RAD HRVATSKE AKADEMIJE ZNANOSTI I UMJETNOSTI
MATEMATIČKE ZNANOSTI

B. Širola

On prime elements in commutative domains

Manuscript accepted for publication

ON PRIME ELEMENTS IN COMMUTATIVE DOMAINS

Boris Širola

To Marko, with respect and admiration

Abstract. We present some results concerning prime elements in integral domains. In particular we deal with the following question: Does every order in an algebraic number field has infinitely many prime elements? Then we show that for real quadratic fields the answer to that question is positive. We also give certain partial results and examples about prime polynomials in two or more variables with coefficients from arbitrary integral domain.

Introduction

Recall that a commutative ring with identity is called an integral domain if the product of any two nonzero elements is nonzero. Given an integral domain A it is interesting to understand the set $\operatorname{Irr} A$ of all irreducible elements in A, and in particular its subset $\operatorname{Pr} A$ of all prime elements in A. (Note here that if A is moreover a UFD, then $\operatorname{Pr} A = \operatorname{Irr} A$; see Proposition 1.6.) In general it might be considerably more difficult, and in fact more interesting, to see if a given element of A is prime than if it is irreducible.

There are not many statements about prime elements, and there are not many examples of prime elements in rings that are not UFDs, in the existing literature. Also those results and examples that are known are scattered throughout various books and papers. The purpose of this work is to present a contribution to the current knowledge. In particular suppose $\mathbb{K}$ is an algebraic number field and let $\mathcal{O}_{\mathbb{K}}$ be its ring of integers. Recall that a subring $R \leq \mathcal{O}_{\mathbb{K}}$

2010 *Mathematics Subject Classification.* 13G05 (primary), 11R04, 11R09 (secondary).

Key words and phrases. Prime element, irreducible element, integral domain, unique factorization domain, quadratic field, ring of integers, order.

is called an *order* in $\mathbb{K}$ if the index $(\mathcal{O}_{\mathbb{K}} : R)$ is finite, for R considered as a subgroup of the additive group $(\mathcal{O}_{\mathbb{K}}, +)$. In particular, $\mathcal{O}_{\mathbb{K}}$ is called the maximal order. As a well known fact we have that an order is a Noetherian integral domain in which every nonzero prime ideal is moreover maximal; see, e.g., [11, Ch. I, (12.2) Prop.]. Further, an order $R \neq \mathcal{O}_{\mathbb{K}}$ is not integrally closed in $\mathbb{K}$, and thus such R is not a UFD; see, e.g., [7, Ex. 6 for Ch. II, p. 337]. Therefore the orders are good candidates for exploring the sets of their prime elements.

The theorem given below illustrates one of the principal aims of our paper. In order to state it first recall the following. Assume $\mathbb{K}|\mathbb{F}$ is a finite field extension. For any $x \in \mathbb{K}$ define an ($\mathbb{F}$-linear) map $f_x : \mathbb{K} \to \mathbb{K}$, $f_x(y) = xy$. Then define a norm map

$$N_{\mathbb{K}|\mathbb{F}} : \mathbb{K} \to \mathbb{F}, \quad N_{\mathbb{K}|\mathbb{F}}(x) = \det f_x.$$

Clearly, the map $N = N_{\mathbb{K}|\mathbb{F}}$ is totally multiplicative; i.e., for $x, y \in \mathbb{K}$ we have $N(xy) = N(x)N(y)$. Now we are ready to state our result.

THEOREM 0.1. *Let $\mathbb{K}$ be an algebraic number field. Suppose R is an order in $\mathbb{K}$ and $\pi \in R$ is an element such that $|N_{\mathbb{K}|\mathbb{Q}}(\pi)| = p$, for some prime number $p \in \mathbb{N}$. Then π is a prime element of R. Also if $\rho \in R$ is such that $|N_{\mathbb{K}|\mathbb{Q}}(\rho)| = m$, where m is a composite number which is not of the form $m = p^k$ for some prime number $p \in \mathbb{N}$ and $k \geq 1$, then ρ is not a prime element of R.*

For a quadratic field $\mathbb{K}$ and $R = \mathcal{O}_{\mathbb{K}}$, the conclusion that under the given assumptions the element π is irreducible is well known, and easy to show; see [12, Thm. 9.24], and Lemma 2.1(iii) below. Thus our result strengthen the later one.

The paper is organized as follows. Section 1 is preparatory. There we first introduce our notation and recall some terminology and certain well known results that will be needed in what follows. Also we prove some results that might be essentially known, but we are not aware of any appropriate reference; see Lemma 1.4, Proposition 1.6 and Corollary 1.7. In Section 2 we prove the above theorem. There we also deal with the question asking whether any order R in an algebraic number field $\mathbb{K}$ has infinitely many prime elements. As one might expect, this question is closely related to the problem of solvability for certain special Diophantine equations; and so it is likely that it would not be easy to answer the posed question in general. At the same time as a relatively simple fact we note that for real quadratic fields the answer to the later question is positive; see Corollary 2.6. As one more interesting observation in Proposition 2.10 we show that there are infinitely many numbers $d = pq$, where $p, q \in \mathbb{N}$ are different primes satisfying $p \equiv 5 \pmod 8$ and $q \equiv 1, 3 \pmod 4$, so that the ring of integers $\mathcal{O}_{\mathbb{K}}$ of the quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ is not a UFD; i.e., it is not a PID. Given some interesting integral domain A it

is a standard problem to understand whether particular polynomials in two or more variables, with coefficients from A, are irreducible or not. A number of the corresponding results are known, in particular when A is moreover a field; see, e.g., [10]. In Section 3 we present some basic results and examples where for arbitrary integral domain A we deduce that certain A-polynomials are prime elements of the corresponding polynomial ring. As the central result there we have Proposition 3.4.

1. Some basic results

In what follows every ring we consider is commutative and with identity. Given a ring A, by $A^\times$ we denote the set of its nonzero elements and by A^* the group of its invertible elements (i.e., units). For any positive integer n by $A[X] = A[X_1, \ldots, X_n]$ we denote the ring of A-polynomials in variables $X_1, \ldots, X_n$. Recall that a nonzero polynomial $f \in A[X]$ is reducible if $f \notin A[X]^*$ and f can be written as a product $f = gh$, for some non-invertible polynomials $g, h \in A[X]$. Otherwise we say that f is irreducible. As it is customary, a unique factorization domain will be abbreviated as UFD and a principal ideal domain as PID.

It is well known that the above notions of polynomial (ir)reducibility can be generalized. For the convenience of the reader we recall some terminology, and introduce the corresponding notation. For all the unexplained terminology and notation, or proofs of some known results, see for example [8], [9] or [13]. Given a ring A, elements $x, y \in A$ are associates if there is some $u \in A^*$ such that $x = uy$. We write $x \sim y$ if x and y are associates. Then $\sim$ is an equivalence relation on A. For any $x \in A$ define $[x]$ to be the corresponding class in the quotient set $A/\sim$. An element $c \in A^\times$ is irreducible in A if $c \notin A^*$ and the following holds: *If $c = ab$ for some $a, b \in A$, then either $a \in A^*$ or $b \in A^*$.* By $\operatorname{Irr} A$ we denote the set of all irreducible elements in A. Further for two elements $x, y \in A$, by $x|y$ we denote the fact that x divides y. An element $p \in A^\times$ is prime in A if $p \notin A^*$ and the following holds: *If $p|ab$ for some $a, b \in A$, then $p|a$ or $p|b$.* By $\operatorname{Pr} A$ we denote the set of all prime elements in A.

Observe that the notions of an irreducible element and prime element are strictly related to the ring under consideration. More precisely, we can have two rings $A \subseteq B$ and an element $c \in A$ which is irreducible (resp. prime) in A, but the same does not hold in B. On the other hand we can have $c \in A$ such that c is irreducible (resp. prime) as an element of B, but it is not the same true for A. Related to this observation it might be convenient to state the following simple result; cf. Corollary 1.7 given below.

Proposition 1.1. *Let A be an integral domain and $m < n$ positive integers. Define $R_0 = A$, the ring of polynomials $R_m = A[X_1, \ldots, X_m]$ and analogously R_n. Also define $R_\infty = A[X_1, X_2, \ldots]$, the ring of A-polynomials*

in infinitely many variables. We consider the chain of subrings $A \leq R_m \leq R_n \leq R_\infty$*, in the obvious way. If* $c \in R_m$ *is irreducible in* R_m*, then it is irreducible both as an element of* R_n *and as an element of* R_∞*. That is we have the inclusions*

$$\operatorname{Irr} A \subseteq \operatorname{Irr} R_m \subseteq \operatorname{Irr} R_n \subseteq \operatorname{Irr} R_\infty.$$

PROOF. First note that $R_m^* = R_n^* = R_\infty^* = A^*$. It is sufficient to treat the case of the ring R_∞. Thus assume that for an element $0 \neq c \notin R_\infty^*$ there are some $a, b \in R_\infty$ satisfying $c = ab$. Then it is clear there is a positive integer N so that $c, a, b \in A[X_1, \ldots, X_N]$. Here recall that given any integer $\ell \geq 2$ and any $1 \leq k < \ell$ we have an isomorphism

$$A[X_1, \ldots, X_\ell] \cong A[X_1, \ldots, X_k]\big[X_{k+1}, \ldots, X_\ell\big].$$

Hence it is immediate that in fact we can take $N = m$. So, if c is irreducible in R_m, we conclude that $a \in R_\infty^*$ or $b \in R_\infty^*$; i.e., that c is irreducible as an element of R_∞. □

For later use recall also the following well known facts.

LEMMA 1.2. *Let* A *be a ring.*

(i) *An element* $x \in A^\times$ *is irreducible (resp. prime) if and only if every* $y \in [x]$ *is irreducible (resp. prime).*
(ii) *Assume that* A *is an integral domain. If an element* $p \in A$ *is prime, then it is irreducible as well; i.e., we have the inclusion* $\operatorname{Pr} A \subseteq \operatorname{Irr} A$*.*
(iii) *Assume that* A *is a PID. An element* $p \in A$ *is prime if and only if it is irreducible; i.e., we have the equality* $\operatorname{Pr} A = \operatorname{Irr} A$*.*

Recall also one more well known fact emphasizing the role of prime elements in the ideal theory.

LEMMA 1.3. *Given a ring* A*,* $p \in A^\times$ *is a prime element if and only if the principal ideal* Ap *of* A *is prime.*

Related to the last two claims of Lemma 1.2 we should note some further facts. As we already mentioned, for a particular element of a given ring it is always more demanding to see whether it is prime than if it is irreducible. Here we want to state an interesting characterization of UFDs within the class of Noetherian integral domains; see Proposition 1.6 below. As the referee pointed out to us, a proof of the following auxiliary lemma can be found in [1, Theorems 3.2.1 and 3.2.2]; and so we omitted our proof given in the first version of the paper.

LEMMA 1.4. *Let* A *be a Noetherian integral domain. Then* A *is a factorization domain; i.e. every nonzero non-invertible element* $x \in A$ *can be written as a finite product of irreducible elements (perhaps in a non-unique way). In particular, in every Noetherian integral domain which is not a field there is at least one irreducible element.*

REMARK 1.5. Here it is instructive to note that there are UFDs that are not Noetherian rings. For example if A is a UFD, then the ring of polynomials $R_\infty = A[X_1, X_2, \ldots]$ is a UFD as well; which is easy to show having in mind Proposition 1.1. Obviously, R_∞ is not Noetherian.

Now we are ready for the announced proposition, which is a stronger statement than the one of Lemma 1.2(iii).

PROPOSITION 1.6. *Let A be a factorization domain; e.g., A is a Noetherian domain. Then the following are equivalent.*

(a) *The ring A is a UFD.*
(b) $\Pr A = \operatorname{Irr} A$.

PROOF. As it was again pointed out to us by the referee, a proof that (a) implies (b) can be found in [1, Thm. 3.3.2].

Now suppose that (b) holds. In order to see that A is a UFD it must be shown the uniqueness condition in the definition of a UFD. But this is an easy inductive argument; the same one as for the basic fact that every PID is a UFD as well. □

The next observation is an analogue of Proposition 1.1, where now instead of irreducible elements we consider prime elements.

COROLLARY 1.7. *Let A be a UFD and $m < n$ positive integers. Let R_m, R_n and R_∞ be the same polynomial rings as in Proposition* 1.1. *If $p \in R_m$ is prime in R_m, then it is prime both as an element of R_n and as an element of R_∞. That is we have the inclusions*

$$\Pr R_m \subseteq \Pr R_n \subseteq \Pr R_\infty.$$

PROOF. The rings R_m, R_n and R_∞ are UFDs; see Remark 1.5. Now one just has to combine Propositions 1.6 and 1.1. □

REMARK 1.8. As a concrete and very useful consequence of the above corollary we have the following nontrivial fact. Suppose A is a UFD. Within the ring of polynomials $R = A[X_1, \ldots, X_m, T_1, \ldots, T_n]$ we consider $S = A[X_1, \ldots, X_m]$ as a subring in the standard way. Suppose $p \in S$ is an irreducible polynomial and that $g, h \in R$ are some polynomials such that p divides the polynomial product gh. Then p divides g or h; i.e., p is a prime as an element of R.

2. EXAMPLES OF PRIME ELEMENTS

Suppose $\mathbb{K}$ is an algebraic number field; i.e., we have a finite field extension $\mathbb{K}|\mathbb{Q}$. Let $\mathcal{O}_\mathbb{K}$ be the corresponding ring of integers. For the convenience of the reader here we include one more lemma which gives three well known claims. A proof of the first one is an easy consequence of the fact that $\mathcal{O}_\mathbb{K}$ has a free $\mathbb{Z}$-basis with $[\mathbb{K} : \mathbb{Q}]$ elements; see [7, Ch. II]. For a proof of the second

claim (ii) see [7, Ch. IV, (4.2)]. Using that the norm $N = N_{\mathbb{K}|\mathbb{Q}}$ is totally multiplicative and taking into account (ii), a proof of (iii) is in fact the same as in [12, Thm. 9.24] where $\mathbb{K}$ is a quadratic field; see, e.g., [1, Thm. 9.2.3].

LEMMA 2.1. *Let $\mathbb{K}$ be an algebraic number field, $\mathcal{O}_\mathbb{K}$ its ring of integers and $N = N_{\mathbb{K}|\mathbb{Q}}$ the corresponding norm map.*

(i) *The restriction of N to $\mathcal{O}_\mathbb{K}$ have values in $\mathbb{Z}$; i.e., we have the restricted norm map $N : \mathcal{O}_\mathbb{K} \to \mathbb{Z}$.*
(ii) *An element $\alpha \in \mathcal{O}_\mathbb{K}$ is a unit if and only if $|N(\alpha)| = 1$.*
(iii) *If $c \in \mathcal{O}_\mathbb{K}$ is such that $|N(c)| = p$, for some prime number $p \in \mathbb{N}$, then c is an irreducible element.*

For later use we also state the following known observation about finitely generated abelian groups, which is interesting in itself. Although we are not aware of any suitable reference, its (somewhat involved) proof will be omitted as it is not crucial for the understanding of what follows.

LEMMA 2.2. *Let A be an $n \times n$ matrix with entries from $\mathbb{Z}$. Then define an endomorphism $z \mapsto Az$ of the additive group $\mathbb{Z}^n$ and consider its image $A\mathbb{Z}^n$.*

(i) *If A is a regular matrix, then the quotient group $\mathbb{Z}^n/A\mathbb{Z}^n$ is finite of order $|\det A|$.*
(ii) *If A is not regular and so its rank $\operatorname{rk}(A) < n$, then the rank of the quotient group $\mathbb{Z}^n/A\mathbb{Z}^n$ is equal to $n - \operatorname{rk}(A)$.*

Now we are prepared for the following.

PROOF OF Theorem 0.1.
As R is a free abelian additive group of rank $[\mathbb{K} : \mathbb{Q}] = n$, we can choose some basis $\mathcal{B} = (v_1, \dots, v_n)$ of R. For arbitrary $\rho \in R$ consider the map $f_\rho : R \to R$ defined as before by $f_\rho(r) = \rho r$. And let then $A = (a_{ij})$ be an $n \times n$ matrix with entries from $\mathbb{Z}$ defined by

$$f_\rho(v_j) = \sum_{j=1}^{n} a_{ij} v_j, \qquad \text{for } j = 1, \dots, n.$$

Next define a map $\phi : R \to \mathbb{Z}^n$ so that for $v = z_1 v_1 + \cdots + z_n v_n$, where $z_i \in \mathbb{Z}$, we put $\phi(v) = (z_1, \dots, z_n)$. Clearly, ϕ is an isomorphism of additive groups. Further define a map

$$\vartheta : R/R\rho \to \phi(R)/\phi(R\rho)$$

so that for $v \in R$ we put $\vartheta(v + R\rho) = \phi(v) + \phi(R\rho)$. It is easy to check that ϑ is a well defined isomorphism of groups. Here also note that

$$\phi(R)/\phi(R\rho) = \mathbb{Z}^n/A\mathbb{Z}^n.$$

Taking into account the claim (i) of Lemma 2.2 we conclude that

$$\operatorname{card}(R/R\rho) = |\det A|.$$

It remains to observe that $\det A = \det f_\rho = N_{\mathbb{K}|\mathbb{Q}}(\rho)$.

Now let $\rho = \pi \in R$ be as in the statement of our theorem. As we have that $|N_{\mathbb{K}|\mathbb{Q}}(\pi)| = p$ is a prime number in $\mathbb{N}$, it is immediate that the quotient ring $R/R\pi$ is isomorphic to the field $\mathbb{Z}/p\mathbb{Z}$. And so the principal ideal $R\pi$ is maximal and therefore prime as well. By Lemma 1.3, π is prime as an element of R.

On the other hand suppose ρ is such that $|N_{\mathbb{K}|\mathbb{Q}}(\rho)| = m$, for m as in the statement of the theorem. Now we get that $R/R\rho$ is a ring with m elements. But such a ring cannot be an integral domain, and consequently ρ cannot be a prime element. Namely otherwise it would follow that this ring is moreover a field; i.e., a Galois field. This is clearly impossible. □

Suppose we have algebraic number fields $\mathbb{F}$ and $\mathbb{K}$ so that $\mathbb{K}|\mathbb{F}|\mathbb{Q}$ and an order $R \leq \mathcal{O}_\mathbb{K}$. What we would like to find out are some prime elements of R. A helpful idea is to have some prime elements $\mathfrak{p} \in \operatorname{Pr} \mathcal{O}_\mathbb{F}$ such that the norm $N_{\mathbb{F}|\mathbb{Q}}(\mathfrak{p}) \in \operatorname{Pr} \mathbb{Z}$. And then we can try to find some elements $\pi \in R$ satisfying $N_{\mathbb{K}|\mathbb{F}}(\pi) = \mathfrak{p}$. Clearly every such π will be a prime element of R. It might be instructive to see how that "search in stages" works at one interesting example.

Example 2.3. Consider the quadratic field $\mathbb{F} = \mathbb{Q}(i)$ and the biquadratic field $\mathbb{K} = \mathbb{Q}(i, \sqrt{2})$. Then $\mathcal{O}_\mathbb{F} = \mathbb{Z}[i]$, the ring of Gaussian integers. Also with a little work one can show that the ring of integers $\mathcal{O}_\mathbb{K}$ consists of all elements of the form

$$w = a + bi + c\sqrt{2} + di\sqrt{2}, \qquad \text{for } a, b, c, d \in \mathbb{Z}. \tag{2.1}$$

It is a standard fact that the norm $N_{\mathbb{F}|\mathbb{Q}}(a + bi) = a^2 + b^2$. At the same time for w as above we have that

$$N_{\mathbb{K}|\mathbb{F}}(w) = (a + bi)^2 - 2(c + di)^2,$$

and also

$$N_{\mathbb{K}|\mathbb{Q}}(w) = N_{\mathbb{F}|\mathbb{Q}}(N_{\mathbb{K}|\mathbb{F}}(w)) = (a^2 - b^2 - 2c^2 + 2d^2)^2 + 4(ab - 2cd)^2. \tag{2.2}$$

As the first useful observation we have the following claim.

Claim. *The ring of integers $\mathcal{O}_\mathbb{K}$ is not a UFD.*

In order to prove this we begin by showing that there is no $w \in \mathcal{O}_\mathbb{K}$ such that $|N_{\mathbb{K}|\mathbb{Q}}(w)| = 2$. Namely suppose to the contrary, that $N_{\mathbb{K}|\mathbb{Q}}(w) = \pm 2$ for some w. If we write w as in (2.1) then by the above expression (2.2) it is clear that $a^2 - b^2$ is even, and therefore $N_{\mathbb{K}|\mathbb{Q}}(w)$ must be divisible by 4; which is impossible. Now as an immediate consequence we deduce that $\sqrt{2} \in \operatorname{Irr} \mathcal{O}_\mathbb{K}$. But we claim that $\sqrt{2}$ is not a prime element. Namely $\sqrt{2}$ divides $(1+i)(1-i)$, but does not divide neither of the two factors. Namely suppose that we have some $w \in \mathcal{O}_\mathbb{K}$ satisfying $1 \pm i = \sqrt{2}w$. If we write w as in (2.1) it follows that

in particular $1 = x\sqrt{2} + 2z$ for some integers x and z. But this is impossible. Thus, as $\mathcal{O}_{\mathbb{K}}$ is a Noetherian domain and $\Pr \mathcal{O}_{\mathbb{K}} \neq \operatorname{Irr} \mathcal{O}_{\mathbb{K}}$, by Proposition 1.6 our Claim follows.

Further recall the description of the set $\Pr \mathbb{Z}[i]$; see, e.g., [11, Ch. I, (1.4) Thm.]. Every prime $\mathfrak{p}$ of $\mathbb{Z}[i]$, up to multiplication by an invertible element, has one of the following three forms:

(**1**) $\mathfrak{p} = 1 + i$;
(**2**) $\mathfrak{p} = \alpha + \beta i$, where $\alpha^2 + \beta^2 = p$ with $\alpha > |\beta| > 0$ and $p \equiv 1 \pmod 4$;
(**3**) $\mathfrak{p} = p$, where $p \equiv 3 \pmod 4$.

(In (**2**) and (**3**) the symbol p denotes a prime in $\mathbb{N}$.) First observe that $\mathfrak{p} = 1 + i$ is not suitable for our approach as there is no $w \in \mathcal{O}_{\mathbb{K}}$ satisfying $N_{\mathbb{K}|\mathbb{F}}(w) = 1 + i$. Also for $\mathfrak{p}$ of type (**3**) we can have some $\rho \in \mathcal{O}_{\mathbb{K}}$ such that $N_{\mathbb{K}|\mathbb{F}}(\rho) = \mathfrak{p}$, but at the same time we have $N_{\mathbb{F}|\mathbb{Q}}(\mathfrak{p}) = p^2$ and therefore it is not clear whether such ρ is prime or not. (Note that for the above considered non-prime element $w = \sqrt{2}$ the quotient ring $\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\sqrt{2}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.) But the primes of type (**2**) are good for our approach. Namely now the equality $N_{\mathbb{K}|\mathbb{F}}(w) = \mathfrak{p}$, where w is as in (2.1), is equivalent to the system of Diophantine equations

$$\begin{cases} a^2 - b^2 - 2c^2 + 2d^2 &= \alpha \\ \quad 2ab + 4cd &= \beta \end{cases} \tag{2.3}$$

As an easy exercise we have to check that the smallest prime $p \in \mathbb{N}$ satisfying both $p \equiv 1 \pmod 4$ and $\alpha^2 + \beta^2 = p$, and such that the above system (2.3) has a solution, is $p = 41$. For example for $p = 29$ the only two possibilities for (α, β) as in (**2**) are $(5, \pm 2)$. But then by the second equation in (2.3) we have that ab is necessarily odd. And then the left-hand side of the first equation is even; which cannot be. Similarly we rule out every $p \in \{5, 13, 17, 37\}$. On the other hand for $p = 41$ we have that (α, β) is either $(5, 4)$ or $(5, -4)$. Thus the system (2.3) becomes

$$\begin{cases} a^2 - b^2 - 2c^2 + 2d^2 &= 5 \\ \quad ab + 2cd &= \pm 2 \end{cases}$$

By inspection we obtain as a conclusion that for example every π from the set

$$\mathcal{S}(41) = \{2 + i + i\sqrt{2}, 3 - 2i + 2\sqrt{2} + 2i\sqrt{2}, 6 + i - 4\sqrt{2} + i\sqrt{2}, \ldots\}$$

is prime in $\mathcal{O}_{\mathbb{K}}$. It is easy to see that the next smallest p of the form as in (**2**) is 97, when for (α, β) we again have just two possibilities; either $(9, 4)$ or $(9, -4)$. For this $p = 97$ we have for example as primes from $\mathcal{O}_{\mathbb{K}}$ the four elements $3 \pm \sqrt{2} \pm i\sqrt{2}$.

Perhaps it might be interesting to observe here one more thing which is motivated by the above two examples of p. Namely suppose there is an

odd number $x > 1$ such that $p = x^4 + 16$ is a prime number. Then for $(\alpha, \beta) \in \{(x^2, \pm 4)\}$ the system (2.3) becomes

$$\begin{cases} a^2 - b^2 - 2c^2 + 2d^2 & = x^2 \\ ab + 2cd & = \pm 2 \end{cases}$$

Clearly, $(a, b, c, d) = (\pm x, 0, \pm 1, \pm 1)$ are solutions of the later system. As an interesting fact we have that $3^4 + 16 = 97$, $5^4 + 16 = 641$, $7^4 + 16 = 2417$, $9^4 + 16 = 6577$ and $11^4 + 16 = 14567$ are primes. On the other hand for $x = 13$ or 15 we obtain composite numbers $13^4 + 16 = 28577 = 17 \cdot 1681$ and $15^4 + 16 = 50641 = 89 \cdot 569$. But $17^4 + 16 = 83537$ is again a prime. It would be nice to know if there is infinitely many primes of the form $x^4 + 16$ for $x > 1$ odd number.

It is likely that for the field $\mathbb{K} = \mathbb{Q}(i, \sqrt{2})$ the set $\operatorname{Pr} \mathcal{O}_{\mathbb{K}}$ is infinite, but we do not know if this is the case. In general it would be interesting to answer the following question.

QUESTION. *Given an algebraic number field $\mathbb{K}$ and an order R in $\mathbb{K}$, is the set of primes $\operatorname{Pr} R$ necessarily infinite?*

To the end of this section we focus on real quadratic fields. Our first goal is to show that for these fields the answer to the above question is positive. For that purpose let $d \neq 1$ be a square-free positive integer and define $\omega = (1 + \sqrt{d})/2 \in \mathbb{C}$. Define the following subrings of the quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$:

$$A_d = \mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} \mid x, y \in \mathbb{Z}\},$$
$$B_d = \mathbb{Z}[\omega] = \{x + y\omega \mid x, y \in \mathbb{Z}\} \quad \text{if } d \equiv 1 \pmod 4.$$

The statement (i) of the next lemma is clear, while the other two are well known facts; cf. Lemma 2.1(ii).

LEMMA 2.4. *For the field $\mathbb{K}$ and the rings A_d and B_d the following hold.*

(i) *We have $\mathcal{O}_{\mathbb{K}} = A_d$ for $d \equiv 2, 3 \pmod 4$, and $\mathcal{O}_{\mathbb{K}} = B_d$ for $d \equiv 1 \pmod 4$. Further for $d \equiv 1 \pmod 4$ the ring A_d is an order in $\mathbb{K}$ with the index of additive groups $(\mathcal{O}_{\mathbb{K}} : A_d) = 2$.*

(ii) *The corresponding norm map $N : \mathbb{K} \to \mathbb{Q}$ is given by $N(x + y\sqrt{d}) = x^2 - dy^2$.*

(iii) *Let C be either some ring A_d or B_d for $d \equiv 1 \pmod 4$. Then an element $u \in C$ is invertible if and only if $|N(u)| = 1$.*

REMARK 2.5. As the first basic observation related to the above Question we have that for the rings A_d we have the following:

> For each square-free positive integer $d \neq 1$ the ring A_d has infinitely many irreducible elements.

(In particular again by Proposition 1.6 we have that for $d \equiv 2, 3 \pmod 4$, such that $\mathcal{O}_{\mathbb{K}} = A_d$ is a PID, the set of primes $\operatorname{Pr} \mathcal{O}_{\mathbb{K}}$ is infinite.) Namely

choose $k \in \mathbb{Z}\setminus\{0,\pm 1\}$ such that the generalized Pell equation $x^2-dy^2=k$ has infinitely many solutions in integers and the absolute value $|k|$ is the minimal possible. Now if $(a,b)\in\mathbb{Z}^2$ is any solution, then the elements $a\pm b\sqrt{d}\in A_d$ are irreducible. For more details about the generalized Pell equations see e.g. [6, 8.3 and 10.3-10.5].

Now recall a well known fact that for $d\equiv 2,3 \pmod 4$ every order in $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ is of the form

$$R_m=\{x+my\sqrt{d}\mid x,y\in\mathbb{Z}\}, \tag{2.4}$$

for some positive integer m; where in particular $R_1=\mathcal{O}_{\mathbb{K}}$. Also for $d\equiv 1 \pmod 4$ every order in $\mathbb{K}$ is of the form

$$R_m=\{x+my\omega\mid x,y\in\mathbb{Z}\}, \tag{2.5}$$

for some positive integer m; and again $R_1=\mathcal{O}_{\mathbb{K}}$. The following corollary presents the mentioned positive answer to the above posed Question. Here we recall one classical but nontrivial theorem, due to Dirichlet, in a form suitable for our purposes; see [5, p. 417] and [2, Abschn. 10]. Namely suppose $q(x,y)=ax^2+bxy+cy^2$ is an integral primitive quadratic form whose discriminant b^2-4ac is not a square. Then q represents infinitely many primes in $\mathbb{N}$.

Corollary 2.6. *Let $d\neq 1$ be a square-free positive integer and R be an order in $\mathbb{K}=\mathbb{Q}(\sqrt{d})$. Then the set of prime elements $\operatorname{Pr} R$ is infinite.*

Proof. For any positive integer m define a quadratic form

$$q_m(x,y)=\begin{cases} x^2-dm^2y^2, & \text{if } d\equiv 2,3 \pmod 4,\\ x^2+mxy+\frac{1-d}{4}m^2y^2, & \text{if } d\equiv 1 \pmod 4;\end{cases}$$

i.e., $q_m(x,y)=N(x+my\sqrt{d})$ if $d\equiv 2,3 \pmod 4$ and $q_m(x,y)=N(x+my\omega)$ if $d\equiv 1 \pmod 4$. Clearly every q_m is primitive and its discriminant is not a square. Thus by the above stated Dirichlet's theorem there are infinitely many primes $p\in\mathbb{N}$ such that the equation

$$q_m(x,y)=p \tag{2.6}$$

is solvable in integers. In particular for $d\equiv 2,3 \pmod 4$ we obtain a generalized Pell equation $x^2-dm^2y^2=p$. And each of these equations has infinitely many solutions $(x,y)\in\mathbb{Z}^2$. By Theorem 0.1 for every such solution (x,y) the element $x+my\sqrt{d}$ belongs to $\operatorname{Pr} R$. Similarly for $d\equiv 1 \pmod 4$ and some solution (x,y) of (2.6) we have that the element $x+my\omega$ belongs to $\operatorname{Pr} R$. Thus we have the corollary proved. □

Note that in the proof of the latter corollary in fact we needed a weaker result than the mentioned Dirichlet's theorem is. More precisely it would suffice to know that for each form q_m there is at least one prime $p\in\mathbb{N}$ so that

at least one of the two Diophantine equations $q_m(x,y) = \pm p$ has a solution in integers. Then we can conclude that the corresponding set $\Pr R$ is infinite. For $d \equiv 2,3 \pmod 4$ we saw that in the given proof of the corollary. And for $d \equiv 1 \pmod 4$ this follows by the next easy lemma.

LEMMA 2.7. *Suppose $d \equiv 1 \pmod 4$ and define $\delta = (d-1)/4$. If for some nonzero $k \in \mathbb{Z}$ the Diophantine equation*

$$x^2 + mxy - \delta m^2 y^2 = k \tag{2.7}$$

has a solution in integers, then it has infinitely many solutions in integers.

PROOF. As we in fact already noted, the equation (2.7) can be written in an equivalent form as $N(x + my\omega) = k$. Suppose $(x_0, y_0) \in \mathbb{Z}^2$ is its solution. Also let $(u,v) \in \mathbb{Z}^2$ be any solution of the Pell equation $U^2 - dm^2V^2 = 1$; i.e., that $N(u + mv\sqrt{d}) = 1$. As the norm N is totally multiplicative, for

$$z = (x_0 + my_0\omega)(u + mv\sqrt{d})$$

we have that $N(z) = k$. It is straightforward to see that $z = \widetilde{x} + m\widetilde{y}\omega$, where

$$\widetilde{x} = x_0(u - mv) + 2\delta m^2 v y_0 \quad \text{and} \quad \widetilde{y} = y_0(u + mv) + 2x_0 v.$$

In other words, every $(\widetilde{x}, \widetilde{y}) \in \mathbb{Z}^2$ is a solution of (2.7). □

EXAMPLE 2.8. (I) Take $d = 2$ and consider $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. By a little work one can check the following interesting fact. For every integer $2 \le m \le 100$ we can find a positive integer x such that $x^2 - 2m^2 = -p$ for some prime number $p \in \mathbb{N}$; i.e., we can always take $y = 1$ in order to represent $-p$ by the corresponding form q_m. This in particular gives a direct computational argument that every set of primes $\Pr R_m$, where R_m is as in (2.4), is infinite for $2 \le m \le 100$. More precisely, define $\mathcal{M}(x)$ as the set of all $m \in \{2, \dots, 100\}$ such that $x^2 - 2m^2 \in \Pr \mathbb{Z}$ and there is no positive integer $x_0 < x$ so that for $m \in \mathcal{M}(x)$ we also have $m \in \mathcal{M}(x_0)$. (That is, for $m \in \mathcal{M}(x)$ this x is "minimal possible".) Then we have $\mathcal{M}(23) = \{90\}$, $\mathcal{M}(19) = \{75, 93\}$, $\mathcal{M}(17) = \{30\}$, $\mathcal{M}(15) = \{71\}$, $\mathcal{M}(13) = \{55\}$, $\mathcal{M}(11) = \{96\}$, $\mathcal{M}(9) = \{65\}$ and also

$$\mathcal{M}(7) = \{19, 20, 51, 53, 60, 66, 74, 82, 83, 88, 94\},$$
$$\mathcal{M}(5) = \{9, 12, 26, 27, 29, 33, 48, 54, 57, 72, 77, 78, 84, 89, 97, 99\},$$
$$\mathcal{M}(3) = \{5, 14, 16, 23, 31, 32, 35, 37, 40, 44, 47, 58, 61, 67, 68, 70, 79, 86, 100\}.$$

The other 45 values of m belong to the set $\mathcal{M}(1)$.

(II) Now take $d = 5$ and consider $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. Here we have $q_m(x,y) = x^2 + mxy - m^2y^2$ and therefore $q_m(x,2) = (x+m)^2 - 5m^2$. We claim that for every integer $2 \le m \le 100$ we can find a positive integer x such that $x^2 - 5m^2 = -p$ for some prime number $p \in \mathbb{N}$. Note that for every m we can take $x \le 23$, where in particular for $m = 60$ we get $23^2 - 5 \cdot 60^2 = -17471$.

We leave to the reader to compute the nonzero sets $\mathcal{M}(x)$, for $1 \leq x \leq 9$ and $x \in \{11, 13, 14, 16, 19\}$; where $\mathcal{M}(x)$ have the same meaning as in (I). In particular, we have that $\mathcal{M}(1)$ contains 28 values. As a conclusion, again we have a direct argument showing that every set of primes $\Pr R_m$, where R_m is as in (2.5), is infinite for $2 \leq m \leq 100$.

Remark 2.9. For the above given two examples note the following. As one might expect the stated Question is closely related to the question of solvability of certain Diophantine equations. In particular for quadratic fields we had the question of representability of certain prime integers via particular quadratic forms in two variables. As one special case of that we can expect that for every square-free positive integer d the set $\Sigma_d = \{dm^2 - 1 | m \in \mathbb{N}\}$ will contain infinitely many prime integers. Of course we have no idea how to deal with this. But as one more heuristic fact for example note the following. Let $\mathcal{S}$ be the set of all numbers m satisfying both $200 \leq m \leq 300$ and $6m^2 - 1$ is a prime number. Clearly, for the 40 values of m satisfying $m \equiv 1, 4, 6, 9 \pmod{10}$, the number $6m^2 - 1$ is divisible by 5. For the remaining 61 values of m, 33 of them belong to the set $\mathcal{S}$. More precisely, we have

$$\begin{aligned}\mathcal{S} = \{&200, 207, 208, 210, 212, 220, 222, 223, 225, 227, 230, 235, 237, 238,\\ &240, 242, 247, 248, 257, 260, 263, 265, 267, 273, 277, 280, 283, 285,\\ &287, 288, 290, 292, 298\}.\end{aligned}$$

We conclude this section with one more result about real quadratic fields. First recall some well known facts; see, e.g., [4, Ch. VII, §§2 and 3]. The ring of integers $\mathcal{O}_{\mathbb{K}}$ of an algebraic number field $\mathbb{K}$ is a Dedekind domain. Further, a Dedekind domain is a UFD if and only if it is a PID. Consequently, we have the equivalences

$$h_{\mathbb{K}} = 1 \Longleftrightarrow \mathcal{O}_{\mathbb{K}} \text{ is a UFD} \Longleftrightarrow \mathcal{O}_{\mathbb{K}} \text{ is a PID},$$

where $h_{\mathbb{K}}$ is the class number of the algebraic number field $\mathbb{K}$; see, e.g., [1, Thm. 12.1.1]. Related to that a still unsolved problem asks whether we have infinitely many algebraic number fields $\mathbb{K}$ for which $\mathcal{O}_{\mathbb{K}}$ is a PID. Moreover a famous conjecture due to Gauss states that there are infinitely many real quadratic fields $\mathbb{K}$ so that the corresponding $\mathcal{O}_{\mathbb{K}}$ is a PID. At the same time we know that there are infinitely many real fields $\mathbb{K}$ so that its $\mathcal{O}_{\mathbb{K}}$ is not a PID. That is there are infinitely many real fields $\mathbb{K}$ for which the corresponding class number $h_{\mathbb{K}}$ is greater than 1. For example we know that $h_{\mathbb{K}}$ is even if the discriminant $d_{\mathbb{K}}$ of a real quadratic field $\mathbb{K}$ is divisible by three different primes; see, e.g., [7, Ch. V, Thm. 39, Cor. 1] and [3, Ch. 3, Sect. 8, Thm. 8] for more details. Further we know that given a positive integer e there are infinitely many real quadratic fields $\mathbb{K}$ such that e divides $h_{\mathbb{K}}$. The later result is due to Yamamoto [16] and Weinberger [15]. Here note that the corresponding numbers d, of the fields $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ for which the above stated claims hold,

will often be composite numbers with more than two prime divisors. So it might be of some interest to observe the following. Perhaps this is known, but we are not aware of any reference and so its proof is included.

PROPOSITION 2.10. *There are infinitely many positive square-free integers d such that the ring of integers $\mathcal{O}_{\mathbb{K}}$, of the quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, is not a PID. More precisely, take any prime number $p \in \mathbb{N}$ satisfying $p \equiv 5 \pmod 8$. Then we have infinitely many such positive square-free integers d satisfying both $d \equiv 1 \pmod 4$ and $p|d$. Also there are infinitely many positive square-free integers d satisfying both $d \equiv 3 \pmod 4$ and $p|d$.*

In particular there are infinitely many positive integers d of the form $d = pq$, for some different primes $p, q \in \mathbb{N}$, so that the corresponding ring of integers $\mathcal{O}_{\mathbb{K}}$ is not a PID.

Keeping the above notation in force we first prove one auxiliary result about the norm map.

LEMMA 2.11. *Let $p \in \mathbb{N}$ be a prime number and d a square-free positive integer divisible by p. Then the following are equivalent.*

(a) *There is no $w \in \mathcal{O}_{\mathbb{K}}$ satisfying any of the two congruences $N(w) \equiv \pm 2 \pmod p$.*
(b) *We have $p \equiv 5 \pmod 8$.*

PROOF. First consider the case $d \equiv 2, 3 \pmod 4$. Then an element $w = x + y\sqrt{d} \in \mathcal{O}_{\mathbb{K}}$ satisfies $N(w) \equiv \pm 2 \pmod p$ if and only if $x^2 - dy^2 \equiv x^2 \equiv \pm 2 \pmod p$. Assume that (a) holds. Then each of the two congruences $x^2 \equiv \pm 2 \pmod p$ has no solutions, or equivalently for the corresponding Legendre symbols we have $\left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = -1$. We have that the Legendre symbol $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod 8$; see, e.g., [6, Thm. 4.5]. Also we have $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ and $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$; see, e.g., [6, Prop. 4.3]. Thus if (a) holds we must have that either $p \equiv 3 \pmod 8$ or $p \equiv 5 \pmod 8$, and at the same time that $p \equiv 1 \pmod 4$. So we conclude that necessarily (b) holds. For the opposite implication note that (b) implies that $\left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = -1$. Therefore, if (b) holds, then each of the two congruences $x^2 \equiv \pm 2 \pmod p$ has no solutions. Thus (a) holds.

Next assume that $d \equiv 1 \pmod 4$. Then an element $w = x + y\omega \in \mathcal{O}_{\mathbb{K}}$ would be a solution of one of the congruences $N(w) \equiv \pm 2 \pmod p$ if and only if we have

$$x^2 + xy + \frac{1-d}{4}y^2 \equiv \pm 2 \pmod p.$$

Hence it follows that for $t = 2x + y$ we have $t^2 - dy^2 \equiv \pm 8 \pmod p$. Here observe that the congruence $t^2 \equiv \varepsilon 8 \pmod p$ has a solution if and only if the congruence $t^2 \equiv \varepsilon 2 \pmod p$ has a solution, for $\varepsilon \in \{\pm 1\}$. This is a clear consequence of the fact that $\left(\frac{\varepsilon 8}{p}\right) = \left(\frac{\varepsilon 2}{p}\right)^3$. Therefore by what we have already

shown it is immediate that the equivalence of (a) and (b) holds in this case as well. □

Proof of Proposition 2.10. First suppose that $d \equiv 1 \pmod 4$ and let then $\delta = (d-1)/4$ be as before. For $x + y\omega, a + b\omega \in \mathcal{O}_{\mathbb{K}}$ we have

$$(x + y\omega)(a + b\omega) = xa + yb\delta + (xb + ya + yb)\omega.$$

Let us try to find some convenient integers x, y, a, b and d so that $xb+ya+yb = 0$ and $xa + yb\delta$ is equal to some even positive integer 2ν. For example take $y = a = b = 1$, and then we have $x = -2$. Also take $d \equiv 1 \pmod 8$; i.e., write $d = 8\ell + 1$ for some positive integer ℓ. Now choose a (unique) number $m \in \{1, \dots, p-1\}$ so that $d = 8(pk + m) + 1$ is divisible by p, for any integer k. Clearly we have $m = (5p - 1)/8$ and then $d = p(8k + 5)$. Finally, by the classical Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many natural numbers k so that d is square-free. It remains to observe the following two facts. First, by the previous lemma it is clear that 2 is an irreducible element. Second, note that by our choice we have that

$$(-2 + \omega)(1 + \omega) = 2\nu.$$

And hence it is immediate that 2 is not prime. Therefore $\mathcal{O}_{\mathbb{K}}$ is not a PID.

Now consider the case $d \equiv 2, 3 \pmod 4$. Similarly as above for the product of elements $x + y\sqrt{d}, a + b\sqrt{d} \in \mathcal{O}_{\mathbb{K}}$ we want both $xb + ya = 0$ and $xa + dby = 2\nu$ for some positive integer ν. Take again $y = a = b = 1$, where now $x = -1$. Thus we in particular obtain that $-1 + d = 2\nu$, and therefore we have to take $d \equiv 3 \pmod 4$. But if $d = 4\ell + 3$, then as above there is a unique $m \in \{1, \dots, p-1\}$ so that $d = 4(pk + m) + 3$ is divisible by p. This time we have $m = 3(p-1)/4$ and then $d = p(4k + 3)$. Clearly for infinitely many values of k the natural number d will be square-free and again we will have that $2 \in \operatorname{Irr} \mathcal{O}_{\mathbb{K}}$ and $2 \notin \operatorname{Pr} \mathcal{O}_{\mathbb{K}}$. □

Remark 2.12. Suppose $p \in \mathbb{N}$ is a prime number satisfying $p \equiv 5 \pmod 8$. Then for $k \in \mathbb{N}$ define $d_p^1(k) = p(8k + 5)$ and $d_p^2(k) = p(4k + 3)$. By Proposition 2.10 and its proof we know that for $d = d_p^1(k)$ or $d_p^2(k)$ square-free the corresponding ring of integers $\mathcal{O}_{\mathbb{K}}$ is not a PID. Thus in particular for $1 < d < 1000$ square-free we obtain in total 104 values of d for which $\mathcal{O}_{\mathbb{K}}$ is not a PID. Further, there are 22 values of square-free $d \in \{2, \dots, 100\}$ such that the corresponding $\mathcal{O}_{\mathbb{K}}$ is not a PID. By our proposition we obtain 8 out of all these 22 values. These are: 15, 35, 39, 55, 65, 87, 91 and 95.

As the final remark here we note that one could adapt our approach via Proposition 2.10 and Lemma 2.11 so that some other square-free values of d could be ruled-out in the sense that the corresponding ring $\mathcal{O}_{\mathbb{K}}$ is not a PID.

3. On irreducible and prime polynomials

Given an integral domain A it is interesting to find out whether a particular polynomial $p = p(X)$ of the ring of polynomials $A[X]$, in one variable, is irreducible or not. If A is not a UFD, it would be often very helpful to see if p is moreover a prime element or not. The main purpose of this section is to present some basic results concerning the problems of polynomial reducibility for polynomials in two or more variables.

In order to better understand our setting, and the difference between the cases when A is a UFD and when it is not, it might be helpful to start with the following general observation. We omit its proof.

Lemma 3.1. *Let A be a Noetherian integral domain. Then the following are equivalent.*

(a) *The ring A is a UFD.*
(b) *For every positive integer n the ring of polynomials $A[X_1, \ldots, X_n]$ is a UFD.*
(c) *There is a positive integer n so that the ring of polynomials $A[X_1, \ldots, X_n]$ is a UFD.*

Recall that given a polynomial $p \in \mathbb{Q}[X]$, in one variable, it is in general a difficult problem to find out whether p is reducible or not. Related to that we could first ask does the set $\operatorname{Irr}\mathbb{Q}[X] = \operatorname{Pr}\mathbb{Q}[X]$ have infinitely many elements. The following result, whose proof is an adaptation of the one proving that $\mathbb{N}$ has infinitely many primes, is certainly known. For the convenience of the reader we include its short proof.

Proposition 3.2. *Let A be a Noetherian UFD. Then for every positive integer n the ring of polynomials $R = A[X_1, \ldots, X_n]$ has infinitely many irreducible (i.e., prime) polynomials.*

Proof. As R is a Noetherian UFD as well, by Proposition 1.6 we in particular have that $\operatorname{Irr} R = \operatorname{Pr} R$. Now assume R has finitely many irreducible polynomials, say $f_1, \ldots, f_n$. Define a polynomial $F = f_1 \cdots f_n + 1_A$, where 1_A is the identity of A. Now a classical argument gives an irreducible polynomial $q \in R$ which divides F and which cannot be equal to any of f_i; a contradiction. □

To the end of this section we present some interesting facts and results about the reducibility of polynomials in two or more variables. We begin with two examples.

Example 3.3. Let A be an integral domain.

(I) For any integer $n \geq 1$ consider the ring of polynomials $R = A[X_1, \ldots, X_n, Y]$, in variables $X_1, \ldots, X_n$ and Y. If we define $B = A[X_1, \ldots, X_n]$, then up to an isomorphism $R = B[Y]$. We claim the following:

For every $\varphi \in B$, the element $p = Y - \varphi(X_1, \dots, X_n)$ is prime in R.

In order to show this assume $f, g \in R$ are nonzero polynomials such that $p|fg$. Consider f and g as elements of $B[Y]$ and then by the division algorithm we have some $q_1, q_2 \in R$ and $r_1, r_2 \in B$ such that $f = q_1 p + r_1$ and $g = q_2 p + r_2$. Now suppose r_1 and r_2 are nonzero polynomials. As clearly p divides $\rho = r_1 r_2 \in B$, there is some $h \in R$ such that

$$\rho(X_1, \dots, X_n) = ph(X_1, \dots, X_n, Y).$$

Then write $h \in B[Y]$ as $h = h_0 + h_1 Y + \cdots + h_m Y^m$, for some $h_i \in B$ where in particular $h_m \neq 0$. It follows that

$$\rho = (-\varphi h_0) + \cdots + h_m Y^{m+1},$$

which is impossible since $m+1 \geq 1$. Thus we conclude that necessarily $r_1 = 0$ or $r_2 = 0$; i.e., that $p|f$ or $p|g$.

As a special consequence of the above claim we have that each variable X_i of the polynomial ring $A[X_1, \dots, X_n]$ is a prime element.

(II) Now define the ring of polynomials $R = A[X, Y]$, in variables X and Y. For arbitrary $a, b \in A$ define a polynomial

$$\varphi(X) = X^3 + aX + b.$$

We claim the following:

The element $p = Y^2 - \varphi(X)$ is prime in R.

(Note that, for "nice" A, the equality $p = 0$ becomes the "Weierstrass form of an elliptic curve". Also observe that the argument given in what follows remains valid for any $\varphi \in A[X]$ of odd degree; cf. Proposition 3.4 below.)

Our argument is similar to the one in (I). Namely assume $f, g \in R$ are nonzero polynomials such that $p|fg$. Then we can find some $q_1, q_2, r_1, r_2 \in R$ such that

$$f = q_1(Y^2 - \varphi) + r_1, \qquad g = q_2(Y^2 - \varphi) + r_2. \tag{3.8}$$

Here we can write $r_1 = s_0 + s_1 Y$ and $r_2 = t_0 + t_1 Y$, for some $s_i, t_i \in A[X]$. Again assume that $r_1, r_2 \neq 0$. As $p|r_1 r_2$ there is some $h \in R$ satisfying $r_1 r_2 = ph$; i.e., we have that

$$s_0 t_0 + (s_0 t_1 + s_1 t_0) Y + s_1 t_1 Y^2 = (Y^2 - \varphi)h.$$

Hence it is clear that necessarily $h = h_0 \in A[X]^\times$. And then we have equalities

$$s_1 t_1 = h_0, \quad s_0 t_1 + s_1 t_0 = 0, \quad s_0 t_0 = -\varphi h_0. \tag{3.9}$$

By multiplying the first equality by s_0 we get $s_1 s_0 t_1 = s_0 h_0$. By multiplying the second equality by s_1 we get $s_0 s_1 t_1 = -s_1^2 t_0$. Finally by multiplying the third equality by s_0 we get $s_0^2 t_0 = -\varphi h_0 s_0$. By the three newly obtained equalities it is immediate that $s_0^2 t_0 = \varphi s_1^2 t_0$. Observe that necessarily $t_0 \neq 0$,

and therefore $s_0^2 = \varphi s_1^2$. But as the degrees of s_0^2 and s_1^2 are even, while the degree of φ is odd, this is impossible.

It is worth to note that the claim in (II) od the previous Example can be in part further generalized so that we can have the polynomial $\varphi(X)$ there to be of even degree. Namely we have the following proposition. Its part (ii) shows one more time, on a rather special example, that proving for a particular element to be prime could be a quite demanding task.

PROPOSITION 3.4. *Let A be an integral domain and $\varphi(X) \in A[X]$ a polynomial. Define $p = Y^2 - \varphi(X)$, a polynomial in $R = A[X, Y]$.*

(i) *The polynomial p is irreducible in R if and only if there is no polynomial $\omega(X) \in A[X]$ such that $\omega^2(X) = \varphi(X)$.*
(ii) *Suppose the characteristic* $\operatorname{char} A \neq 2$ *and let then $\varphi(X) = X^4 + aX + b$, where $a, b \in A$ are not both equal to zero. Then p is an irreducible element of R. Furthermore suppose* $\operatorname{char} A \neq 2, 3$ *and $a, b \in A$ are such that $256b^3 \neq 27a^4$. Then p is a prime element of R.*

PROOF. (i) Suppose p is reducible; i.e., there are polynomials $g, h \in R \setminus A^*$ such that $p = gh$. By considering g and h as polynomials in the variable Y, with coefficients from $A[X]$, we have two possibilities. First assume that

$$g = a_0(X) \quad \text{and} \quad h = b_2(X)Y^2 + b_1(X)Y + b_0(X),$$

for some $a_0, b_j \in A[X]$. Then we in particular have that $a_0(X)b_2(X) = 1$, which gives that $g \in A^*$; a contradiction. The second possibility is that

$$g = a_1(X)Y + a_0(X) \quad \text{and} \quad h = b_1(X)Y + b_0(X),$$

for some $a_j, b_j \in A[X]$. Now we have $a_1(X)b_1(X) = 1$, which means that $a_1(X), b_1(X) \in A^*$. With no loss of generality we can take $a_1(X) = b_1(X) = 1$; and so $g = Y + a_0(X)$ and $h = Y + b_0(X)$. But then it is immediate that

$$a_0(X) + b_0(X) = 0 \quad \text{and} \quad a_0(X)b_0(X) = -\varphi(X).$$

Hence by putting $\omega(X) = a_0(X) = -b_0(X)$ we have that $\omega^2(X) = \varphi(X)$; or in other words we have a factorization $p = (Y - \omega(X))(Y + \omega(X))$. This finishes our proof of the implication from right to left, while the opposite one is clear.

(ii) By (i) we just have to show that there is no $\omega \in A[X]$ such that $\omega^2(X) = \varphi(X)$. So assume to the contrary, that there is some such ω and then write it as $\omega(X) = X^2 + uX + v$, with $u, v \in A$. Then it would easily follow that we have

$$2u = 0 = u^2 + 2v, \qquad 2uv = a, \qquad v^2 = b;$$

which is impossible since $\operatorname{char} A \neq 2$ and a, b are not both equal to zero.

For the second claim we proceed as in (II) of Example 3.3. That is suppose $p|fg$ and write $f, g \in A[X]$ as in (3.8). For $s_0, s_1 \in A[X]$ as there we have again the equality

$$s_0^2 = \varphi s_1^2, \tag{3.10}$$

where both s_0 and s_1 are nonzero polynomials. Our goal is to prove that in fact such s_0 and s_1 do not exist. Namely suppose to the contrary and let s_0, s_1 be chosen so that the degree of s_0 is the minimal possible. Then by the division algorithm one more time we can write

$$s_0 = Q_0\varphi + R_0 \quad \text{and} \quad s_1 = Q_1\varphi + R_1, \tag{3.11}$$

where $Q_i, R_i \in A[X]$ and $\deg R_i < 4$ for $i = 1, 2$. Clearly $R_0 \neq 0$, as otherwise it would follow that $s_1^2 = \varphi Q_0^2$, which contradicts to the stated minimality condition. Also if we rewrite (3.10) using (3.11) it is immediate that $\varphi | R_0^2$. Let us show that this is impossible. For that purpose define $\mathbb{K}$ to be the quotient field of A and $\overline{\mathbb{K}}$ be its algebraic closure. Also suppose there is some $\vartheta \in A[X]$ such that $R_0^2 = \varphi\vartheta$. Of course the last equality can be considered as an equality of polynomials in $\overline{\mathbb{K}}[X]$. Observe that R_0^2 has at most three mutually different roots in $\overline{\mathbb{K}}$. We want to show that φ has four mutually different roots in $\overline{\mathbb{K}}$, which will suffice for our argument. For that purpose assume $x_0 \in \overline{\mathbb{K}}$ is a multiple root of φ. Then x_0 is a root of the derivative φ' as well. As we have that $\varphi(x_0) = x_0\varphi'(x_0)$ is equivalent to $x_0^4 = b/3$, it follows at once that $ax_0 = -4b/3$. If $a = 0$, then it is clear that φ cannot have a multiple root. And if $a \neq 0$, we have that $x_0 = -4b/(3a)$. Hence we deduce that

$$0 = \varphi(x_0) = \Big(-\frac{4b}{3a}\Big)^4 + a\Big(-\frac{4b}{3a}\Big) + b,$$

which is equivalent to the equality $256b^3 = 27a^4$; a contradiction. □

Remark 3.5. Note that for our polynomials φ and p in the second claim of (ii) in the previous proposition we have that $p = 0$ can be considered as a hyperelliptic curve over $\mathbb{K}$, which is in fact an elliptic curve (as all the roots of φ in $\overline{\mathbb{K}}$ are simple). Here also note that $256b^3 - 27a^4$ is the discriminant of the polynomial φ.

We conclude the paper with two more examples, where we treat the question of reducibility for some specific polynomials with some "ad hoc methods". For the first one we need the following easy lemma.

Lemma 3.6. *Let B be an integral domain with identity 1_B such that the element $2_B = 1_B + 1_B$ is invertible. Let $f \in B[T]$ be a quadratic polynomial of the form $f(T) = T^2 + \alpha T + \beta$. Then f is reducible if and only if the element $(2_B^{-1}\alpha)^2 - \beta$ is a square in B.*

Proof. Our argument is similar to the one for (i) of the last proposition. Namely suppose f is reducible and $g, h \in B[T] \setminus B^*$ are such that $f = gh$.

We can assume that $g = a_1T + a_0$ and $h = b_1T + b_0$, for some $a_i, b_i \in B$. In fact we can take $a_1 = b_1 = 1_B$. Hence it is immediate that $a_0^2 - \alpha a_0 + \beta = 0$, which can be written in an equivalent form as

$$(a_0 - 2_B^{-1}\alpha)^2 = (2_B^{-1}\alpha)^2 - \beta.$$

Now if $\omega \in B$ is such that ω^2 is equal to the right-hand side of the above equality, then $a_0 \in \{2_B^{-1}\alpha \pm \omega\}$ and $b_0 = \alpha - a_0$. And therefore f is reducible. Clearly we have the opposite implication as well; i.e., if f is reducible, then $(2_B^{-1}\alpha)^2 - \beta$ must be a square in B. □

Example 3.7. (I) Suppose A is an integral domain with identity 1_A such that the element $2_A = 1_A + 1_A$ is invertible. Let also g and h be polynomials from the ring $B = A[X, Y]$ such that the total degree $\deg h$ is odd and greater than $2 \deg g$. Then the polynomial

$$f = Z^2 + g(X, Y)Z + h(X, Y)$$

is irreducible in $R = A[X, Y, Z]$. In order to see that put $\alpha = g$ and $\beta = h$ and then define a polynomial

$$\varphi = (2_A^{-1}\alpha)^2 - \beta.$$

As the degree $\deg \varphi = \deg h$ is odd, it is clear that φ is not a square in the ring B. By the previous lemma we know that then f is an irreducible element in R.

(II) Suppose A is an integral domain and φ is a polynomial from the ring $B = A[X, Y]$ whose total degree is not divisible by 3. Then we claim that the polynomial

$$f = Z^3 + \varphi(X, Y)$$

is irreducible in $R = A[X, Y, Z]$. For that purpose suppose to the contrary, that f is reducible. Then we would have some $a_i, b_j \in B$ so that for the polynomials

$$g = a_2(X, Y)Z^2 + a_1(X, Y)Z + a_0(X, Y) \quad \text{and} \quad h = b_1(X, Y)Z + b_0(X, Y)$$

we have $f = gh$. With no loss of generality we can take that $a_2 = b_1 = 1$. Then we get at once that necessarily

$$a_0 + b_0a_1 = 0 = a_1 + b_0 \quad \text{and} \quad a_0b_0 = \varphi.$$

Hence we obtain that $a_1 = -b_0$, further $a_0 = b_0^2$ and finally $b_0^3 = \varphi$. But the last equality gives in particular that $\deg \varphi = 3 \deg b_0$, which is impossible.

Remark 3.8. As the final remark we would like to say that the last two examples above are just special cases of a more general and powerful technique which enables to treat reducibility questions of polynomials from the polynomial ring $A[X]$, where A belongs to a rather wide class of integral domains. The details will appear in [14].

Acknowledgements.

The author is grateful to his friend and colleague Andrej Dujella for his help during the preparation of this paper. His expert insight and numerous hints, that significantly improved the first version of the paper, were so valuable that cannot be overestimated. The author is also indebted to the referee for the numerous remarks and/or suggestions that improved and clarified the presentation.

This work was supported in part by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004).

References

[1] S. Alaca and K. S. Williams, *Introductory Algebraic Number Theory,* Cambridge Univ. Press, New York, 2004.
[2] P. Bachmann, *Die Analytische Zahlentheorie,* Teubner, Leipzig, 1894.
[3] Z. I. Borevich and I. R. Shafarevich, *Number theory,* Academic Press, New York, 1966.
[4] N. Bourbaki, *Commutative algebra,* Chapters 1–7, Springer-Verlag, New York, 1985.
[5] L. E. Dickson, *History of the Theory of Numbers,* Volume 2: Diophantine analysis, Chelsea, New York, 1966.
[6] A. Dujella, *Number theory,* Školska knjiga, Zagreb, 2021.
[7] A. Fröhlich and M. J. Taylor, *Algebraic number theory,* Cambridge studies in adv. math. 27, Cambridge Univ. Press, 1994.
[8] T. W. Hungerford, *Algebra,* Grad. Texts in Math., Vol. 73, Springer, New York, 1974.
[9] S. Lang, *Algebra,* Third Ed., Addison Wesley, Reading, 1994.
[10] S. MacLane, *The Schonemann-Eisenstein irreducibility criteria in terms of prime ideals,* Trans. Amer. Math. Soc. **43** (1938), 226–239.
[11] J. Neukirch, *Algebraic Number Theory,* Springer, Berlin, 1999.
[12] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An introduction to the theory of numbers,* Wiley, New York, 1991.
[13] J. J. Rotman, *Advanced modern algebra,* Second Ed., Grad. Studies in Math., Vol. 114, Amer. Math. Soc., Providence, 2010.
[14] B. Širola, *A generalization of Dumas-Eisenstein criterion,* in preparation.
[15] P. J. Weinberger, *Real quadratic fields with class numbers divisible by n,* J. Number Th. **5** (1973), 237–241.
[16] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields,* Osaka J. Math. **7** (1970), 57–76.

Prosti elementi u komutativnim domenama

Boris Širola

Sažetak. U radu su prikazani neki rezultati o prostim elementima u integralnim domenama. Posebno se bavimo sljedećim pitanjem: Da li svaki poredak u polju algebarskih brojeva ima beskonačno mnogo prostih elemenata? I onda pokazujemo da je za slučaj realnih kvadratnih polja odgovor na to pitanje potvrdan. Nadalje, dajemo neke parcijalne rezultate i primjere o prostim polinomima u dvije ili više varijabli s koeficijentima iz proizvoljne integralne domene.

B. Širola
Department of Mathematics
University of Zagreb
10 000 Zagreb, Croatia
E-mail: sirola@math.hr