Maximal ideals in $\mathbb{Z}[x]$

A bit of notation and background: Given a polynomial $f(x) \in \mathbb{Z}[x]$ and a prime p, we denote by $\bar{f} \in \mathbb{F}_p[x]$ the polynomial obtained by reducing the coefficients of f mod p. For example, if $f(x) = 100x^3 + 3x^2 + 5x - 1$ and $p = 3$, then $\bar{f} = x^3 + 2x + 2$.

We will also review a version of the Gauss Lemma. This is not strictly necessary for our discussion, but is convenient. We call a polynomial in $\mathbb{Z}[x]$ *primitive* if its coefficients are relatively prime. Note that any non-zero polynomial $f(x) \in \mathbb{Q}[x]$ has a constant multiple $cf(x) \in \mathbb{Z}[x]$ which is primitive.

Lemma 0.1. *If $f, g \in \mathbb{Z}[x]$ are both primitive, then fg is also primitive.*

Proof. Suppose p is a prime dividing the coefficients of fg. Then reducing mod p, we would have $\bar{f}\bar{g} = 0$ in $\mathbb{F}_p[x]$. But $\mathbb{F}_p[x]$ is an integral domain, so this implies $\bar{f} = 0$ or $\bar{g} = 0$. Hence, p must divide all coefficients of f or of g, contradicting primitivity. □

Corollary 0.2. *Suppose $0 \neq a \in \mathbb{Z}[x]$ is a multiple in $\mathbb{Q}[x]$ of the primitive polynomial $g \in \mathbb{Z}[x]$. Then a is a multiple of g in $\mathbb{Z}[x]$.*

Proof. We are assuming that $a = fg$ with $f \in \mathbb{Q}[x]$. Write $f = cf_1$, where $f_1 \in \mathbb{Z}[x]$ is primitive and $c \in \mathbb{Q}^*$. So $a = cf_1g$. Since $a \in \mathbb{Z}[x]$, we know that $cb_i \in \mathbb{Z}$ for every coefficient b_i of f_1g. But by the previous lemma, we know that the b_i are relatively prime. So we can find integers n_i such that $\sum_i n_ib_i = 1$. This implies that $c = c(\sum_i n_ib_i) = \sum_i n_i(cb_i)$ is an integer. So $f \in \mathbb{Z}[x]$. □

Corollary 0.3. *Suppose $f(x) \in \mathbb{Z}[x]$ is a primitive polynomial and denote by $f(x)\mathbb{Q}[x]$ the ideal it generates in $\mathbb{Q}[x]$. Then $[f(x)\mathbb{Q}[x]] \cap \mathbb{Z}[x] = f(x)\mathbb{Z}[x]$, the ideal generated by $f(x)$ in $\mathbb{Z}[x]$.*

Of course, we are denoting the ideal generated by a polynomial in a slightly cumbersome manner in the previously corollary to avoid confusion about the ring in which the ideal sits.

Proposition 0.4. *Let $M \subset \mathbb{Z}[x]$ be a maximal ideal. Then M is of the form*

$$M = (p, f(x)) \tag{0.1}$$

where $f \in \mathbb{Z}[x]$ is a polynomial such that $\bar{f}(x) \in \mathbb{F}_p[x]$ is irreducible.

To put it differently, to generate a maximal ideal in $\mathbb{Z}[x]$, we should choose a prime p and an irreducible polynomial $f_0 \in \mathbb{F}_p[x]$. We then lift f_0 any way we want to a polynomial $f \in \mathbb{Z}[x]$, that is, so that $\bar{f} = f_0$. Then $(p, f) \subset \mathbb{Z}[x]$ is a maximal ideal, and all maximal ideals are obtained in this way. By the way, you should check that the ideal is independent of the choice of lift f.
Here are some examples:

$$(2, x^2 + x + 1) = (2, x^2 + 3x - 1) \tag{0.2}$$

$$(3, x^3 + x^2 + 2) \tag{0.3}$$

$$(5, x^2 - 3) \tag{0.4}$$

We now proceed to prove the proposition. Firstly, given p and f as in the proposition, we have

$$\mathbb{Z}[x]/(p, f(x)) = \mathbb{F}_p[x]/(\bar{f}(x)).$$

The second quotient ring is a field since $\bar{f}$ is assumed irreducible. So $(p, f(x))$ is a maximal ideal.
Now assume that $M \subset \mathbb{Z}[x]$ is an arbitrary maximal ideal and denote by k the quotient ring $\mathbb{Z}[x]/M$, which of course is a field. Consider the composition

$$\phi : \mathbb{Z} \to k := \mathbb{Z}[x]/M \tag{0.5}$$

of the two natural maps

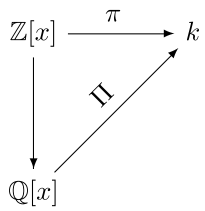
$$i : \mathbb{Z} \hookrightarrow \mathbb{Z}[x] \tag{0.6}$$

and

$$\pi : \mathbb{Z}[x] \to k. \tag{0.7}$$

Lemma 0.5. *The map ϕ is not injective.*

Proof. (of Lemma) Suppose ϕ were injective. Then, since k is a field, ϕ would extend to an injection $\Phi : \mathbb{Q} \hookrightarrow k$. By sending x to the element $\pi(x)$, we see therefore that the natural projection π also extends to a homomorphism $\Pi : \mathbb{Q}[x] \rightarrow k$:



The map Π is clearly surjective, since π already is. Now, if Π were injective, we would have an isomorphism $\mathbb{Q}[x] \simeq k$, which we can't because $\mathbb{Q}[x]$ is not a field. Therefore, $Ker(\Pi) = (g(x))$ for a non-zero polynomial g, which must then be irreducible. By replacing g with a non-zero constant multiple, we can assume that g is a primitive polynomial in $\mathbb{Z}[x]$. We thus have an isomorphism

$$\mathbb{Q}[x]/(g) \simeq k.$$

But this would imply that the natural map $\mathbb{Z}[x] \hookrightarrow \mathbb{Q}[x]$ induces a surjection

$$\mathbb{Z}[x] \rightarrow \mathbb{Q}[x]/(g).$$

By corollary (0.3), this would induce an isomoprhism

$$\mathbb{Z}[x]/(g) \simeq \mathbb{Q}[x]/(g).$$

It should be plausible that this is a contradiction, as we will now go on to show. Write

$$g(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0$$

with $a_n \neq 0$. Therefore, in $\mathbb{Q}[x]/(g)$ we have

$$a_n \bar{x}^n + \cdots a_1 \bar{x} + a_0 = 0.$$

So we could write

$$\bar{x}^n = (-a_{n-1}/a_n)\bar{x}^{n-1} + \cdots + (-a_1/a_n)\bar{x} + (-a_0/a_n).$$

That is, $\bar{x}^n$ can be written as a linear combination of the lower powers with coefficients in $\mathbb{Z}[1/a_n]$. Using this and an easy induction, we deduce that any element of $\mathbb{Q}[x]/(g)$ can be written as a linear combination of elements in the set

$$B = \{1, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}\}$$

with coefficients in $\mathbb{Z}[1/a_n]$. However,

B is linearly independent in $\mathbb{Q}[x]/(g)$.

This is clear since a linear relation

$$\sum_{i=0}^{n-1} c_i \bar{x}^i = 0$$

implies

$$\sum_{i=0}^{n-1} c_i x^i \in (g(x)).$$

But then, by examining degrees, we must have $c_i = 0$ for all i. Now take any prime p that doesn't divide a_n. Then $1/p$ cannot be spanned by B with coefficients in $\mathbb{Z}[1/a_n]$. □

We return to the proposition. We know now that $Ker(\phi) = (n)$ for some n non-zero. However, since the image of ϕ is an integral domain n must be a prime p. Therefore, we must have $p \in M$ for some prime p. Recall that the maximal ideals in $\mathbb{Z}[x]$ that contain p are in bijection with the maximal ideals in $\mathbb{Z}[x]/p \simeq \mathbb{F}_p[x]$. So $M/(p) = (f_0(x))$ for an irreducible polynomial $f_0 \in \mathbb{F}_p[x]$. But then $M = (p, f)$ for any lift f of f_0, as was to be shown.