Commutative Algebra

lecture 13: Normalization

Misha Verbitsky

http://verbit.ru/IMPA/CA-2022/

IMPA, sala 232

January 31, 2022

Integral closure (reminder)

DEFINITION: Let $A \subset B$ be rings. An element $b \in B$ is called **integral over A** if the subring $A[b] = A \cdot \langle 1, b, b^2, b^3, ... \rangle$, generated by b and A, is finitely generated as A-module.

DEFINITION: Let $A \subset B$ be rings. The set of all elements in B which are integral over A is called **the integral closure of A in B**.

DEFINITION: Let A be the ring without zero divisors, and $k(A)$ its field of fractions. The set of all elements $a \in k(A)$ which are integral over A is called **the integral closure of A**. A ring A is called **integrally closed** if A coincides with its interal closure in $k(A)$.

REMARK: The integral closure is a ring.

DEFINITION: An affine variety X is called **normal** if its irreducible components X_i don't intersect, and the ring of functions $\mathcal{O}_{X_i}$ for each of these irreducible components is integrally closed.

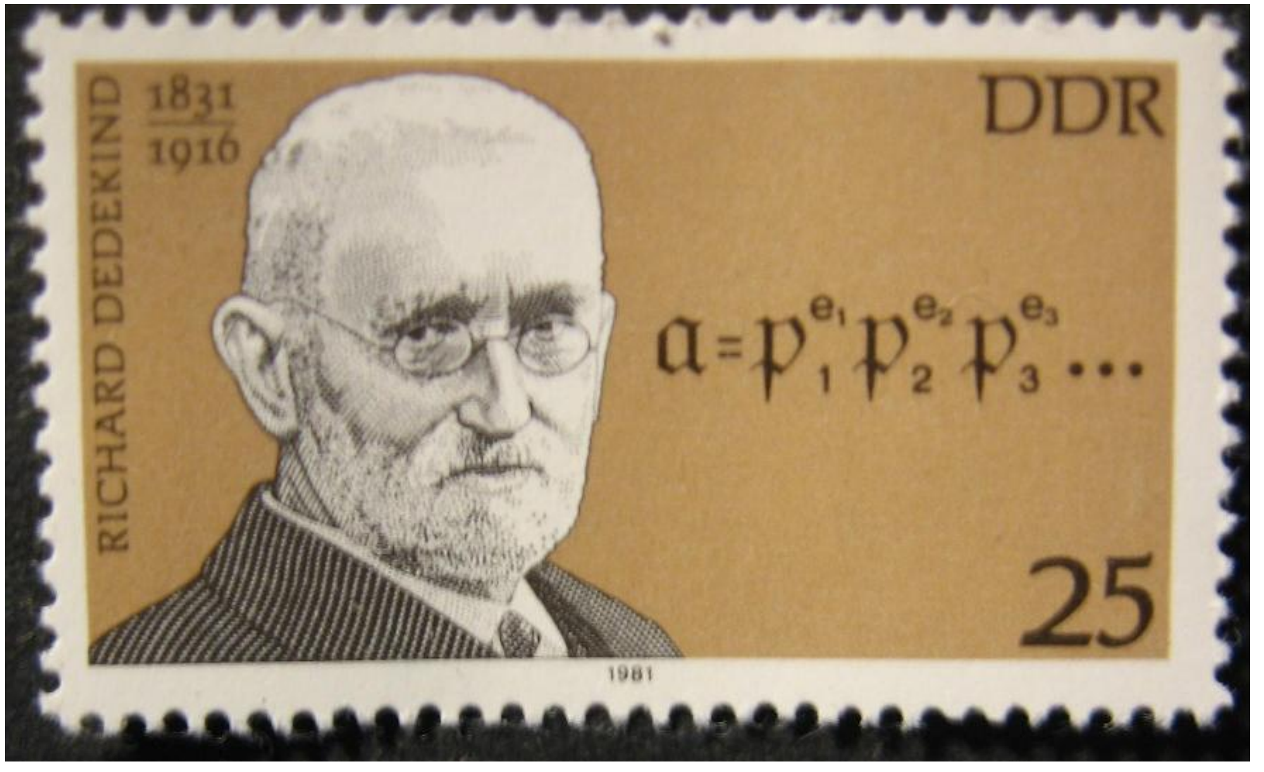
REMARK: Equivalently, **X is normal if any finite, birational morphism $Y \longrightarrow X$ is an isomorphism.**

PROPOSITION: Let A be a factorial ring. Then it is integrally closed.

Ernst Kummer

Ernst Eduard Kummer (1810-1893)

Richard Dedekind



Richard Dedekind (1831 - 1916)

Gauss lemma

EXERCISE: Let R be a ring without zero divisors. **Prove that the polynomial ring $R[t]$ has no zero divisors.**

THEOREM: ("Gauss lemma")
Let R be a factorial ring. **Then the ring of polynomials $R[t]$ is also factorial.**

Proof: See the next slide.

DEFINITION: Let R be a factorial ring. A polynomial $P(t) \in R[t]$ is called **primitive** if the greatest common divisor of its coefficients is 1.

Lemma 1: Let $P_1, P_2 \in R[t]$ be primitive polynomials. **Then their product is also primitive**.

Proof: Let $p \in R$ be a prime. Since the polynomials P_1, P_2 are primitive, they are non-zero modulo p. Since the ring $R/(p)$ has no zero divisors, **the product P_1P_2 is non-zero in $R/(p)[t]$,** hence the greatest common divisor of the coefficients of P_1P_2 is not divisible by p. ■

Irreducibility of polynomials in $R[t]$ and $K[t]$

Lemma 1: Let $P_1, P_2 \in R[t]$ be primitive polynomials. **Then their product is also primitive**.

Lemma 2: Let R be a factorial ring, and K its fraction field. **Then any primitive polynomial $P \in R[t]$, which is irreducible in $R[t]$, is also irreducible in $K[t]$.**

Proof: Assume that P is decomposable in $K[t]$. Then $rP = P_1 P_2$, where $P_1, P_2 \in R[t]$ and $r \in R$. Let s_1, s_2 be the greatest common divisors of the coefficients of P_1, P_2. Then $rP = s_1 s_2 P_1' P_2'$, and P_1', P_2' are primitive. In this case $P_1' P_2'$ is primitive (Lemma 1), hence the greatest common divisor of the coefficients of $s_1 s_2 P_1' P_2'$ is $s_1 s_2$. Since P is also primitive, the greatest common divisor of the coefficients of $rP = s_1 s_2 P_1' P_2'$ is r. **Then $\frac{r}{s_1 s_2}$ is invertible, and P is decomposable in $R[t]$.** ■

Gauss lemma (proof)

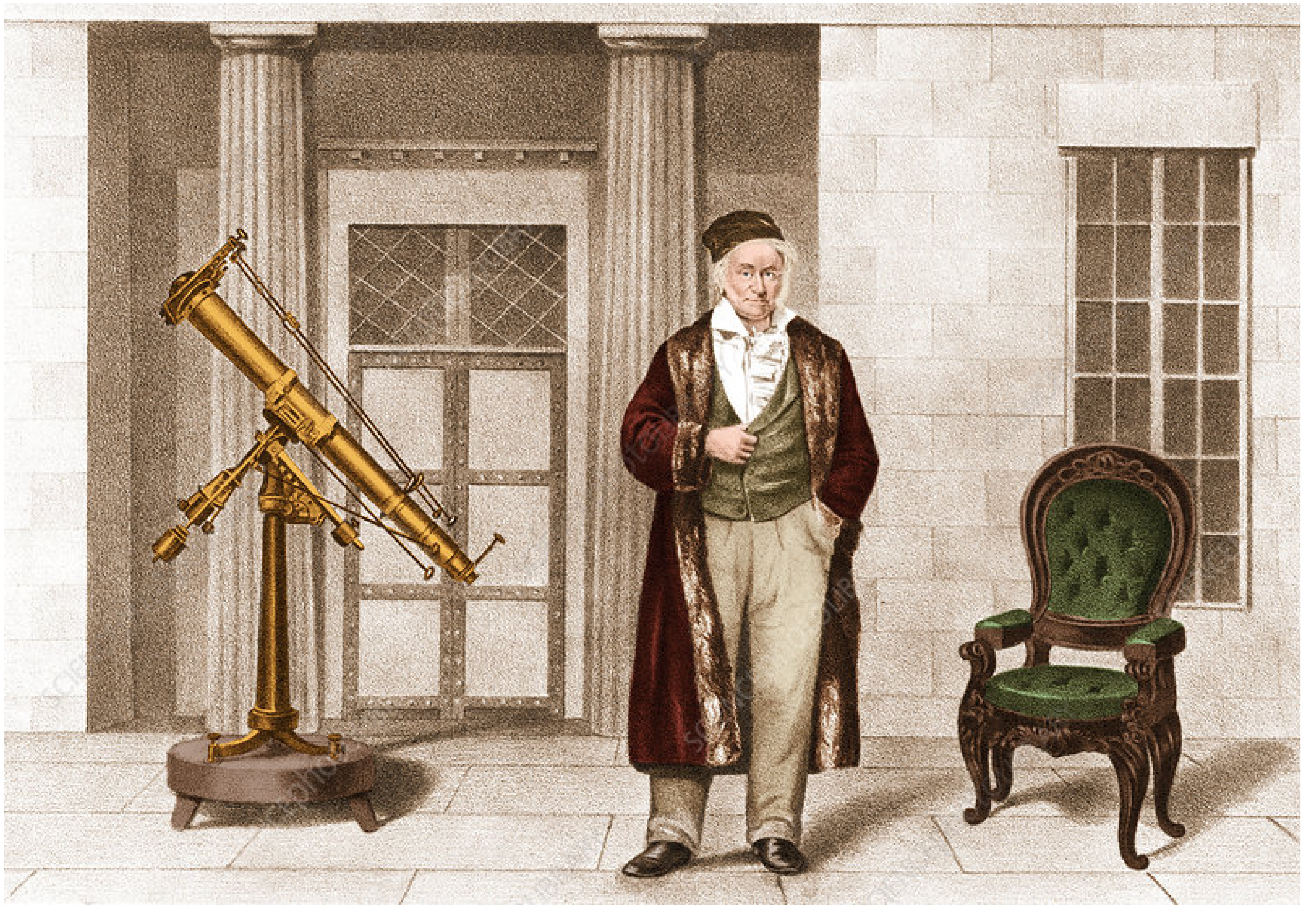
THEOREM: ("Gauss lemma")
Let R be a factorial ring. **Then the ring of polynomials $R[t]$ is also factorial.**

Proof: Let K be the fraction field of R. The ring $K[t]$ is factorial, because it is Euclidean (handout 3). Lemma 2 implies that a prime decomposition of a primitive polynomial $P(t) \in R[t]$ is uniquely determined by its prime decomposition in $K[t]$, hence it is unique. A non-primitive polynomial is decomposed as a product of the greatest common divisor of its coefficients and a primitive polynomial, hence its prime decomposition is also unique. ■

COROLLARY: The affine space $\mathbb{C}^n$ is a normal variety. Moreover, **for any variety X with factorial ring $\mathcal{O}_X$ of regular functions, the product $X \times \mathbb{C}^n$ is also normal.**

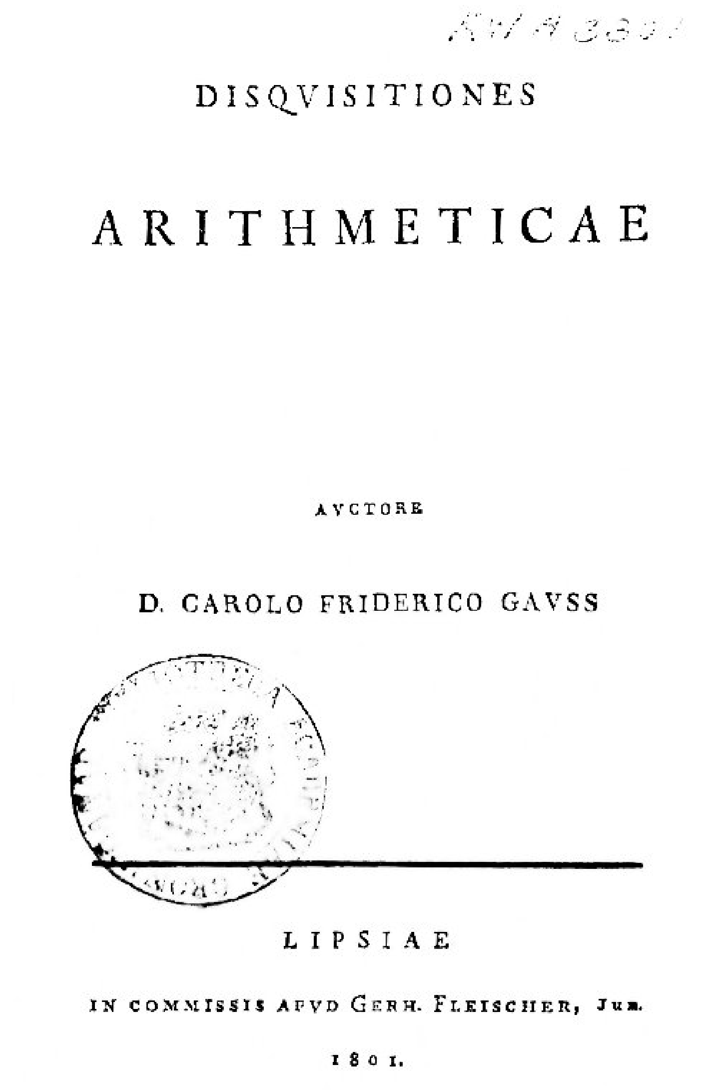
Proof: As we have shown previously, $\mathcal{O}_{X\times\mathbb{C}^n} = \mathcal{O}_X \otimes_{\mathbb{C}} \mathbb{C}[t_1, ..., t_n] = \mathcal{O}_X[t_1, ..., t_n]$. This ring is factorial by Gauss lemma. ■

Carl Friedrich Gauss



Carl Friedrich Gauss (1777 - 1855)

Disquisitiones Arithmeticae


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, IVN.

1801.

"Disquisitiones Arithmeticae",
written by Gauss in 1798, in Latin, when he was 21.
This book contains "Gauss Lemma".

Finiteness of integral closure

THEOREM: Let A be an integrally closed Noetherian ring, $[K : k(A)]$ a finite extension of its field of fractions, and B the integral closure of A in K. **Then B is finitely generated as an A-module.**

Proof. Step1: For any $b \in B$, denote by $L_b : \ K \longrightarrow K$ the map of multiplication by b. Consider L_b as a $k(A)$-linear endomorphism of the finite-dimensional space K over $k(A)$, and define **the trace** $\operatorname{Tr}(b) := \operatorname{Tr}(L_b)$. Clearly $\operatorname{Tr}(b) = \frac{d}{dt}\det(tId_K - tL_b)(0)$. Since b is a root of monic polynomial, the operator $L_b \in \operatorname{End}_k(K)$ can be represented by a matrix with coefficients in A. Therefore, for any $b \in B$ integral over A, **the trace of b is integral over A**.

Step 2: The bilinear symmetric form $x, y \longrightarrow \operatorname{Tr}(xy)$ is non-degenerate. Indeed, $\operatorname{Tr}(xx^{-1}) = \dim_{k(A)} K$, and $\operatorname{char} k(A) = 0$.

Step 3: Choose a basis $e_1, ..., e_n$ in the $k(A)$-vector space K. Let $P_i(t) \in k(A)[t]$ be the minimal polynomials of e_i. Write $P_i(t) = A_i t^{n_i} + \sum_{j<n_i} a_{ij} t^j$, where $A_i, a_{ij} \in A$. Then $A_i e_i$ is a root of a monic polynomial $\tilde{P}_i(t) = t^{n_i} + \sum_{j<n_i} A^{n_i - j} a_{ij} t^j$. **This proves that the basis $e_1, ..., e_n$ in $K : k(A)$ can be chosen such that all e_i are integral over A,** that is, **all e_i belong to B.**

Finiteness of integral closure (2)

Step 4: Let $e_i^* \in K$ be the dual basis with respect to the form Tr, with $\operatorname{Tr}(e_i^* e_j) = \delta_{ij}$. Consider the A-module $M \subset K$ generated by e_i^*. Clearly, $M := \{b \in K \ | \ \operatorname{Tr}(be_i) \in A\}$.

Step 5: For any $b \in B$, the trace $\operatorname{Tr}(be_i)$ belongs to A, because be_i is integral over A (Step 1). Then $B \subset M$, and **B is a submodule of a finitely generated A-module M.** Since A is Noetherian, B is finitely generated as A-module. ■

COROLLARY: Let B be a ring over $\mathbb{C}$. Assume that there exists an injective ring morphism from $A = \mathbb{C}[x_1, ..., x_k]$ to B such that B is finitely generated as an A-module. **Then its integral closure $\hat{B}$ is a finitely generated A-module**. In particlular, **$\hat{B}$ is a finitely generated ring.**

Proof: Since A is factorial, it is integrally closed, and the previous theorem applies. ■

DEFINITION: Let X be an affine variety, and $\hat{A}$ the integral closure of its ring of regular functions. Assume that $\hat{A}$ is a finitely generated ring. Then $\tilde{X} := \operatorname{Spec}(\hat{A})$ is called **the normalization of X**.

REMARK: Using Noether's normalization lemma, **we shall prove that $\hat{A}$ is always finitely generated.**