_i \mapsto x_i$, $i = 1,\ldots,n$, to pass on the result to the ring B. The advantage is that one can facilitate the calculation in the polynomial algebra $A[X_1,\ldots,X_n]$ which has special properties. For example:

(a) For arbitrary square matrices $\mathfrak{A},\ \mathfrak{B} \in \mathrm{M}_n(B)$ over a commutative ring B, we have

$$\mathrm{Adj}\,(\mathfrak{A}\mathfrak{B}) = (\mathrm{Adj}\,\mathfrak{B})(\mathrm{Adj}\,\mathfrak{A})\,..$$

(For a proof we may assume that $B = \mathbb{Z}[X_{ij}, Y_{ij} \mid i,j \in \{1,\ldots,n\}]$ and $\mathfrak{A} = \big(X_{ij}\big)$ and $\mathfrak{B} = \big(Y_{ij}\big)$. Then the determinant Det $\mathfrak{A}$ is a homogeneous polynomial of degree n in X_{ij}, $1 \le i,j \le n$ and $\neq 0$ (as this can be seen by substituting the unit matrix) and hence is a non-zero divisor in the integral domain. The same also holds for the determinant Det $\mathfrak{B}$. Now the formula follows from the *Standard Determinant Adjoint Formula*[13])

(b) Let K be an *infinite* field, $L|K$ is a field extension of K and $\mathfrak{A}$, $\mathfrak{B} \in \mathrm{M}_n(K)$ be square matrices over K. Then $\mathfrak{A}$ and $\mathfrak{B}$ are similar over K if and only if $\mathfrak{A}$ and $\mathfrak{B}$ are similar over L. (Use Kronecker's method of indeterminates and the Exercise 4.16. — This result also holds for finite fields K.)

[11] Walther von Tschirnhaus (1651-1708) was a German mathematician, physicist, physician, and philosopher, who introduced the *Tschirnhaus transformation*. Some considered him the inventor of European porcelain, but others claim porcelain had been made by English manufacturers at an even earlier date.

[12] Leopold Kronecker (1823-1891) was a German mathematician who worked on number theory, algebra and logic. He criticized Georg Cantor's work on set theory, and was quoted as having said,"Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk" ("God made the integers, all else is the work of man"). See [Kronecker, L.: Grundzüge einer arithmetischen Theorie der algebraischen Grössen, *J. Reine Angew. Math.* **92** (1882), pp. 1–122]

[13] **Standard Determinant Adjoint Formula.** For every square matrix $\mathfrak{A} \in \mathrm{M}_n(B)$ over a commutative ring B, we have $\mathfrak{A}\cdot(\mathrm{Adj}\,\mathfrak{A}) = (\mathrm{Adj}\,\mathfrak{A})\cdot\mathfrak{A} = (\mathrm{Det}\ \mathfrak{A})\cdot\mathfrak{E}$.