A constructive characterization of maximal ideals in $\mathbb{Z}[X]$

Franziskus Wiesnet

August 6, 2022

Abstract

We give a constructive characterisation of all maximial ideals in $\mathbb{Z}[X]$ using a simple version of Zariski's lemma.

Keywords: material interpretation, constructive algebra, Zariski's lemma

Definition 1. In the setting of this article a RING STRUCTURE $(R, +, \cdot, 0, 1, -, =)$ is a set R equipped with an addition operator $+ : R \times R \to R$, a multiplication operator $\cdot : R \times R \to R$, a zero element $0 \in R$, an one element $1 \in R$, an additive inverse function $- : R \to R$ and an equality $=\subsetneq R \times R$. If furthermore $=$ is an equivalence relation and compatible with $+, \cdot, -$, i.e. $=$ is a congruence relation on $(R, +, \cdot, 0, 1, -)$, and the other ring axioms are fulfilled (w.r.t. the equality $=$), we call R a RING. We call $(K, +, \cdot, 0, 1, -, ^{-1}, =)$ a FIELD STRUCTURE if $(K, +, \cdot, 0, 1, -, =)$ is a ring structure and $^{-1} : K \to K$ is a map. If K is a ring and $xx^{-1} = 1$ for all $x \in K$ with $x \neq 0$, we call K a field.

The notions DISCRETE RING STRUCTURE and DISCRETE FIELD STRUCTURE are analogously defined as discrete rings and discrete fields, respectively. In particular, if a structure is discrete, we can freely use their operators in the algorithms.

Since the notations of $+, \cdot, 0, 1, -,^{-1}$ and $=$ will not change, we suppress them in the notation and say that R is a ring (structure) or K is a field (structure). A HOMOMORPHISM $\phi : R \to S$ between two ring structures R and S is a map which preserves the structure in the canonical way.

For a ring structure R we define the RING STRUCTURE OF POLYNOMIALS $R[X]$ with coefficients in R by the well-known construction. Formally the underling set of $R[X]$ is the set R^* of all finite sequences in R.

An ALGEBRA STRUCTURE R over a field structure K, or short K-algebra structure, is a ring structure together with a map $K \to R$. If R is a ring, K is a field and the map $K \to R$ is a homomorphism, we call it K-ALGEBRA. For a K-algebra R and $x_1, \dots, x_n \in R$ we get an extension $K[X_1, \dots, X_n] \to R$ of the homomorphism by $X_i \mapsto x_i$. We denote the image by $K[x_1, \dots, x_n]$, where an element is in the image of a homomorphism if it is equal (w.r.t. $=$) to a value of the homomorphism.

Definition 2. We call a ring (structure) R DISCRETE if $=$, $+$, $-$ and $\cdot$ are computable. Hereby $=$ is seen as a boolean valued function. A field (structure) K is called discrete if it is discrete as ring and a^{-1} is computable. Here "computable" means that the equality is decidable and we can use the operators freely in our algorithms. In particular, the equality can be seen as a boolean valued function and we have $a = b \vee a \neq b$ for all a, b in the ring even if a and b are terms which contains $+, -, \cdot$ and $^{-1}$. An algebra (structure) R over a field structure K is called discrete, if R and K are discrete and the map $K \to R$ is computable.

In the following we assume that everything is discrete.

Definition 3. Let R be a ring. For $M \subsetneq R$ and $\nu : R \to R$, (M, ν) is called an EXPLICIT MAXIMAL IDEAL if for all $x \in R \setminus M$

$$x\nu(x) - 1 \in M.$$

Definition 4. Let K be a field structure, R a K-algebra structure and $x \in R$. A map $\iota : K[X] \to K[X]$ is called an ALGEBRAIC INVERSE ON $K[x]$ FUNCTION if

$$(\iota(f))(x)f(x) - 1 = 0$$

for all $f \in K[X]$ with $f(x) \neq 0$.

Definition 5. Here and in the rest of this chapter let a numeration of the field axioms, ring axioms and algebra axioms be given.

For a field structure K we say that there is an EVIDENCE THAT K IS NOT A FIELD if there is a concrete counter example that one of the field axiom is not full field. Such a counter example consist of the number i of the not fulfilled axiom and a list of elements in K with constitute this counterexample. Analogously, we define the notion that there is an EVIDENCE THAT R IS NOT A RING for a given ring structure and that there is an EVIDENCE THAT R IS NOT A K-ALGEBRA for a given field structure K, a given ring structure R and a map from K to R (i.e. a K-algebra structure R).

For a given field structure K, $\vec{x} \in K$ and a map $\iota : K[\vec{X}] \to K[\vec{X}]$, an EVIDENCE THAT ι IS NOT AN ALGEBRAIC INVERSE FUNCTION ON $K[\vec{x}]$ is an $f \in K[\vec{X}]$ such that $f(\vec{x}) \neq 0$ and $f(\vec{x})(\iota(f))(\vec{x}) - 1 \neq 0$.

Algorithm 1. Given a discrete field structure K, a discrete K-algebra structure R, $x \in R$ and $\iota : K[X] \to K[X]$, we compute an element $f \in K[X]$ as follows:

$$f := \begin{cases} X & \text{if } \ x = 0 \\ X\iota(X) - 1 & \text{if } \ x \neq 0 \end{cases}$$

Lemma 1. In the situation of Algorithm 1 let $f = 0$ or $f(x) \neq 0$. Then one of the following statements holds:

- There is evidence that K is not a field.
- There is evidence that R is not a K-algebra.
- There is evidence that ι is not an algebraic inverse function on $K[x]$.

Proof. As in Algorithm 1 we consider the cases $x = 0$ and $x \neq 0$:

Case 1: If $x = 0$, we have $f = X$, which is an abbreviation for $1X$.

Case 1.1: If $f = 0$ it follows $1 = 0$ in K which gives an evidence that K is not a field.

Case 1.2: If $f(x) \neq 0$ then $1 \cdot 0 \neq 0$ in R. This provides a counterexample to the axiom that 1 is the neutral element of the multiplication.

Case 2: $f = X\iota(X) - 1$.

Case 2.1: First we assume $f = 0$ and consider the constant coefficients of this polynomial equation and receive $-1 = 0$ in K. It follows that either $-1 + 1 = 0 + 1$ or we have a counterexample that the equality is not compatible with the addition. Hence, either we have a counterexample to the axiom that $-$ is the additive inverse function and we are done, or $-1 + 1 = 0$, and hence either we have a counterexample that to the axiom that 0 is the neutral element of the addition or $0 - 1 = 0$. Together, either we have a counterexample that the equality is not transitive, or $0 = 1$. Finally, either there is a counterexample to the symmetry axiom of the equality or $1 = 0$ and we have a counterexample to the axiom $1 \neq 0$.

Cases 2.2: Now we assume $f(x) \neq 0$. It follows either $f(x) = (X\iota(X) - 1)(x) = x\iota(X)(x) - 1$ or we get a counterexample to one of the ring axioms. (Details are left to the reader.) In the last case we are done. In the first case we have either $x\iota(X)(x) - 1 = 0$ and get an counterexample to the transitivity of the equality or there is evidence that ι is not an algebraic inverse function. $\square$

Theorem 1. Let (M, ν) be an explicit maximal ideal in $\mathbb{Z}[X]$, then $M = \langle p, f \rangle$ such that p is a prime and f irreducible in $(\mathbb{Z}/p\mathbb{Z})[X]$.

Proof. Our first aim is to compute the prime number p.

We consider the map $\phi : \mathbb{Q}[X] \to \mathbb{Z}[X]/M, \sum_i \frac{p_i}{q_i} X^i \mapsto \sum_i p_i \nu(q_i) X^i$. This turns $\mathbb{Z}[X]/M$ into a $\mathbb{Q}$-algebra structure.

Furthermore, we define $\iota : \mathbb{Q}[X] \to \mathbb{Q}[X]$ as follows:

Given some $f = \sum_i \frac{p_i}{q_i} X^i \in \mathbb{Q}[X]$. Define $d := \prod_i p_i$ and $d_i := \prod_{j \neq i} q_i$ and return $\iota(f) := d \cdot \nu(\sum_i p_i d_i X^i)$.

We apply Algorithm 1 to $\mathbb{Q}$, $\mathbb{Z}[X]/M$, $\overline{X} \in \mathbb{Z}[X]/M$ and ι. The algorithm returns $f \in \mathbb{Q}[X]$ with the property from in Lemma 1. And consider several cases.

Case 1: If $f \neq 0$ and $f(\overline{X}) = 0$, we get $f = \sum_i \frac{p_i}{q_i} X^i \in \mathbb{Q}[X]$ such that $g := \sum p_i \nu(q_i) X^i \in M \subseteq \mathbb{Z}[X]$. If $g \neq 0$, let d be the leading coefficient of g. Then $\mathbb{Z}[d^{-1}] \subseteq \mathbb{Z}[X]/M$ is a integral extension, where $\mathbb{Z}[X]/M$ is a field. Hence, $\mathbb{Z}[d^{-1}]$ is a field. This cannot happen. Therefore, $g = 0$, where as $f \neq 0$. Let $\frac{a}{b}$ be the leading coefficient of f. Then $\nu(b) = 0$, and therefore $b \in M$. As M is maximal, one prime factor of b must be in M. Hence, we have a prime number $p \in M$ in this case.

Case 2: If $f = 0$ or $f(\overline{X}) \neq 0$, then one of the three properties of Lemma 1 holds:

Case 2.1: The first property can not hold, as $\mathbb{Q}$ is indeed a field.

Case 2.2: Assume that the second property hold, then there is evidence, that $\mathbb{Z}[X]/M$ is not a $\mathbb{Q}$ algebra. As $\mathbb{Q}$ and $\mathbb{Z}[X]/M$ are indeed fields and therefore rings, it follows that there is evidence the map $\phi : \mathbb{Q}[X] \to \mathbb{Z}[X]/M, \sum \frac{p_i}{q_i} X^i \mapsto \sum p_i \nu(q_i) X^i$ is not a homomorphism. In particular,

- $\phi(1) \neq 1$ or
- there are $f, g \in \mathbb{Q}[X]$ with $\phi(fg) \neq \phi(f)\phi(g)$ or
- there are $f, g \in \mathbb{Q}[X]$ with $\phi(f+g) \neq \phi(f) + \phi(g)$.

We have $\phi(1) = 1\nu(1) = 1$ in $\mathbb{Z}[X]/M$, hence only the last two properties can hold. Once can easily check by using the proprety of ν that $\phi(fg) = \phi(f)\phi(g)$ and $\phi(f+g) = \phi(f) + \phi(g)$ if for all coeeficents $\frac{a}{b}$ of f and g, $b \notin M$. Hence, there must be a coefficent of $\frac{a}{b}$ of some given $f \in \mathbb{Q}[X]$ such that $b \in M$. Hence, there is a prime factor p of b which is in M.

Case 2.3: Assume that there is evidence that ι is not an algebraic inverse function. In particular, there is some $f = \sum_i \frac{p_i}{q_i} X^i$ such that $F = \sum_i p_i \nu(q_i) X^i \notin M$ and $FG - 1 \notin M$ for $G := d \cdot \nu(\sum_i p_i d_i X^i)$, $d := \prod_i q_i$ and $d_i := \prod_{j \neq i} q_j$. If one $q_i \in M$, we are done as then there must be a prime divisor p of this q_i such that $p \in M$. Hence, it surfices to show that $q_i \notin M$ for all i cannot be the case:
If this were the case, also $d \notin M$ and $d_i \notin M$ for all i, as M is a maximal ideal. It follows $d \cdot F \notin M$ and $d \cdot F = \sum_i p_i d_i X^i \mod M$. Therefore, $\sum_i p_i d_i X^i \notin M$. By the property of ν we get $\sum_i p_i d_i X^i \cdot \nu(\sum_i p_i d_i X^i) - 1 \in M$. This is a contradiction to $FG - 1 \notin M$.

Hence, in each case we have found a prime number p such that $p \in M$.

Now we compute some $f \in \mathbb{Z}[X]$ with $\langle p, f \rangle = M$:

As $p \in M$ we have an epimorphism $\phi : (\mathbb{Z}/p\mathbb{Z})[X] \to \mathbb{Z}[X]/M$. We consider $X \in \mathbb{Z}[X]$ and consider two cases:

Case 1: If $X \in M$ we define $f := X$.

Case 2: If $X \notin F$, we consider $g := X\nu(X) - 1$. As $-1 \notin M$, we have $\deg(g) \geq 1$ and in particular $g \neq 0$. Furthermore, g seen in $(\mathbb{Z}/p\mathbb{Z})[X]$ is not zero as the constant coefficient is -1. However $\phi(g) = 0$. Therefore, g is in the kernel of ϕ and hence a monic and irreducible factor of $g \in (\mathbb{Z}/p\mathbb{Z})[X]$ must be in the kernel of ϕ. We define f to be a lifting of this factor in $\mathbb{Z}[X]$.

Hence, we have $\langle p, f \rangle \subseteq M$ for a prime number p and $f \in \mathbb{Z}[X]$ such that $f \in (\mathbb{Z}/p\mathbb{Z})[X]$ is irreducible.

We show that $M \subseteq \langle p, f \rangle$: Let $g \in M$ be given. We consider $h := \gcd(f, g) \in (\mathbb{Z}/p\mathbb{Z})[X]$. As $(\mathbb{Z}/p\mathbb{Z})[X]$ is an euclidean ring, we get $g_1, g_2 \in (\mathbb{Z}/p\mathbb{Z})[X]$ with $h = g_1 g + g_2 f$. Lifting this equality to $\mathbb{Z}[X]$, we get $h = f_1 g + f_2 f + f_3 p$ for some $f_1, f_2, f_3 \in \mathbb{Z}[X]$. Furthermore, we have either $h = f$ or $h = 1$, since f is irreducible in $(\mathbb{Z}/p\mathbb{Z})[X]$. In the first case, $g \in \langle p, f \rangle$, in the second case we have $1 \in M$, which can not be. Hence $M = \langle p, f \rangle$. $\square$