Rings of Integers and Beyond
(Meeting Notes)

Felix Gotti

April 30, 2026

Contents

Introduction

Number Fields and their Rings of Integers

A subfield K of $\mathbb{C}$ is called an *algebraic number field* or, simply, a *number field* if K is a finite-dimensional vector space over $\mathbb{Q}$, in which case, one can write K as $\mathbb{Q}(\alpha)$ for some algebraic number α. Historically, these fields arose from the desire to solve higher-degree polynomial equations and understand the symmetries of their roots, a pursuit that transitioned from Galois's revolutionary group-theoretic work to Dedekind's formalization of field theory. The relevance of number fields lies in their ability to act as a "macroscope" for arithmetic as, by moving from $\mathbb{Q}$ to a larger field K, we can decompose numbers into new, algebraic factors that reveal the underlying structure of equations.

The *ring of integers* $\mathcal{O}_K$ of a number field K is the set of all elements in K that are roots of monic polynomials with coefficients in $\mathbb{Z}$. The study of these algebraic structures emerged in the 19-th century when prominent mathematicians, including Carl Gauss, Gotthold Eisenstein, and Ernst Kummer, sought to extend the known laws of arithmetic beyond the set $\mathbb{Z}$ of rational or standard integers. From a more philosophical perspective, rings of integers represent the transition from the empirical observation of numbers to the structural understanding of mathematical reality, turning tangible the tension between the concrete nature of specific numbers and the universal algebraic laws that govern them.

Rings of Integers and the Non-Unique Factorizations Crisis

The study of rings of integers was significantly catalyzed by the "crisis of non-unique factorization," most notably when Gabriel Lamé incorrectly assumed that inside every cyclotomic ring extension $\mathbb{Z}[\zeta_p]$ of $\mathbb{Z}$ by a primitive p-th root of unity (with p prime), factorization into irreducibles was essentially unique, a claim debunked by Kummer's discovery that the unique factorization (UF) property collapses in $\mathbb{Z}[\zeta_{23}]$. Today, rings of integers are the central objects of study in algebraic number theory, serving as the "local" playgrounds where we investigate the failure of the UF property and the behavior of prime ideals. Beyond their theoretical beauty, they are foundational to modern cryptography (specifically in lattice-based and isogeny-based systems), provide the framework for solving Diophantine equations, and offer deep insights into factorization theory through invariants like the divisor class group.

Cyclotomic Rings of Integers and Fermat's Last Theorem

At the heart of Fermat's Last Theorem (FLT) lies the fundamental tension between the arithmetic of the rational integers $\mathbb{Z}$ and the rings of integers $\mathscr{O}_K$ of cyclotomic fields. The equation $x^n + y^n = z^n$ can be elegantly factored as

$$z^n = \prod_{j=0}^{n-1} (x + \zeta_n^j y)$$

only by stepping into the ring $\mathbb{Z}[\zeta_n]$. The historical drama of FLT was driven by the discovery that these rings often lack unique factorization, a "failure" that initially thwarted Lamé but led Kummer to develop the theory of ideal numbers. By categorizing primes as "regular" based on whether they divide the class number of $\mathscr{O}_K$, Kummer was able to prove the theorem for a vast majority of exponents. Even in Wiles's final proof, the connection remains intrinsic: the modularity theorem bridges the gap between elliptic curves and the Galois representations associated with these rings of integers. Ultimately, FLT is not merely a statement about $\mathbb{Z}$, but a profound testament to how the structural properties of rings of integers govern the existence (or non-existence) of solutions to Diophantine equations.

Rings of Integers in Connections to Ideal Theory and Valuation Theory

The same crisis ignited the transition from classical number theory to modern abstract algebra. When Kummer introduced "ideal numbers" to rectify the non-unique factorization phenomenon in cyclotomic fields, he provided a computational workaround, but it was Richard Dedekind who transformed this into a robust structural theory. By defining an ideal as a set-theoretic object (a submodule of the ring closed under multiplication), Dedekind shifted the focus from individual elements to collections of numbers, creating (or perhaps discovering) the modern concept of an ideal to restore unique factorization at the level of sets. This Dedekind's clever creation gave life to ideal theory. Ideals provided both the template for Noetherian rings and the axiomatic study of commutative algebra. Furthermore, the quest to understand the size and multiplicity of these ideals led directly to the development of valuation theory. By viewing the power of a prime ideal $\mathfrak{p}$ dividing an element as a valuation $v_\mathfrak{p}$, mathematicians like Kurt Hensel and József Kürschák were able to unify the arithmetic of rings of integers with the analytic properties of power series. Thus, the ring of integers served as the original laboratory for these theories, proving that the local behavior of valuations and the global structure of ideals are two sides of the same arithmetic coin.

Rings of Integers and Arithmetic Geometry

The earliest and most profound applications of factorization theory lie in algebraic number theory. Kummer's ideal numbers and Dedekind's subsequent formalization of ideals provided the conceptual foundation for the study of *ideal class groups*, whose structure measures the failure of unique factorization in rings of integers. Class groups play a central role in

understanding the arithmetic of number fields, influencing the solvability of Diophantine equations, the structure of algebraic curves, and the arithmetic of algebraic varieties (see [1]). The modern theory of global fields, divisor class groups, and Picard groups in algebraic geometry continues to depend fundamentally on these ideas (see [15]).

Foundations – Sets, Monoids, and Groups

In this preliminary chapter, we introduce the set theory notation and briefly recall some basics of commutative monoids and abelian groups we will be referring to later.

General Notation

As it is customary, we let $\mathbb{Z}$ denote the ring of integers and $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ the fields of rational, real, and complex numbers, respectively. In addition, we let $\mathbb{P}$ denote the sets of rational (standard) primes, while we let $\mathbb{N}$ denote the multiplicative monoid of positive integers. Finally, we set

$$\mathbb{N}_0 := \{0\} \cup \mathbb{N}.$$

For each prime $p \in \mathbb{P}$ and positive integer $n \in \mathbb{N}$, we let $\mathbb{F}_{p^n}$ denote the field with p^n elements (it is well known that the cardinality of every finite field is a prime power). For any real number r and a subset S of the real line, we set $S_{\geq r} := \{s \in S : s \geq r\}$. For any pair $(m, n) \in \mathbb{Z}^2$ with $m \leq n$, we set

$$[\![m, n]\!] := \{k \in \mathbb{Z} : m \leq k \leq n\}.$$

For any positive rational q, call the unique relatively primes $\mathsf{n}(q)$ and $\mathsf{d}(q)$ positive integers such that $q = \mathsf{n}(q)/\mathsf{d}(q)$ the *numerator* and the *denominator* of q, respectively. For a prime p, the *p-adic valuation* on $\mathbb{Q}$ is the map $v_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ defined as follows: $v_p(0) = \infty$ and $v_p(q) = v_p(\mathsf{n}(q)) - v_p(\mathsf{d}(q))$ for any $q \neq 0$, where for $n \in \mathbb{N}$ the value $v_p(n)$ is the exponent of the maximal power of p dividing n. One can readily verify that $q_1, \ldots, q_n \in \mathbb{Q}_{>0}$:

$$v_p(q_1 + \cdots + q_n) \geq \min\{v_p(q_1), \ldots, v_p(q_n)\}$$

Commutative Semigroups and Monoids

A *binary operation* on a set S is a function $* \colon S \times S \to S$. When $*$ si a binary operation on a set S, it is customary to write $s * t$ instead of $*(s, t)$ for any $s, t \in S$. A pair $(S, *)$, where S is

a set and $*$ is a binary operation on S is called a semigroup provided that the operation $*$ is associate: $r*(s*t)=(r*s)*t$ for all $r,s,t\in S$.

Let $(S,*)$ be a semigroup. An element $e\in S$ is called an *identity element* of S if $e*s=s*e=s$ for all $s\in S$. Every semigroup has at most one identity element: indeed, if $e_1,e_2\in S$ are both identity elements, then $e_1=e_1*e_2=e_2$. The semigroup $(S,*)$ is said to be *commutative* if $s*t=t*s$ for all $s,t\in S$. A semigroup having an identity element is called a *monoid*.

Let $(M,*)$ be a monoid with identity element denoted by e, and let us denote $(M,*)$ simply by M. An element $u\in M$ is called *invertible* or a *unit* if $u*v=v*u=e$ for some $v\in M$, in which case such an element v is called an *inverse* of u. As the identity element $e\in M$ satisfies $e*e=e$, it is its own inverse and, therefore, a unit. In a monoid, every unit has a unique inverse: indeed, if $v_1,v_2\in M$ are two inverses of a unit u, then $v_1=v_1*(u*v_2)=(v_1*u)*v_2=v_2$.

A subset S of M is called a *submonoid* of M if S contains the identity element of M and is *closed* under the operation of M, which means that $b*c\in S$ for all $b,c\in S$. If S is a submonoid of M such that $S\neq M$, then S is called a *proper* submonoid of M. It is routine to prove that the property of being submonoids of a given monoid is preserved under taking arbitrary intersections.

Let N denote a monoid $(N,*')$ with identity element e_N. A function $\varphi\colon M\to N$ is called a *monoid homomorphism* if $\varphi(e)=e_N$ and $\varphi(b*c)=\varphi(b)*'\varphi(c)$ for all $b,c\in M$. If $\varphi\colon M\to N$ is a bijective homomorphism, then φ is called a *monoid isomorphism* and, in this case, we say that the monoids M and N are *isomorphic*.

Abelian Groups

We recall the basic language of abelian groups, and briefly discuss the quotient of abelian groups.

Definition 0.1. A *group* is a monoid where every element is invertible. A group is said to be *abelian* if it is commutative as a monoid.

Unless we explicitly state otherwise, every abelian group we deal with in this note is written additively. For the rest of this section, let A be an abelian group. A submonoid S of A is said to be a *subgroup* provided that S is a group with the operation it inherits from A, in which case, we write $S\leq A$. If S is a subgroup of A such that $S\neq A$, then S is called a *proper* subgroup of A. Given abelian groups A and B, a map $\varphi\colon A\to B$ is called a *group homomorphism* provided that $\varphi(a+a')=\varphi(a)+\varphi(a')$ for all $a,a'\in A$. We say that a group homomorphism is an *isomorphism* if it is a bijection. Given a group homomorphism $\varphi\colon A\to B$, one can check that $f(A)$ is a subgroup of B, while the subset $\ker\varphi$ of A consisting of all the elements mapped to 0 by φ is a subgroup of A called the *kernel* of φ:

$$\ker\varphi:=\{a\in A:\varphi(a)=0\}.$$

Observe that a group homomorphism is injective if and only if its kernel is the trivial group. Thus, images and kernels of group homomorphisms are groups.

Now let S be a subgroup of A. For each $a \in A$, we define the *coset* of a with respect to S as follows: $a + S := \{a + s : s \in S$. Now set

$$A/S := \{a + S : a \in A\},$$

Let us define now a binary operation on A/S based on the operation of A: for any cosets $a + S$ and $a' + S$ of A/S,

$$(a + S) + (a' + S) := (a + a') + S. \tag{1}$$

It is routine to verify that this binary operation is well defined and also that A/S is a an abelian group under such operation: the group A/S is called the *quotient group* of A by S. Then we can project A onto its quotient group A/S via the map $\pi\colon A \to A/S$ defined by $\pi(a) = a + S$ for all $a \in A$, which is clearly a surjective group homomorphism such that $\ker \pi = S$. In light of this, we see that every subgroup of the abelian group A is the kernel of a group homomorphism with domain A. The following theorem, whose proof we left as an exercise, is known as the First Isomorphism Theorem.

Proposition 0.2. *Let $\varphi\colon A \to A'$ be a group homomorphism. Then the quotient group $A/\ker\varphi$ is isomorphic to the subgroup $\varphi(A)$ of A' via the group homomorphism determined by the assignments $a + \ker\varphi \mapsto \varphi(a)$ for all $a \in A$.*

Chapter 1

Preliminaries on Commutative Rings

1.1 Commutative Rings – Ideals, Quotients, and Homomorphisms

We now recall the notion of a commutative ring (with identity).

Definition 1.1. A triple $(R, +, \cdot)$, where R is a set and $+$ and $\cdot$ are two binary operations on R, is called a *ring* if the following conditions hold:

- $(R, +)$ is an abelian group,
- $(R, \cdot)$ is a monoid, and
- $r \cdot (s + t) = r \cdot s + r \cdot t$ and $(s + t) \cdot r = s \cdot r + t \cdot r$ for all $r, s, t \in R$.

Let $(R, +, \cdot)$ be a ring and, from now on, let us denote this triple simply by R (this is customary in the literature). The identity of the monoid $(R, +)$, is denoted by 0 and called the *zero element* of R or simply *zero*. For all $r \in R$, the equality $0 \cdot r = 0$ holds: it can be deduced from $0 \cdot r = (0 + 0) \cdot r = 0 \cdot r + 0 \cdot r$, as $0 \cdot r$ has an additive inverse. Similarly, $r \cdot 0 = 0$ for all $r \in R$. For $r, s \in R$, we write rs instead of $r \cdot s$ if we see not risk of confusion. We say that R is *commutative* if the semigroup $(R, \cdot)$ is commutative. In addition, we say that an element of R is an *identity* if it is an identity of the semigroup $(S, \cdot)$. Thus, if R contains an identity, then it must be unique and we denote it by either 1_R or 1 and refers to it as *the* identity element. In the scope of this exposition, we are only interested in commutative rings with identity, and we tacitly assume that the identity is not the zero element (otherwise, R is a singleton, which is not an interesting case to consider).

For a commutative ring R with identity, we let $R^\times$ denote its group of units (i.e., invertible elements) of R. For $r, s \in R$, we say that s *divides* r and write $s \mid_R r$ if $r = st$ for some $t \in R$. Elements $r, s \in R$ are *associates* if $s = ur$ for some $u \in R^\times$.

An additive subgroup S of R is called a *subring* if S is closed under multiplication and contains 1. Clearly, a subring of R is a commutative ring with identity under the binary operations it inherits from R.

Let R be a commutative ring with identity 1. An additive subgroup I of R is called an *ideal* if $ra \in I$ for all $r \in R$ and $a \in I$. It is clear that $\{0\}$ and R are ideals of R, and we call $\{0\}$ the *zero ideal* of R. An ideal I of R is called *proper* if $I \subsetneq R$. An ideal I of R is proper if and only if $I \cap R^\times$ is empty: for the less trivial direction, observe that if $u \in I \cap R^\times$ then $R = u(u^{-1}R) \subseteq IR = I$. Hence the only ideals of a field are the zero ideal and the whole field. For any $a \in R$, we can verify that $aR := \{ar : r \in R\}$ is the smallest ideal of R containing a: ideals of the form aR are called *principal ideals*. When often write (a) instead of aR. The zero ideal and the whole ideal R are both principal ideals as $\{0\} = 0R$ and $R = 1R$.

Example 1.2. We verify that the every ideal of $\mathbb{Z}$ is principal. Let I be a nonzero proper ideal, and take $m \in I \setminus \{0\}$ such that $|m| := \min\{|a| : a \in I \setminus \{0\}\}$. Then $m\mathbb{Z} \subseteq I\mathbb{Z} = I$. Conversely, for any $a \in I$ we can take $q, r \in \mathbb{Z}$ with $|r| < |m|$ such that $a = qm + r$ and, as $r = a - qm \in I - m\mathbb{Z} \subseteq I$, and $r = 0$ must hold by the minimality of $|m|$, whence $a = mq \in m\mathbb{Z}$. Hence $I = m\mathbb{Z}$ is a principal ideal. ■

Let R and S be commutative rings with identities 1_R and 1_S, respectively. A map $\phi\colon R \to S$ is called a *ring homomorphism* if ϕ is a group homomorphism between the underlying additive groups of R and S and the following two conditions hold:

- $\phi(1_R) = 1_S$ and
- $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$ for all $r_1, r_2 \in R$.

If $\varphi\colon R \to S$ is a ring homomorphism, one can readily check that the subgroup $\ker\varphi$ of the underlying abelian group of R is indeed an ideal and that the subgroup $\varphi(R)$ of S is indeed a subring. An *isomorphism* of rings is a bijective ring homomorphism. If there exists an isomorphism between R and S, we say that R and S are *isomorphic* and write $R \cong S$.

The main relevance of ideals in ring theory is that we can quotient by them. For an ideal I of R, we can define a multiplicative operation on the quotient group R/I as follows:

$$(r + I)(s + I) := rs + I$$

for all $r, s \in R$, It is routine to verify that, under this multiplication, the quotient group R/I is a commutative ring with identity $1 + I$ (the absorbing property of the ideal I is needed for the multiplication to be well defined). We call R/I the *quotient ring* of R by I. Observe that the group homomorphism $\pi\colon R \to R/I$ is now a ring homomorphism. There is a version of the First Isomorphism Theorem in the setting of commutative rings, and this result describes the structural relationship among homomorphisms, ideals, and quotients.

Proposition 1.3. *Let $\varphi\colon R \to S$ be a ring homomorphism. Then the map $R/\ker\varphi \to S$ defined via the assignment $r + \ker f \mapsto f(r)$ (for all $r \in R$) is an injective ring homomorphism with image $\varphi(R)$, whence $R/\ker f \cong f(R)$.*

With notation as in Proposition 1.3, if $I \subseteq \ker f$, then f factors through π, that is, there exists a unique ring homomorphism $\varphi\colon R/I \to S$ such that $f = \varphi \circ \pi$.

1.2 Integral Domains – UFDs, PIDs, and Euclidean Domains

TO BE INCLUDED...

1.3 Localization

TO BE INCLUDED...

1.4 Polynomial Rings – Irreducibility and Factorizations

TO BE INCLUDED...

Chapter 2

Algebraic Field Extensions and Number Fields

Given two fields K and L, the notation L/K means that K is a subfield of L, in which case we say that either L is an *extension field* of K or that L/K is a *field extension*. For the rest of this section, we let L/K be a field extension.

2.1 Algebraic Extensions

One can show that the action $K \times L \to L$ of K on L induced by the multiplication of L turns (the underlying additive group of) L into a K-vector space. The *degree* of a field extension L/K, denoted by $[L : K]$, is the dimension of L as a K-vector space. The extension L/K is *finite* if L is a finite-dimensional vector space over K or, equivalently, $[L : K] < \infty$. We are interested in whether $\alpha \in F$ satisfies a polynomial equation with coefficients in K. An element $\alpha \in L$ is *algebraic* over K if there exists a nonzero polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$. An element of L is *transcendental* over K if it is not algebraic over K. For an element $\alpha \in L$ that is algebraic over K, there is a unique monic polynomial $m_\alpha(x) \in K[x]$ that vanishes at α and divides any other polynomial in $K[x]$ vanishing at α.

Definition 2.1. Let L/K be a field extension. For any $\alpha \in L$ that is algebraic over K, the unique monic irreducible polynomial in $K[x]$ that divides any other polynomial in $K[x]$ having α as a root is called the *minimal polynomial* of α over K.

Throughout these notes, we often denote the minimal polynomial of an algebraic number α by either $m_\alpha(x)$ or $m_{\alpha,K}(x)$. The extension field L of K is called *simple* if there exists $\alpha \in F$ such that $F = K(\alpha)$. As we proceed to prove, a simple extension $K(\alpha)/K$ is finite if and only if α is algebraic over K, in which case the dimension of the K-vector space $K(\alpha)$ equals the degree of the minimal polynomial of α.

Theorem 2.2. *For a field extension L/K, let $\alpha \in L$ be an algebraic element over K whose minimal polynomial $m(x) \in K[x]$ has degree d. Then the following statements hold.*

1. $K(\alpha) \cong K[x]/(m(x))$.
2. *The set* $\{1, \alpha, \ldots, \alpha^{d-1}\}$ *is a basis for* $K(\alpha)$ *over* K.
3. $[K(\alpha) : K] = \deg\, m(x)$.

Proof. Forthcoming... □

2.2 Primitive Element Theorem

In this section we shall prove that certain extensions L/K, including any finite field extension of $\mathbb{Q}$, are simple.

An element $\alpha \in L$ that is algebraic over K is called *separable* if its minimal polynomial has no repeated roots in any splitting field. We say that the extension L/K is *separable* if it is algebraic and every element of L is separable.

Proposition 2.3. *Let* L/K *be an algebraic field extension. If* K *has characteristic* 0*, then the extension* L/K *is separable.*

Proof. Forthcoming... □

It turns out that every finite separable extension is simple, and this result is known as the Primitive Element Theorem.

Theorem 2.4 (Primitive Element Theorem)**.** *If* L/K *is a finite separable field extension, then there exists* $\theta \in L$ *such that* $L = K(\theta)$.

Proof. Forthcoming... □

As $\mathbb{Q}$ is a field of characteristic zero, any algebraic extension of $\mathbb{Q}$ is separable. Then, in light of the Primitive Theorem, every finite extension field of $\mathbb{Q}$ has the form $\mathbb{Q}(\alpha)$ for some algebraic number α,

Corollary 2.5. *Every finite field extension* $L/\mathbb{Q}$ *is a simple field extension.*

Every ring of integers sits into an algebraic number field. One can readily verify that every subfield of $\mathbb{C}$ contains $\mathbb{Q}$. Indeed, $\mathbb{Q}$ acts on every subfield K by the standard multiplication of complex numbers, and K is a vector space over $\mathbb{Q}$ under such an action.

Definition 2.6. A subfield K of $\mathbb{C}$ is called an *algebraic number field* or, simply, a *number field* provided that K is a finite dimensional vector space over $\mathbb{Q}$. If K is a number field, then $[K : \mathbb{Q}]$ denote the dimension of K as a $\mathbb{Q}$-vector space.

2.3 Number Fields and Rings of Integers

TO BE INCLUDED...

2.4 The Gaussian Rings of Integers

TO BE INCLUDED...

2.5 Exercises – Algebraic Extension and Number Fields

TO BE INCLUDED...

Bibliography

[1] E. Artin and J. Tate, *Class Field Theory*, Addison-Wesley, Reading, MA, 1967.

[2] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. **11** (I960), 391–392.

[3] P. Cohn, *Bezout rings and their subrings*, Proc. Camb. Phil. Soc. **64** (1968) 251–264.

[4] R. Dedekind, *Über die Theorie der ganzen algebraischen Zahlen*, Supplement X to P. G. Lejeune Dirichlet, Vorlesungen über Zahlentheorie, 1st ed., Vieweg, Braunschweig, 1871, pp. 265–290.

[5] D. S. Dummit and R. M. Foote, *Abstract Algebra* (Third Edition), John Wiley & Sons, 2004.

[6] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations: a survey*. In: Multiplicative Ideal Theory in Commutative Algebra (Eds. J. W. Brewer, S. Glaz, W. J. Heinzer, and B. M. Olberding), Springer, Boston, 2006.

[7] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations: Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics Vol. 278, Chapman & Hall/CRC, Boca Raton, 2006.

[8] R. Gilmer, *Multiplicative Ideal Theory*, Queen's Papers in Pure and Applied Mathematics, No. 12, Queen's Univ. Press, Kingston, Ontario, 1968.

[9] A. Grams, *Atomic domains and ascending chain conditions on principal ideals*, Math. Proc. Cambridge Philos. Soc. **75** (1974) 321–329.

[10] F. Halter-Koch, *Finiteness theorems for factorizations*, Semigroup Forum **44** (1992) 112–117.

[11] A. Heinle and V. Levandovskyy, *A factorization algorithm for G-algebras and applications*. Preprint on arXiv: https://arxiv.org/abs/1602.00296

[12] D. Hilbert, *Über die Theorie der algebraishen Formen*, Math. Ann. **36** (1890) 473–534.

[13] E. E. Kummer, *Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren*, Journal für die reine und angewandte Mathematik **35** (1847) 327–367.

[14] J.-P. G. Lamé, *Sur le dernier théoréme de Fermat*, Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences **24** (1847) 410–416 (session of March 1, 1847).

[15] S. Lang, *Algebraic Number Theory*, 2nd ed., Springer-Verlag, New York, 1994.

[16] D. Mumford, J. Fogarty, and F. Kirwan, *Geometric Invariant Theory*, 3rd ed., Springer-Verlag, Berlin, 1994.

[17] E. Noether: *Idealtheorie in Ringbereichen*, Math. Ann. **83** (1921) 24–66.