Slide #6.

(1) Write

$$\begin{cases} f = q_1 h + r & \text{where either } \deg r < \deg h \text{ or } r = 0. \\ g = q_2 h + s & \text{where either } \deg s < \deg h \text{ or } s = 0. \end{cases}$$

Note that $r = f \bmod h$ and $s = g \bmod h$. Hence,

$$f + g = (q_1 + q_2)h + (r + s)$$

where either $\deg(r + s) < \deg h$ or $r + s = 0$. That is,

$$[f + g]_h = r + s = [f]_h + [g]_h.$$

(2) Notation as in (1), we have:

$$f \cdot g = h \cdot (\cdots) + rs.$$

However, it is not necessarily true that $\deg rs < \deg h$ or $rs = 0$. So we write $rs = q_3 h + t$ where either $\deg t < \deg h$ or $t = 0$. That is, $t = rs \bmod h$. Then

$$f \cdot g = h \cdot (\cdots) + \underbrace{q_3 h + t}_{rs} = h \cdot (\cdots) + t,$$

whence $(fg) \bmod h = t = (rs) \bmod h$. That is,

$$[f \cdot g]_h = [rs]_h = [[f]_h \cdot [g]_h]_h.$$

Slide #9. Proof of the **Remark**:

Suppose $f \equiv g \pmod{h}$. By definition,

$$\begin{cases} f = q_1 h + r \\ g = q_2 h + r, \end{cases}$$

where either $\deg r < \deg h$ or $r = 0$. Thus, $f + g = k \cdot h$, where $k = q_1 + q_2$.

Conversely, suppose $f + g = k \cdot h$. That is,

$$(f + g) \text{ mod } h = 0. \quad (*)$$

Let

$$\begin{cases} f = q_1 h + r \ \text{ where either } \deg r < \deg h \text{ or } r = 0. \\ g = q_2 h + s \ \text{ where either } \deg s < \deg h \text{ or } s = 0. \end{cases}$$

Then $f + g = (q_1 + q_2) \cdot h + (r + s)$ where either $\deg(r + s) < \deg h$ or $r + s = 0$. This implies that $(f + g) \text{ mod } h = r + s$. From $(*)$, we now have $r + s = 0$.

Slide #14. Proof of Property ❶ : Recall that

$$\pi(v)(x) = [x \cdot v(x)]_{[x^n+1]}.$$

Then:

$$\begin{aligned}\pi^2(v) &= \pi(\pi(v)) = \pi([x \cdot v(x)]_{[x^n+1]}) \\ &= [x \cdot [x \cdot v(x)]_{[x^n+1]}]_{[x^n+1]} \\ &= [[x]_{[x^n+1]} \cdot [x \cdot v(x)]_{[x^n+1]}]_{[x^n+1]} \\ &= [x^2 \cdot v(x)]_{[x^n+1]}\end{aligned}$$

Now one can proceed by mathematical induction to show that

$$\pi^i(v)(x) = [x^i \cdot v(x)]_{[x^n+1]}$$

for any $i \geq 3$.

Slide #16. Proof of Theorem 4.2.13 part 3:
($\Longrightarrow$) Suppose $c(x) \in C$. Long divide $c(x)$ by $g(x)$:

$$c(x) = a(x) \cdot g(x) + r(x),$$

where $\deg a(x) < n - \deg g(x)$ and either $\deg r(x) < \deg g(x)$ or $r(x) = 0$. Since both $c(x)$ and $a(x) \cdot g(x)$ belong to C, then $r(x) \in C$. Since $g(x)$ is the polynomial of smallest degree in C, we have $r(x) = 0$.

($\Longleftarrow$) Suppose $a(x)$ is any polynomial in $K[x]$ of degree less than $n - \deg g(x)$. By Property ❷ on slide #14, we have $a(x) \cdot g(x) \in C$. $\square$

Slide #17. Proof of Theorem 4.2.13 parts 1 & 2:
Let $k = n - r$, where $r = \deg g$. The polynomials $g(x), x \cdot g(x), \ldots, x^{k-1} \cdot g(x)$ all belong to C and they are linearly independent: Indeed, suppose there exist $a_0, a_1, \ldots, a_{k-1}$, not all zero, such that

$$a_0 \cdot g(x) + a_1 x \cdot g(x) + \cdots + a_{k-1} x^{k-1} \cdot g(x) = 0.$$

This is equivalent to saying that $a(x) \cdot g(x) = 0$ for some nonzero polynomial $a(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}$, which is a contradiction. Thus, $a(x) = 0$. From Theorem 4.2.13 part 3, we know that any $c(x) \in C$ can be written as $a(x) \cdot g(x)$ where

$$a(x) = a_0 \cdot g(x) + a_1 x \cdot g(x) + \cdots + a_{k-1} x^{k-1} \cdot g(x).$$

In conclusion, $g(x), x \cdot g(x), \ldots, x^{k-1} \cdot g(x)$ form a basis for C. From Chapter 2, the dimension of C equals k.

Slide #18. Proof of Theorem 4.2.17:
($\Longrightarrow$) Long divide $x^n + 1$ by $g(x)$:

$$x^n + 1 = g(x) \cdot q(x) + r(x),$$

where either $\deg r(x) < \deg g(x)$ or $r(x) = 0$. The above equality implies

$$g(x) \cdot q(x) \bmod (x^n + 1) = r(x) \bmod (x^n + 1) = r(x).$$

By Property ❷ on slide #14, we have
$g(x) \cdot q(x) \bmod (x^n + 1) \in C$, i.e., $r(x) \in C$.
Since $\deg r(x)$ cannot be smaller than $\deg g(x)$, we have $r(x) = 0$. Thus, $g(x)$ is a divisor of $x^n + 1$.

($\Longleftarrow$) Now suppose $g(x) \in K[x]$ is a divisor of $x^n + 1$. Let

$$C = \{a(x) \cdot g(x) \bmod (x^n + 1) \mid a(x) \in K[x]\}.$$

Observe that C is a cyclic code of length n because it consists of all linear combinations of all cyclic shifts of $g(x)$. We will prove that $g(x)$ is a generator polynomial for C by showing that $g(x)$ is the polynomial of smallest degree in C. Indeed, any polynomial $c(x) \in C$ equals the remainder when $a(x) \cdot g(x)$ is divided by $x^n + 1$, that is,

$$x^n + 1 = q(x) \cdot (a(x) \cdot g(x)) + r(x).$$

Since $x^n + 1 = t(x) \cdot g(x)$, we have

$$r(x) = (t(x) + q(x)a(x)) \cdot g(x).$$

The above equality yields either $r(x) = g(x)$ or
$\deg r(x) > \deg g(x)$. $\square$