A material interpretation of maximal ideals in $\mathbb{Z}[X]$

Franziskus Wiesnet

May 6, 2023

Abstract

This article is about a constructive characterization of the maximal ideal in $\mathbb{Z}[X]$. First, a classical formulation of the theorem and a proof are given, which is transformed into a constructive proof.

Keywords: material interpretation, constructive algebra, program extraction

Theorem 1. Let $M \subseteq \mathbb{Z}[X]$ be a maximal ideal. Then there is a prime number p with $p \in M$.

Proof. If $X \notin M$, there is some $g \in \mathbb{Z}[X]$ with $gX - 1 \in M$ because M is a maximal ideal. $gX - 1$ is not constant as the constant coefficient is -1 and g cannot be 0. Hence, in both cases ($X \in M$ and $X \notin M$) there is some non constant $f \in M$. Let d be the leading coefficient of f.

We now assume that there is no prime number p with $p \in M$. As M is a maximal and hence a prime ideal, it follows $M \cap \mathbb{Z} = \{0\}$. Hence the canonical homomorphism $\mathbb{Z} \to \mathbb{Z}[X]/M$ is injective and induces a ring extension $\mathbb{Z}[d^{-1}] \to \mathbb{Z}[X]/M$. This is an integral ring extension with the integral polynomial $d^{-1}f$. As $\mathbb{Z}[X]/M$ is a field, also $\mathbb{Z}[d^{-1}]$ must be field. This is not possible. $\square$

Lemma 1. Let $f, g \in \mathbb{Z}[X]$ be given and $d \neq 0$ be the leading coefficient of f. Then there is $k \in \mathbb{N}$ and $h \in \mathbb{Z}[X]$ such that $\deg(d^k g + hf) < \deg(f)$

Proof. Let $m := \deg(f)$ and $n := \deg(g)$. For fix m use induction on n. If $n < m$, we take $k := 0$ and $h := 0$. Otherwise, let c be the leading coefficient of g. Then $\deg(dg - cx^{n-m}f) < n$, hence we get k' and h' such that $\deg(d^{k'}(dg - cx^{n-m}f) + h'f) < m$. Hence, $k := k' + 1$ and $h := h' - d^{k'}cx^{n-m}$ do the trick. $\square$

Definition 1. Let R be a ring. For a subset $M \subseteq R$ and a function $\nu : R \to R$, we say that (M, ν) is an EXPLICIT MAXIMAL IDEAL if M is an ideal, $1 \notin M$ and $a\nu(a) - 1 \in M$ for all $a \in R \setminus M$.

Furthermore, we say that there is EVIDENCE THAT (M, ν) IS NOT AN EXPLICIT MAXIMAL IDEAL if one of the following cases holds:

- $0 \notin M$,
- there are $a, b \in M$ with $a + b \notin M$,
- there are $\lambda \in R$ and $a \in M$ with $\lambda a \notin M$,
- $1 \in M$, or
- there is $a \in R \setminus M$ with $a\nu(a) - 1 \notin M$.

Lemma 2. Let R be a ring, $M \subseteq R$, $\nu : R \to R$ and $a_1, \dots, a_n \in R$ with $a_1 \dots a_n \in M$ be given. Then, either there is an $a_i \in M$, or there is evidence that (M, ν) is not an explicit maximal ideal. In heuristic terms: Each explicit maximal ideal is an explicit prime ideal.

Proof. Induction over n. For $n = 0$ it follows $1 \in M$, which is evidence that (M, ν) is not an explicit maximal object. For the induction step, let $a_1 \dots a_n a_{n+1} \in M$. If $a_{n+1} \in M$, we are done. Otherwise, either $a_{n+1}\nu(a_{n+1}) - 1 \in M$ or there is evidence that (M, ν) is not an explicit maximal ideal. This and $a_1 \dots a_n a_{n+1} \in M$ imply that either $a_1 \dots a_n a_{n+1}\nu(a_{n+1}), -a_0 \dots a_n a_{n+1}\nu(a_{n+1}) + a_0 \dots a_n \in M$ or there is evidence that (M, ν) is not an explicit maximal ideal. It follows that $a_0 \dots a_n \in M$ or there is evidence that (M, ν) is not an explicit maximal ideal. By applying the induction hypothesis to $a_0 \dots a_n \in M$, the proof is finished. $\square$

Theorem 2. Let $M \subseteq \mathbb{Z}[X]$ and $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$ be given. Then, either there exists a prime number $p \in M$, or there is evidence that (M, ν) is not an explicit maximal ideal in $\mathbb{Z}[X]$.

Proof. First we construct some non constant $f \in M$: If $X \in M$ we are done. Otherwise, $X\nu(X) - 1 \in M$ or there is a witness that (M, ν) is not an explicit maximal ideal. Let d be the leading coefficient of f and $n := \deg(f)$. We take some prime number q which is no divisor of d and consider $\nu(q) \in \mathbb{Z}[X]$. We check if $q \in M$ or $m := q\nu(q) - 1 \notin M$, if yes, we are done. Otherwise, we continue:

For each $i \in \{0, \dots, n-1\}$ we apply $\nu(p)x^i$ to Lemma 1 and get some $k_i \in \mathbb{N}$, $h \in \mathbb{Z}[X]$ and $(a_{ij})_{j \in \{0,\dots,n-1\}} \in \mathbb{Z}^{n \times n}$ with

$$d^{k_i}\nu(q)x^i + h_i f = \sum_{j=0}^{n-1} a_{ij}x^j.$$

Using the Kronecker delta $(\delta_{ij})_{ij}$ we get

$$\sum_{j=0}^{n-1}(d^{k_i}\nu(q)\delta_{ij} - a_{ij})x^j = -h_i f.$$

Let A be the matrix $(d^{k_i}\nu(q)\delta_{ij} - a_{ij})_{i,j\in\{0,\dots,n-1\}}$ then we have

$$A \begin{pmatrix} 1 \\ x \\ \vdots \\ x^{n-1} \end{pmatrix} = \begin{pmatrix} -h_0 f \\ -h_1 f \\ \vdots \\ -h_{n-1} f \end{pmatrix}$$

Multiplying both sides by the adjugate matrix $\hat{A}$ of A and using $\hat{A}A = \det(A)I$ leads to

$$\begin{pmatrix} \det(A) \\ \det(A)x \\ \vdots \\ \det(A)x^{n-1} \end{pmatrix} = \hat{A} \begin{pmatrix} -h_0 f \\ -h_1 f \\ \vdots \\ -h_{n-1} f \end{pmatrix}$$

In particular, the first line is $\det(A) = -\sum_{j=0}^{n-1} \hat{A}_{0j}h_j f$. Looking at the definition of A, we have $\det(A) = d^K\nu(q)^n + b_{n-1}\nu(q)^{n-1} + \cdots + b_1\nu(q) + b_0$ for some $b_0, \dots, b_{n-1} \in \mathbb{Z}$ and $K := \sum k_i$. Hence,

$$d^K\nu(q)^n + b_{n-1}\nu(q)^{n-1} + \cdots + b_1\nu(q) + b_0 = \sum_{j=0}^{n-1}(-\hat{A}_{0j}h_j)f.$$

Multiplying both sides with q^n leads to

$$d^K(q\nu(q))^n + b_{n-1}q(q\nu(q))^{n-1} + \cdots + b_1 q^{n-1}(q\nu(q)) + b_0 q^n = \sum_{j=0}^{n-1}(-q^n\hat{A}_{0j}h_j)f$$

We define $m := q\nu(q) - 1$ which is equvialent to $q\nu(q) = m + 1$. For each $i \in \{1, \dots, n\}$ one can easily compute some polynomial g_i with $(m+1)^i = 1 + mg_i$. This leads to

$$d^K + b_{n-1}q + \cdots + b_1 q^{n-1} + b_0 q^n = \sum_{j=0}^{n-1}(-q^n\hat{A}_{0j}h_j)f + (-d^K g_n - b_{n-1}qg_{n-1} - \cdots - b_1 q^{n-1}g_1)m$$

As the left hand side is in $\mathbb{Z}$ also the right hand side is. Furthermore, the left hand side can not be zero as otherwise $q \mid d$ (or $q \mid 1$ if $K = 0$). By Lemma 2 one prime factor is in M or their is evidence that (M, ν) is not an explicit maximal ideal. □