10.24

($\Leftarrow$)

Suppose $G^T G = 0$.

G is the generator matrix of C, so any codeword $c = Gx$. For any other codeword $c' = Gx'$, we have $\langle c', c \rangle = x'^T G^T G x = x'^T 0 x = 0$. Therefore, $C \subseteq C^\perp$.

($\Rightarrow$)

Suppose a code w/ generator G is weakly self-dual, ie has $C \subseteq C^\perp$.

$C^\perp$ has generator matrix H^T & parity check matrix G^T, ie. $C^\perp$ is the kernel of G^T.

By definition, any $\tilde{c} \in C^\perp$ must satisfy $G^T \cdot \tilde{c} = 0$. But $C \subseteq C^\perp$, i.e. $G \cdot x \subseteq C^\perp \ \forall x$,

so, $G^T \cdot Gx = 0 \ \forall x$. This can only be so if $G^T \cdot G = 0$.

10.25 This statement is only true for binary linear codes

Case 1: $x \in C^\perp \rightarrow x \cdot y = 0 \quad \forall y \in C$

$$\rightarrow \sum_{y \in C} (-1)^{x \cdot y} = \sum_{y \in C} 1 = |C|$$

Case 2: $x \notin C^\perp$. This is surprisingly nontrivial.

$x \notin C^\perp$ implies x is not orthogonal to all codewords in C, ie. $\exists$ at least one codeword c^* s.t. $x \cdot c^* \neq 0$.

Scrutinizing the above, we realize this means $\exists$ at least one column of the generator matrix G, call this $\tilde{c}^*$, s.t. $x \cdot \tilde{c}^* \neq 0$. If we are working w/ binary codes, $\boxed{x \cdot \tilde{c}^* = 1}$.

Now, the codewords are formed by linear combinations of the columns of G.

Intuition ↳ Consider S, the set of linear combinations of columns apart from $\tilde{c}^*$.

Now, form $S^* = S + \tilde{c}^*$. $|S^*| = |S|$ (because suppose $a, b \in S$ and $a + \tilde{c}^* = b + \tilde{c}^* \rightarrow a = b$, but we can always choose a, b to be distinct. This proves $|S^*| \geq |S|$. But clearly $|S^*| \leq |S|$ by S^*'s definition.).

Furthermore, all codewords are contained in $S \cup S^*$, ie. $S \cup S^* = C$.

Note: what we actually want is $S \oplus S^* = C$, ie. we don't want $S^* = S$, which would happen if $\exists\, c_1, c_2 \in S$ s.t. $c_2 - c_1 = \tilde{c}^*$. Because then the first line below the sub-claim would be false.

Sub-claim: we can define S s.t. $\boxed{S \oplus S^* = C}$

Then $$\sum_{y \in C} (-1)^{x \cdot y} = \sum_{y \in S} (-1)^{x \cdot y} + \sum_{y \in S^*} (-1)^{x \cdot y}$$

$$= \sum_{y \in S} (-1)^{x \cdot y} + (-1)^{x \cdot (y + \tilde{c}^*)}$$

Since $x \cdot \tilde{c}^* = 1$, one of these two terms is 1 and the other is -1.

$$= \sum_{y \in S} 0 = 0.$$

Proof of subclaim:

Choose $S = \{$linear combinations of one of the cosets $C / \tilde{c}^* \}$

(ie. then $S^* = \{$L.C. of the other coset$\}$ so $S + \tilde{c}^* \neq S$ as desired).