On the unit group of $\mathbb{Z}_4[x]$.

R. C. Daileda

August 28, 2017

We begin with the statement and proof of our first main result.

Theorem 1. *The unit group of* $\mathbb{Z}_4[x]$ *is*

$$\mathbb{Z}_4[x]^\times = \{2q(x) + 1 \,|\, q(x) \in \mathbb{Z}_4[x]\}.$$

Every element of $\mathbb{Z}_4[x]^\times$ *is its own inverse, i.e. the exponent of* $\mathbb{Z}_4[x]^\times$ *is 2.*

Proof. First note that, since all polynomials have coefficients in $\mathbb{Z}_4$, for any $q(x) \in \mathbb{Z}[x]$ we have

$$(2q(x) + 1)^2 = 4q(x)^2 + 4q(x) + 1 = 1,$$

which proves that $2q(x) + 1 \in \mathbb{Z}_4[x]^\times$. Conversely, let $p(x), q(x) \in \mathbb{Z}_4[x]^\times$ with $p(x)q(x) = 1$. By putting each coefficient in either the form $2k$ or $2k + 1$, it is not difficult to see that we may write

$$\begin{aligned} p(x) &= 2a(x) + b(x), \\ q(x) &= 2c(x) + d(x), \end{aligned} \tag{1}$$

where $a(x), b(x), c(x), d(x) \in \mathbb{Z}_4[x]$ and the (nonzero) coefficients of $b(x)$ and $d(x)$ are all 1. Multiplying these expressions together gives

$$2(a(x)d(x) + b(x)c(x)) + b(x)d(x) = 1. \tag{2}$$

If $b(x)$ or $d(x)$ had positive degree, then the leading term of $b(x)d(x)$ would be x^n for some $n \in \mathbb{N}$. But then the coefficient of x^n on the left hand side of (2) would have the form $2k + 1 \neq 0$, making equation (2) impossible. We conclude, then, that

$$b(x) = d(x) = 1, \tag{3}$$
$$2(a(x)d(x) + c(x)b(x)) = 0. \tag{4}$$

Equation (4) yields

$$0 = 2(a(x)d(x) + c(x)b(x)) = 2(a(x) + c(x)) \;\Rightarrow\; 2a(x) = -2c(x) = 2c(x).$$

Returning to (1) we finally find that

$$p(x) = 2a(x) + 1 = 2c(x) + 1 = q(x),$$

completing the proof. □

Theorem 1 shows that we can construct all of the units in $\mathbb{Z}_4[x]$ by simply choosing arbitrary polynomials, doubling them and then adding 1. We use this operation to define a map

$$\begin{aligned} \phi : \mathbb{Z}_4[x] &\to \mathbb{Z}_4[x]^\times, \\ q(x) &\mapsto 2q(x) + 1. \end{aligned}$$

Because of its nature, we can use ϕ to further elucidate the structure of $\mathbb{Z}_4[x]$.

Proposition 1. *The map ϕ is an epimorphism of abelian groups with kernel $2\mathbb{Z}_4[x] = \{2s(x) \mid s(x) \in \mathbb{Z}_4[x]\}$.*

Proof. We have already established the surjectivity of ϕ. To see that it is operation preserving let $q(x), r(x) \in \mathbb{Z}_4[x]$. We then have

$$\phi(q(x) + r(x)) = 2(q(x) + r(x)) + 1 = (2q(x) + 1)(2r(x) + 1) = \phi(q(x))\phi(r(x))$$

as needed. To prove the statement about the kernel, if $\phi(q(x)) = 1$, then $2q(x) = 0$. This can only occur if every (nonzero) coefficient of $q(x)$ is 2. Hence $q(x) = 2s(x)$ for some $s(x) \in \mathbb{Z}_4[x]$. □

We are now ready for our second main result.

Theorem 2. *We have*

$$\mathbb{Z}_4[x]^\times \cong \bigoplus_{m \in \mathbb{N}} \mathbb{Z}_2.$$

Proof. According to Proposition 1

$$\mathbb{Z}_4[x]^\times \cong \mathbb{Z}_4[x]/\ker\phi = \mathbb{Z}_4[x]/2\mathbb{Z}_4[x] \cong \mathbb{Z}_2[x].$$

Since the latter group is (additively) isomorphic to $\bigoplus_{m \in \mathbb{N}} \mathbb{Z}_2$, the result follows. □